



FileHold

Document & Record Lifecycle Software

LIBRARY ADMINISTRATION GUIDE

VERSION 14

Copyright ©2014 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
2. THE FILEHOLD LIBRARY	3
3. FILEHOLD SECURITY	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	14
4.5.1. MANAGING CABINETS	14
4.5.2. MANAGING DRAWERS	18
4.5.3. MANAGING FOLDER GROUPS	21
4.5.4. MANAGING FOLDERS	22
5. DOCUMENT SCHEMAS	23
5.1. CREATING DOCUMENT SCHEMAS	23
5.1.1. CREATING DOCUMENT SCHEMAS FOR OFFLINE DOCUMENTS	24
5.1.2. VERSION 0 SWITCH FOR OFFLINE DOCUMENTS	25
5.2. DOCUMENT AND VERSION CONTROL NUMBERS	25
5.2.1. VERSION CONTROL NUMBERS	26
5.2.2. DOCUMENT CONTROL NUMBERS	27
5.3. ADDING GROUPS OR USERS TO A SCHEMA	28
5.4. CREATING METADATA FIELDS FOR DOCUMENT SCHEMAS	29
5.4.1. WHY METADATA IS IMPORTANT IN A DOCUMENT MANAGEMENT SYSTEM	29
5.4.2. CREATING METADATA FIELDS	30
5.4.3. CREATING DRILL DOWN MENUS	32
5.4.4. CREATING DROP DOWN MENUS – DATABASE MANAGED	33
5.4.5. ADDING METADATA FIELDS TO SCHEMAS	35
5.5. WORKFLOW TEMPLATES	36
5.5.1. AD-HOC WORKFLOW TEMPLATES	37
5.5.2. WORKFLOW TEMPLATE EXAMPLES	38

5.5.3.	CREATING WORKFLOW TEMPLATES	41
5.5.4.	CLONING WORKFLOW TEMPLATES.....	45
5.5.5.	ADDING WORKFLOW TEMPLATES TO DOCUMENT SCHEMAS	46
5.5.6.	AUTOMATICALLY STARTING WORKFLOWS	46
5.5.7.	EDITING WORKFLOW TEMPLATES.....	47
5.6.	SETTING CUSTOM FILE NAMING.....	47
5.7.	AUTO-FILING SETTINGS.....	50
5.8.	EVENT SCHEDULES.....	51
5.8.1.	USING CUSTOM METADATA FIELDS FOR RETENTION POLICIES.....	53
5.8.2.	APPLYING RETENTION POLICIES TO DOCUMENT SCHEMAS.....	54
5.8.3.	SETTING THE NUMBER OF USER DEFINED NOTIFICATIONS ALLOWED IN A SCHEMA.....	56
5.9.	DATABASE LOOKUP ON THE SCHEMA.....	56
6.	GENERAL LIBRARY SETTINGS	60
6.1.	PERMANENTLY DELETING DOCUMENTS	60
6.2.	EMAIL ATTACHMENT SETTINGS.....	60
6.3.	EMAIL NOTIFICATION	61
6.4.	AUTO-FILING.....	61
6.5.	RESTRICTING ACCESS TO THE DOCUMENT MANAGEMENT SYSTEM.....	61
6.6.	DOCUMENT VIEWER CONFIGURATION.....	62
6.7.	SERVER SIDE OCR	63
6.7.1.	OCR STATUS.....	64
7.	SEARCH ENGINE CONFIGURATION	66
7.1.	SEARCH ENGINE SETTINGS	66
7.1.1.	REBUILDING THE FULL TEXT SEARCH INDEX.....	68
7.2.	SEARCH ENGINE STATUS.....	68
7.3.	UN-INDEXED FILES	69
7.4.	SEARCH ENGINE ERRORS.....	70
7.5.	EXCLUDING FILE TYPES FROM FULL-TEXT SEARCH	71
8.	WORKFLOW REPORTS AND TEMPLATES	73
8.1.	WORKFLOW STATUS REPORT.....	73
8.2.	WORKFLOW TEMPLATES.....	76
8.3.	WORKFLOW DASHBOARD	76
9.	LIBRARY UTILITIES	78
9.1.	CHECK-IN FOR USER.....	78

9.2. CHANGE DOCUMENT OWNER.....	78
9.3. CHANGE CABINET/FOLDER OWNER	79
9.4. RECOVER DOCUMENTS.....	80
9.5. DOCUMENT USAGE LOG.....	80
9.6. LIBRARY AUDIT LOG.....	81
10. SERVER SIDE DOCUMENT IMPORTATION.....	83
11. REPORTING SERVICES	85
11.1. VIEWING FILEHOLD REPORTS	86
11.2. SETTING REPORT SECURITY	87
12. MANAGE IMPORTS TOOL.....	88
13. EXTRACTION RULES	92
13.1. EMAIL HEADER EXTRACTION RULE.....	92
13.2. AUTOMATIC EXTRACTION OF METADATA VALUES FROM FILE PROPERTIES.....	93
13.3. AUTOMATIC EXTRACTION OF XML NODES FROM MICROSOFT WORD CONTENT CONTROLS	96
13.4. METADATA EXTRACTION FROM PDF FORMS	103
APPENDIX A: CONFIGURING THE XML FILE FOR AUTO-FILING.....	106
APPENDIX B: DOCUMENT VIEWER SUPPORTED FILE FORMATS	111
INDEX	114

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 types). 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.

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](#)
- [Library Utilities](#)
- [Server Side Document Importation](#)

- [Extraction Rules](#)

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.

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

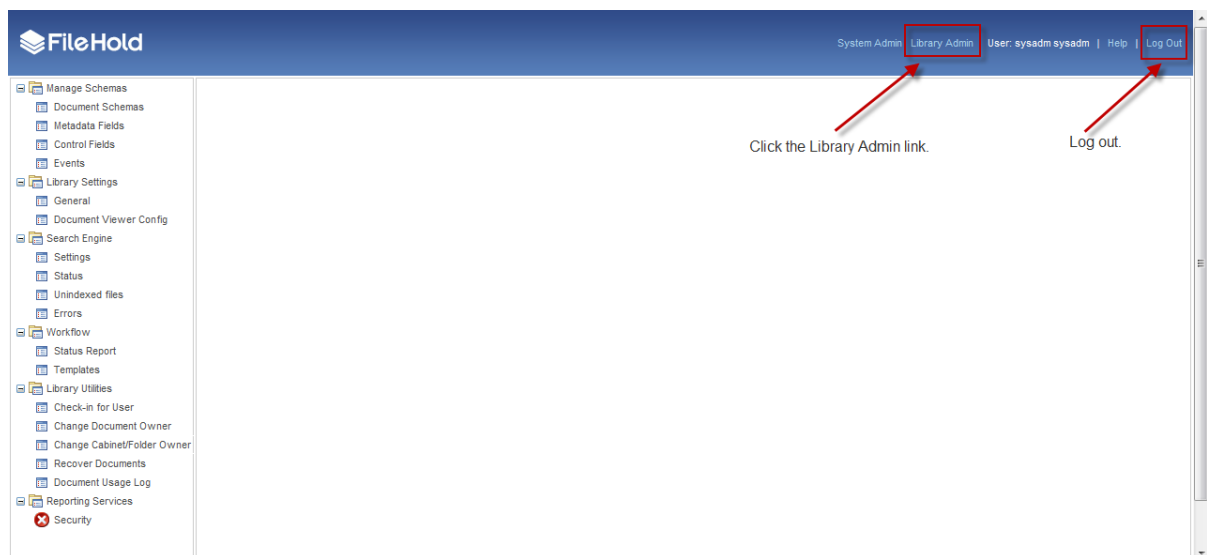
TO LOGIN TO LIBRARY ADMINISTRATOR IN THE WEB CLIENT

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 **Library Admin** link at the top of the screen.



TO LOG OUT FROM LIBRARY ADMINISTRATOR IN THE WEB CLIENT

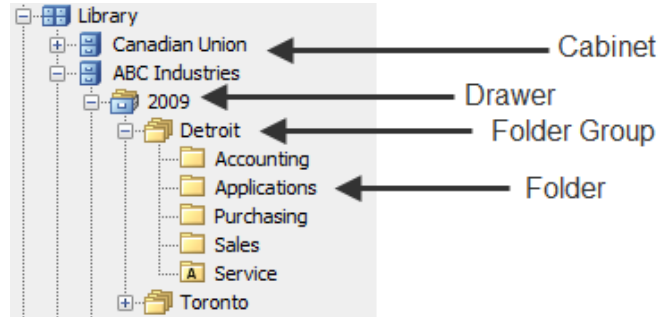
- Click **Log Out**.

TO ACCESS THE LIBRARY ADMINISTRATION FUNCTIONS IN FDA

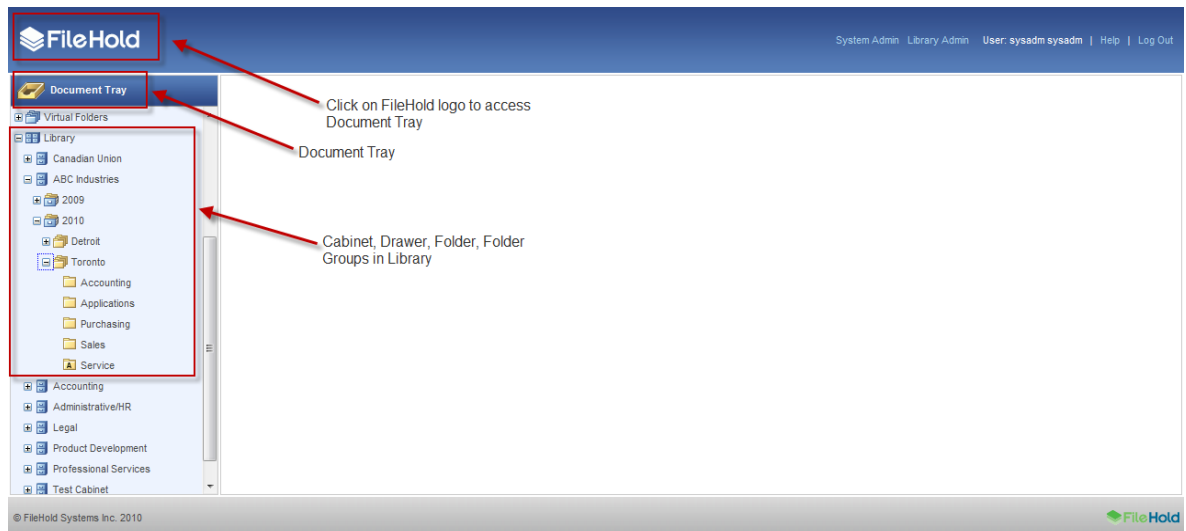
1. Log into FDA and go to **Administration** > **Manage Schemas or Workflows**.

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 or document types 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](#).


System Admin | Library Admin | User: sysadm sysadm | Help | Log Out

- Manage Schemas
 - Document Schemas
 - Metadata Fields
 - Control Fields
 - Events
- Library Settings
 - General
 - Document Viewer Config
- Search Engine
 - Settings
 - Status
 - Unindexed files
 - Errors
- Workflow
 - Status Report
 - Templates
- Library Utilities
 - Check-in for User
 - Change Document Owner
 - Change Cabinet/Folder Owner
 - Recover Documents
 - Document Usage Log
- Reporting Services
- Security

List of Document Schemas Add Schema

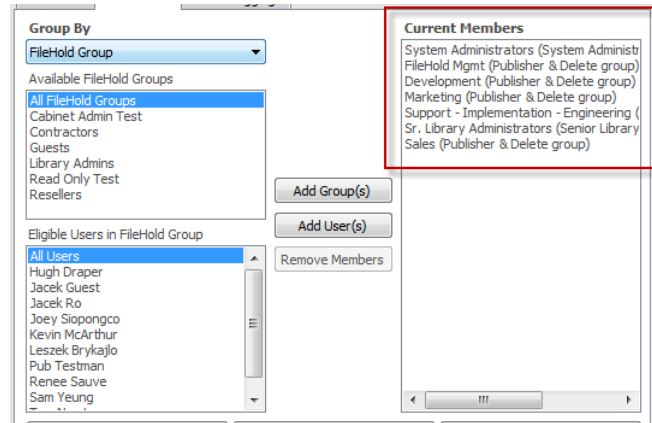
Schema Name	Type	Description	Last Modified	
Client Amendment Forms	Electronic Document		11/10/2010 10:56:28 AM	✘
Client Forms	Electronic Document		11/10/2010 10:56:28 AM	✘
Collective Agreement	Electronic Document	Union documents in the grievance process.	11/10/2010 10:56:28 AM	✘
Employee Forms	Electronic Document	Applications, Contracts, Vacation-Leave Requests etc	11/10/2010 10:56:28 AM	✘
Engineering Drawing	Electronic Document	Documents that are CAD, AUTOCAD format for Customer Projects	11/10/2010 10:56:28 AM	✘
Expense Reports	Electronic Document		11/10/2010 10:56:28 AM	✘
Inbound Email	Electronic Document		11/10/2010 10:56:28 AM	✘
Incoming Cheques	Electronic Document	Cheques to be deposited to Remittance Account	11/10/2010 10:56:28 AM	✘
Invoice	Electronic Document	Document Type Invoice for Corp's Invoices	11/10/2010 10:56:28 AM	✘
Invoices from Scanner	Electronic Document	Import from GSP	11/10/2010 10:56:28 AM	✘
Mortgages	Electronic Document		11/10/2010 10:56:28 AM	✘
Outbound Email	Electronic Document	Emails Being Sent	11/10/2010 10:56:28 AM	✘
Policy	Electronic Document	Vendor Documents	11/10/2010 10:56:28 AM	✘
QSP Invoices	Electronic Document	Import from quick scan pro	11/10/2010 10:56:28 AM	✘
Records Control Sheet	Offline Document	Physical Box Locator	11/10/2010 10:56:28 AM	✘
Test	Electronic Document		11/10/2010 10:56:28 AM	✘
Work Order	Electronic Document	Document Type Work Order. Used for new orders.	11/10/2010 10:56:28 AM	✘

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.

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) — it is not done in the Library Administrator area.

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 www.filehold.com/help/home 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 types is restricted by schema membership. Users must be a member of schema (document type) in order to view files associated with this document type in the document management system. For example, users in the sales department can be restricted to only add, search, and access sales document types (invoices, purchase orders and contracts) while users in the HR department can be restricted to only add, search and access only HR document types (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 Systems Administrator.

NOTE: Only a designated library administrator can change the membership associated with a document type (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 types.
- 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 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.

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	<p>A Guest User has read-only rights. Unlike all other roles, a user with the guest user role can log into FileHold many times. If multiple people log into FileHold with the same guest user name the log files will show 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.</p> <p>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.</p>
Read Only	<p>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.</p>
Document Publisher	<p>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.</p>

Role Name	Description
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	<p>Publisher user role can do everything a Document Publisher can do plus:</p> <ul style="list-style-type: none"> • 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	<p>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:</p> <ul style="list-style-type: none"> • 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. • 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
Organizer + Delete	<p>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.</p> <p>This role should be used by trusted personnel only.</p>

Role Name	Description
Cabinet Administration	<p>Cabinet Administrators can only administer the cabinets that they own; they cannot create cabinets for themselves. They can:</p> <ul style="list-style-type: none"> • 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. • 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. • 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. • Manually move document to and from the library archive as long as they are the Cabinet owner in the library archive.
Library Administration	<p>Library Administrators can perform, within their cabinets, the same functions as Cabinet Administrators plus:</p> <ul style="list-style-type: none"> • Create cabinets for which they will be the owner of and manage them in the Library. • Full access to FileHold's Library Administrator 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. • 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	<p>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.</p>

Role Name	Description
System Administrators	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.

NOTE: All roles provide document emailing capability. This 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.

4.5. CREATING A LIBRARY STRUCTURE

The file structure is 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.

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 with the 'General' tab selected. The 'Attributes' section contains the following fields:

- Name: New Cabinet
- Owner: Sabine Marie
- Description: New cabinet
- Default Schema: Client Forms
- Weight: 0

The 'This Cabinet Contains' section shows a table with the following data:

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

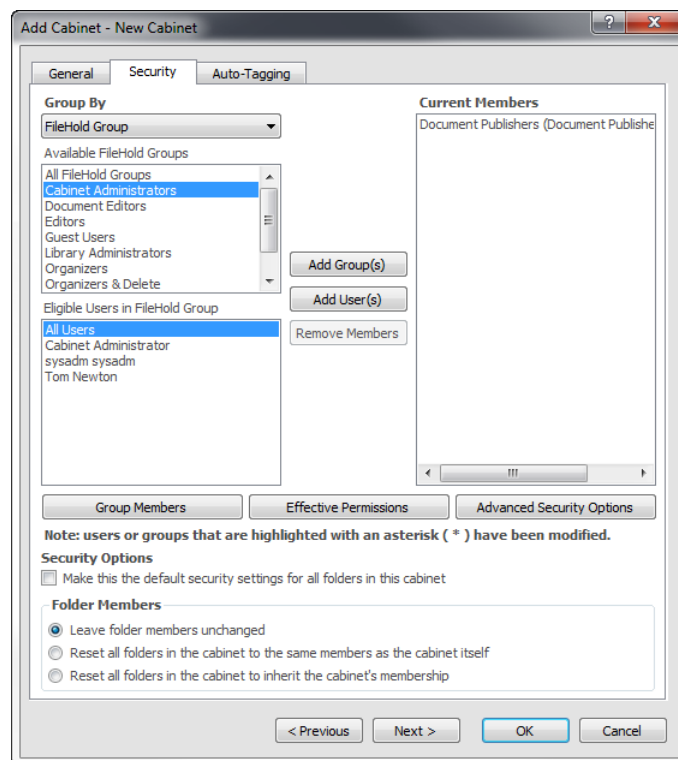
A 'Calculate' button is located to the right of the table. At the bottom of the dialog are buttons for '< Previous', 'Next >', 'OK', and 'Cancel'.

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.

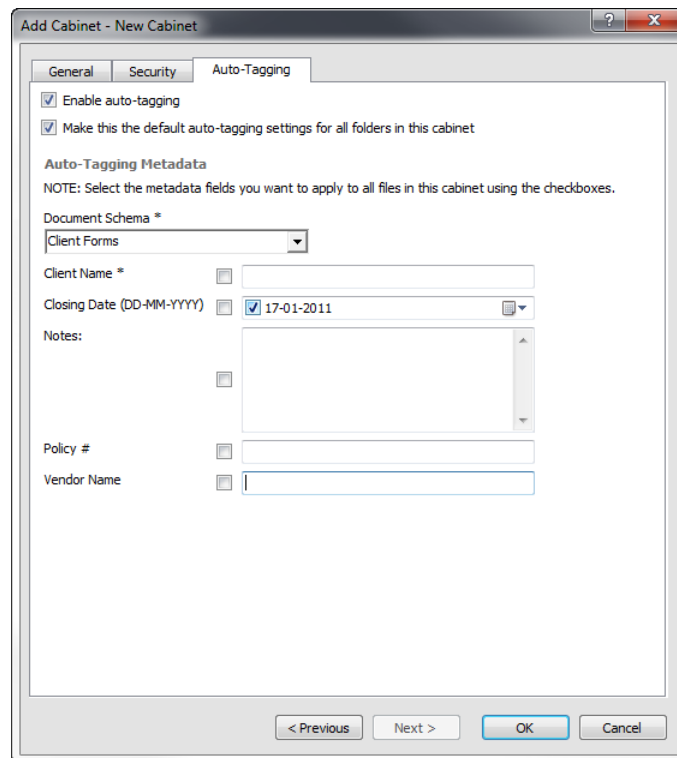
- To see which user roles the user or group belongs to, select the user or group name in the Current Members list and click **Effective Permissions**. The user role for that cabinet member will appear in the Effective Permissions list.
- To set advanced security options on a user or group, select the 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.
- 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.



4. 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.
5. Select the **Make this the default auto-tagging settings for all folders in this cabinet** if desired.

- 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**.



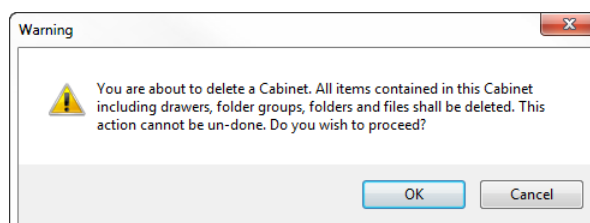
The screenshot shows the 'Add Cabinet - New Cabinet' dialog box with the 'Auto-Tagging' tab selected. The 'Enable auto-tagging' and 'Make this the default auto-tagging settings for all folders in this cabinet' checkboxes are checked. Under 'Auto-Tagging Metadata', a note states: 'NOTE: Select the metadata fields you want to apply to all files in this cabinet using the checkboxes.' The 'Document Schema' dropdown is set to 'Client Forms'. Below it, several metadata fields are listed with checkboxes: 'Client Name *', 'Closing Date (DD-MM-YYYY)' (set to 17-01-2011), 'Notes:', 'Policy #', and 'Vendor Name'. 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

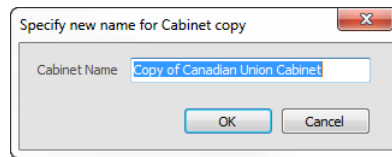
- Right-click on a cabinet in the library and select **Delete Cabinet**.
- You will receive a warning message. Click **OK** to delete the cabinet. The cabinet is removed from the library.



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**.

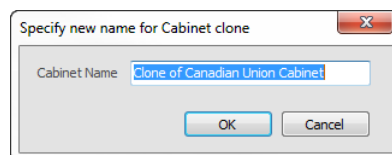
2. Enter a name for the copied cabinet and click **OK**. The copied cabinet appears in the library hierarchy.



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.

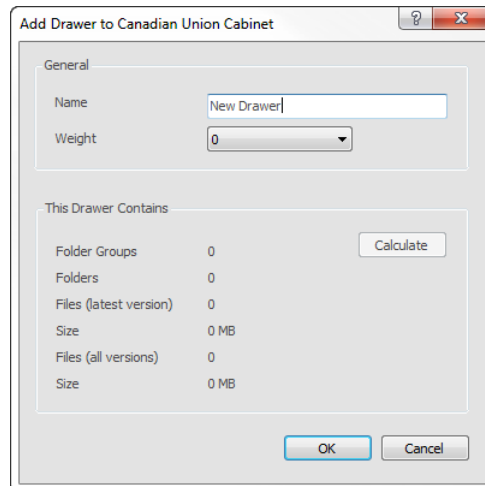
4.5.2. Managing Drawers

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.

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**.

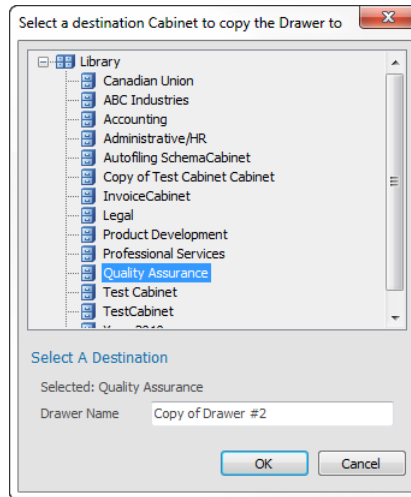
TO MOVE A DRAWER

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.

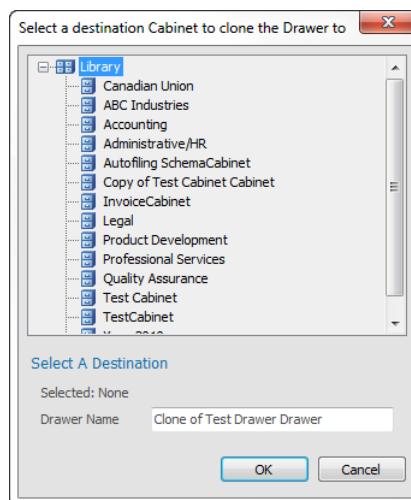
3. Enter a name for the copied drawer and click **OK**. The copied drawer appears in the library hierarchy.



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

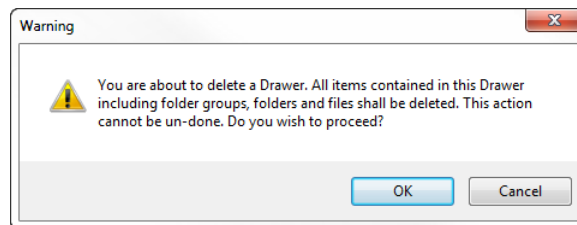
1. To clone a drawer, its security, and all of its contents including folders and folder groups (not documents), right-click on the drawer and select **Clone Drawer Structure**.
2. Select the destination for the cloned drawer and its contents by navigating through the library.
3. Enter a name for the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

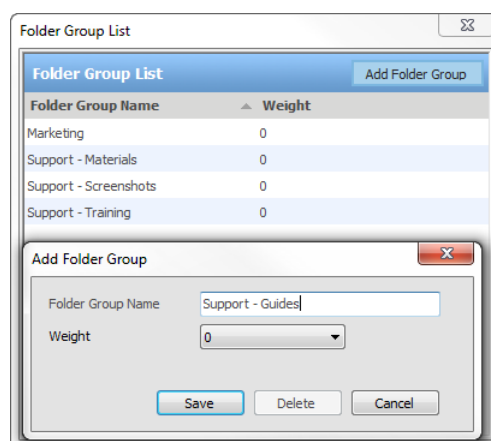


4.5.3. Managing Folder Groups

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.

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**.

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](#).

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 Type field. The schema that is selected will determine what metadata is required and the format that the metadata will take.

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

Document schemas manage the following document features:

- General — Create a schema with name, type, and document numbering conventions. See [Creating Document Schemas](#).
- Schema Membership — Define which groups have access to this schema. See [Adding Groups or Users to a Schema](#).
- Metadata — Define the metadata fields that are applied to a document. See [Creating Metadata Fields for Document Schemas](#).
- Workflow — Set up a review and approval process for a document that belongs to this schema. See [Workflow Templates](#).
- Custom Naming — Set up naming conventions for the documents. See [Setting Custom File Naming](#).
- Auto-Filing — Define the destination folder in the library. See [Auto-filing Settings](#).
- Event Schedule — Determine when to convert the document to a record, archive, or delete the document. See [Event Schedules](#).
- DB Lookup – Do a database lookup for all metadata fields in the schema. See [Database Lookup on the Schema](#).

There are three types of schemas:

- Electronic Documents are files that will change over time. 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.

TO CREATE A DOCUMENT SCHEMA

1. In the Web Client, in the Library Admin area, 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 type of schema:
 - 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** — Used to assign a specific number to a document and use it throughout its lifecycle. This field is useful for when documents are tightly controlled. 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. This feature is also known as a Document Control Number. You will need to set up control fields in the Control Fields section.
 - **Version Control Field** — Used to manage versioned documents. Documents that are checked in and out are given version numbers so files are not overwritten or deleted as they are updated. You can view the document version history and revert to a previous version. 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 type.

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 document type (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 types, 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-aculty-and-staffing-require...	Work Instructions		0	1	Checked In	8/2/2012 10:46 AM	REV-B
mechanical_example-internal	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 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. Log in as System Administrator and go to [System Admin > General > Document/Version Control Fields](#) area.
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 [Library Admin > Manage Schemas > 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 **Document Schemas > Schema Name > Step 2 Membership**, in the Group By field, select a group from the list.
 - Alternatively, in FDA, go to **Administration > Manage Schemas > Document Schemas > Schema Name > Membership** tab.
2. To add a group, select a group in the Available FileHold Groups area and click **Add Groups**.

3. To add individual users, select a user name in the Eligible Users in FileHold Group area and click **Add Users**.
4. 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**.
5. 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 type 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, <!, <?, </, 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 [Manage Schemas > 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 \(+ sign\)](#).

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. <ol style="list-style-type: none"> 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.

Field Type	Description
	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	Set up a list of option items which users can select from. <ol style="list-style-type: none"> To enter menu items, click Manage Menu Items. You can add, delete, and organize the order of the hierarchy by moving the items up and down. If multiple selections are allowed, select the check box. If there are duplicates in the list and would like them removed, select the check box. Enter an initial value, if applicable.
Drop Down Menu – Database Lookup	See Creating Drop Down Menu – Database Managed for more information.
Date	Configure a date field for the metadata properties. <ol style="list-style-type: none"> Select the Date Display Format. 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. <ol style="list-style-type: none"> Enter the number of Decimal Places. Enter the Decimal Separator. Enter the Group Separator. Select an option for how Negative Numbers will be displayed. Enter the Minimum Value. Enter the Maximum Value. Enter an initial value, if applicable.
Currency	Set up a currency field for the metadata properties. <ol style="list-style-type: none"> Enter the number of Decimal Places. Enter the Decimal Separator. Enter the Group Separator. Select an option for how Negative Numbers will be displayed. Select a Currency Symbol from the list. 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. Enter the Minimum Value.

Field Type	Description
	8. Enter the Maximum Value. 9. Enter an initial value, if applicable.
Check Box	Set a check box field for the metadata properties. <ol style="list-style-type: none"> Select on option for the check box: <ul style="list-style-type: none"> 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. <ol style="list-style-type: none"> Enter a URL link, if applicable, in the format <code>http://www.urlname.com</code>

- 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

- In the **Web Client > Library Administrator** area, go to **Manage Schemas > Metadata Fields**.
 - Alternatively, in the FDA, go to **Administration > Manage Schemas > Metadata Fields**.
- In the Add Metadata Field pane, enter a **Name** for the metadata.
- Enter a **Description** for the metadata.
- Select a **Drill Drop Down Menu** type.
- 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.
- Type in the first entry for the drop-down menu and click **Add**. Continue to add menu items until all selections are added.
- 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 – 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

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.

The document management server application has a scheduled task that runs hourly, and can also be run manually on demand, that populates all lookup values. We do not recommend that this task be run at intervals less than the 1 hour default. Please note that when you make a change to your database information, you need to either wait for the hourly scheduled task (FileHold database lookup fields synchronization) or go to the FileHold server and run the scheduled task manually.

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 FileHold Desktop Application (FDA) or ensure that you have your browser cache disabled so that the Web Client is showing you current information. The automatic browser cache of Microsoft Internet Explorer is especially problematic.

When the list retrieved from the database is presented to the user in the drop down list, only the first 100 items will be displayed in the FDA and the first 25 items in the Web Client. As the user scrolls through the list or starting typing the value, more values will be loaded into the view

but is limited to viewing 100 (FDA) or 25 (Web Client) values at a time. To change the number of items displayed in the Web Client drop down list, the parameter `<add key="ItemCountPerRequest" value="n"/>` can be added to the web.config file in `C:\Program Files\FileHold Systems\Application Server\WebClient\` (Windows Server 2008) where n is the number of drop down list items.

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.

TO CREATE A DROP-DOWN DATABASE LOOKUP METADATA FIELD

1. In the **Web Client > Library Administrator** area, go to **Manage Schemas > 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.
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. If using the Web Client, click **Preview** to view a preview of the metadata field.
 - If using the FDA, select the **Preview** tab.
17. If multiple selections of values are allowed, select the **Allow Multiple Selections** check box.
18. Enter an initial value, if applicable.
19. From the Web Client, click **Save**.
 - From the FDA, click **OK**.

5.4.5. 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.

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 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.

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

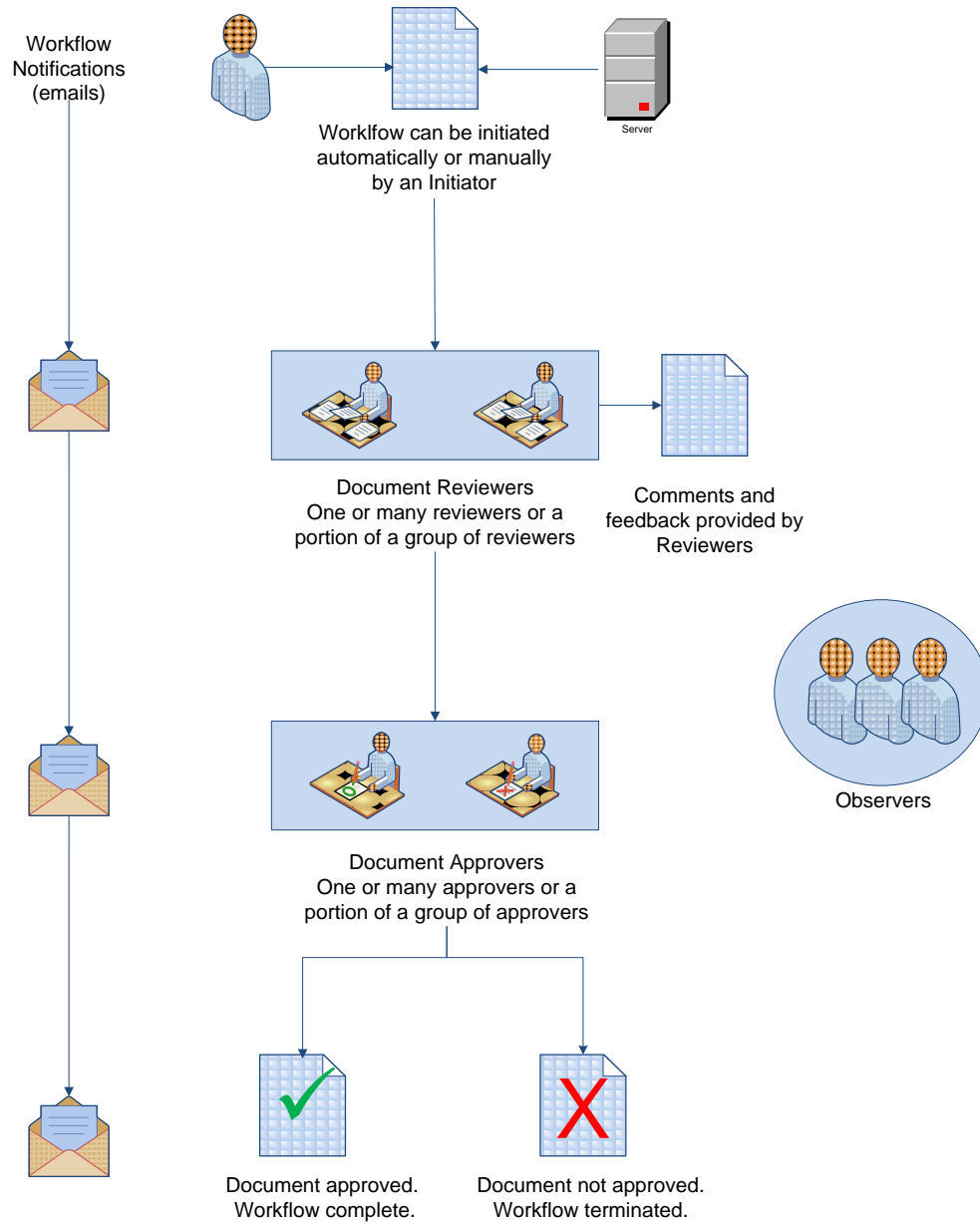
Allow Initiator to Define

5.5.2. Workflow Template Examples

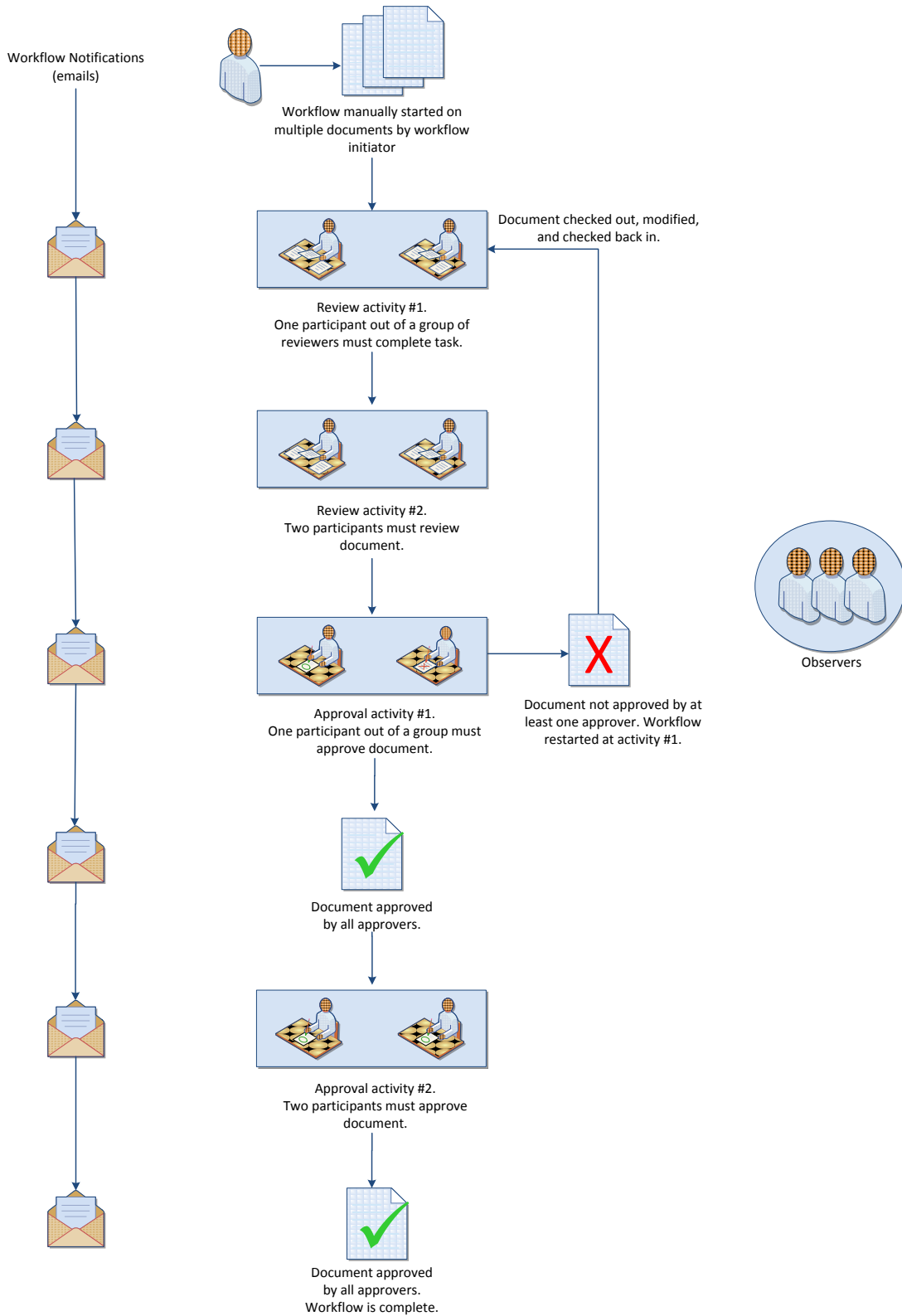
Workflow templates can be created to be as straight-forward or as complex as needed. Simple workflows may have a direct path from start to finish with few activities and minimum of participants involved. Complex workflows may involve one or more restarts, many participants, and several activities.

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 type. 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.
- 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](#).

TO CREATE A WORKFLOW TEMPLATE

1. In the Web Client, in the [Library Admin > Workflow > 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. Enter a name for the workflow. If the Initiator is to define the workflow template name, select the [Allow Initiator to Define](#) check box.

TIP: Renaming the workflow is useful since the My Tasks list and Workflow Status report displays the workflow name instead of individual document names. If the workflow template name is not altered, then several workflows with the same name appear in the views.

3. 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. If the Initiator is to define the description, select the [Allow Initiator to Define](#) check box.

4. The Used in Schemas area states which document schemas this template is being used. This area cannot be edited.
5. Select the **Initiator can modify (add/edit or delete) this workflow on initiation** 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.
6. 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. If the Initiator is to define this setting, select the **Allow Initiator to Define** check box.
7. Enter the number of days or hours before a task is overdue to send a task overdue notification email. If the Initiator is to define this setting, select the **Allow Initiator to Define** check box.
8. 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.
9. 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. If the Initiator is to define this setting, select the **Allow Initiator to Define** check box.
10. Select the **Allow document version owner to observe the workflow** check box to allow the document owner to see the workflow.
11. Click **Add Activity** to define the workflow activities. You can add up to 20 activities in a workflow.
12. In the Workflow Activity 1 area, select if this activity is an **Approval** or **Review** from the drop down list.
13. In the Approvers/Reviewers field, 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. 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.
 - If the Initiator is to define this setting, select the **Allow Initiator to Define** check box.

14. 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.
15. 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.
16. If only one of the 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.
17. 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. See the [End User Guide](#) or the [Knowledge Base](#) for more information on reserving tasks.

Workflow Template Settings	Effect on Workflow
<div style="border: 1px solid black; padding: 10px; width: fit-content; margin: auto;"> <p style="text-align: center;">Workflow Template</p> <div style="display: flex; align-items: center; margin-bottom: 10px;"> <input checked="" style="margin-right: 5px;" type="checkbox"/> 1 of X </div> <div style="display: flex; align-items: center;"> <input style="margin-right: 5px;" type="checkbox"/> Force Reservation </div> </div>	<ul style="list-style-type: none"> 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. <p>If a participant reserves the task:</p> <ul style="list-style-type: none"> 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
<div style="border: 1px solid black; padding: 10px; width: fit-content; margin: auto;"> <p style="text-align: center;">Workflow Template</p> <div style="display: flex; align-items: center; margin-bottom: 10px;"> <input checked="" style="margin-right: 5px;" type="checkbox"/> 1 of X </div> <div style="display: flex; align-items: center;"> <input checked="" style="margin-right: 5px;" type="checkbox"/> Force Reservation </div> </div>	<ul style="list-style-type: none"> • Only one participant in a group of participants in the activity can complete the task. • A participant must reserve the task before the task; the task cannot be completed without the reservation. • First participant to reserve the task voids the task for all other participants. The task is removed from their task list. • The activity is considered complete after the single participant reserves and completes the task. <p>If a participant reserves the task:</p> <ul style="list-style-type: none"> • 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.

18. Select the **Allow Check Out** 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, it must be enabled in the [System Administrator > 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. See the [User Guide](#) or [Knowledge Base](#) for more information. 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.
19. In the Due By field, enter the number of days or hours after workflow initiation that the approval or review is due. If the Initiator is to define this setting, select the **Allow Initiator to Define** check box.
 - 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.
20. In the Task Instructions field, enter the instructions for the reviewer or approver. If the Initiator is to define this setting, select the **Allow Initiator to Define** check box.
21. Repeat the above steps to add up to 20 activities to the workflow template.

22. The order of the activities can be changed using the number drop down list.
23. To remove an activity from the workflow template, click the red **X**.

The screenshot shows the 'Workflow Management' dialog box with the following configuration:

- Workflow Name ***: approval, auto
- Workflow Description**: (empty)
- Used in Schemas**: Application, Supply Agreement, offline with custom naming
- 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 0 days and 3 hours before for tasks that are going to be overdue.
 - Repeat notification every 24 hours
- Observers**: (empty)
- Allow document version owner to observe the workflow.

The second section is titled 'Approve Document' and includes:

- Approvers ***: Deborah Dixon, Renee Sauve
- Include Document Version Owner
- Include Workflow Initiator
- 1 of X
- Force reservation
- Allow Check Out
- Due By ***: 1 days and 0 hours after workflow initiation
- Task Instructions**: please approve

Buttons at the bottom: Add Activity, OK, Cancel.

24. Click **OK** or **Save** when the template is complete.

5.5.4. 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 **Library Admin > 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.

5.5.5. Adding Workflow Templates to Document Schemas

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, in the **Document Schema Wizard > 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 **Next** in the Document Schema Wizard to configure the Custom Naming.

5.5.6. Automatically Starting Workflows

Workflows can be started automatically based on a document type 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 **Document Schema Wizard > Step 4 Workflow**, select the workflow(s) to be associated with this schema and click **Add to Schema**.
2. 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.
3. In the Auto-Start Workflow area, select one of the following options:

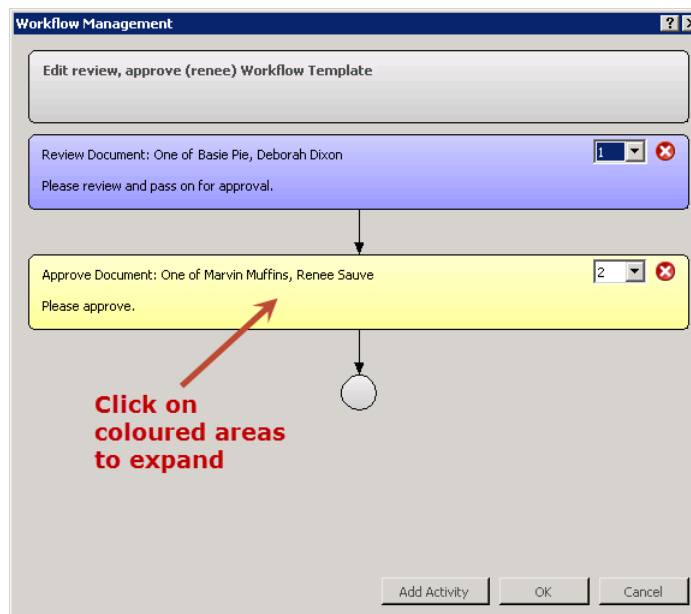
- Do not start any workflow automatically – This option should be selected for ad-hoc workflow templates.
 - Automatically start the following workflow when adding a new document of this type
 - Automatically start the following workflow when adding or checking in a document of this type
4. From the 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.
 5. Click **OK** or **Save** to save the changes.

5.5.7. 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

1. In the Web Client, go to **Library Admin > 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.
2. In the FDA, click on the coloured areas to expand and contract the different areas of the workflow template.



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

5.6. 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 [Manage Schemas > Document Schemas > Schema Name > Step 5 Custom Naming > Custom File Naming Standardization](#) area.
 - 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 the following table for rules.

For Metadata fields of type text, Drop Down Menu, Schema Name, and Owner:	
R	Specifies rightmost characters in a string. One R per character desired.
L	Specifies leftmost characters in a string. One L per character desired.
For Metadata fields of type Number, Currency, Version Number, Document No, and Size:	
9	Optional digit placeholder.
.	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.
-	Place " " (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.
mmmm	Month as its full name.
yy	Year as last two digits; leading zero for years less than 10.
yyyy	Year represented by four digits.

8. In the File Suffix Name field, enter a suffix up to 30 characters in length.

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

Custom File Naming Standardization

Rename files belonging to this Schema Do not rename files. Use the existing file name (default)
 Automatically rename files using the custom file naming pattern settings

Custom File Naming Pattern Settings

Sample Naming Pattern

Blank Spaces Handling Leave blank spaces
 Replace blank spaces with an underscore (_)
 Replace blank spaces with a hyphen (-)

File Name Prefix

Constant	Profile Field	Field Mask
<input type="text"/>	Customer Name - InvOCR	L10
<input type="text"/>	Invoice #	
<input type="text"/>	Invoice Date	DD MMM YYYY
<input type="text" value="_"/>	None Selected	
<input type="text" value="_"/>	None Selected	
<input type="text" value="_"/>	None Selected	
<input type="text" value="_"/>	None Selected	
<input type="text" value="_"/>	None Selected	
<input type="text" value="_"/>	None Selected	
<input type="text" value="_"/>	None Selected	
<input type="text" value="_"/>	None Selected	
<input type="text" value="_"/>	None Selected	

File Name Suffix

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

5.7. AUTO-FILING SETTINGS

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 four 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.

Once you have decided which auto-filing script to use for the schema, you will need to configure an XML file to set the proper membership (user or group) for the automatically created hierarchy. For more information on editing the AutoFilingMembership.XML file, please see [Appendix A](#).

FileHold is 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.

In order to be able to use the Auto-Filing settings, you will need to enable it first.

TO ENABLE AUTO-FILING

1. Go to **Library Settings > General**.
2. In the Auto-filing area, select the **Allow Auto-filing** check box.

TO SET AUTO-FILING

1. In the Document Schema Wizard > Step 6 Auto-Filing, select **the Automatically detect/create a destination folder based on auto-filing rules** option.
2. Select the auto-filing script you want to use from the list.

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

5.8. 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

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

Notifications Recurring Event

Send days before the event occurs.

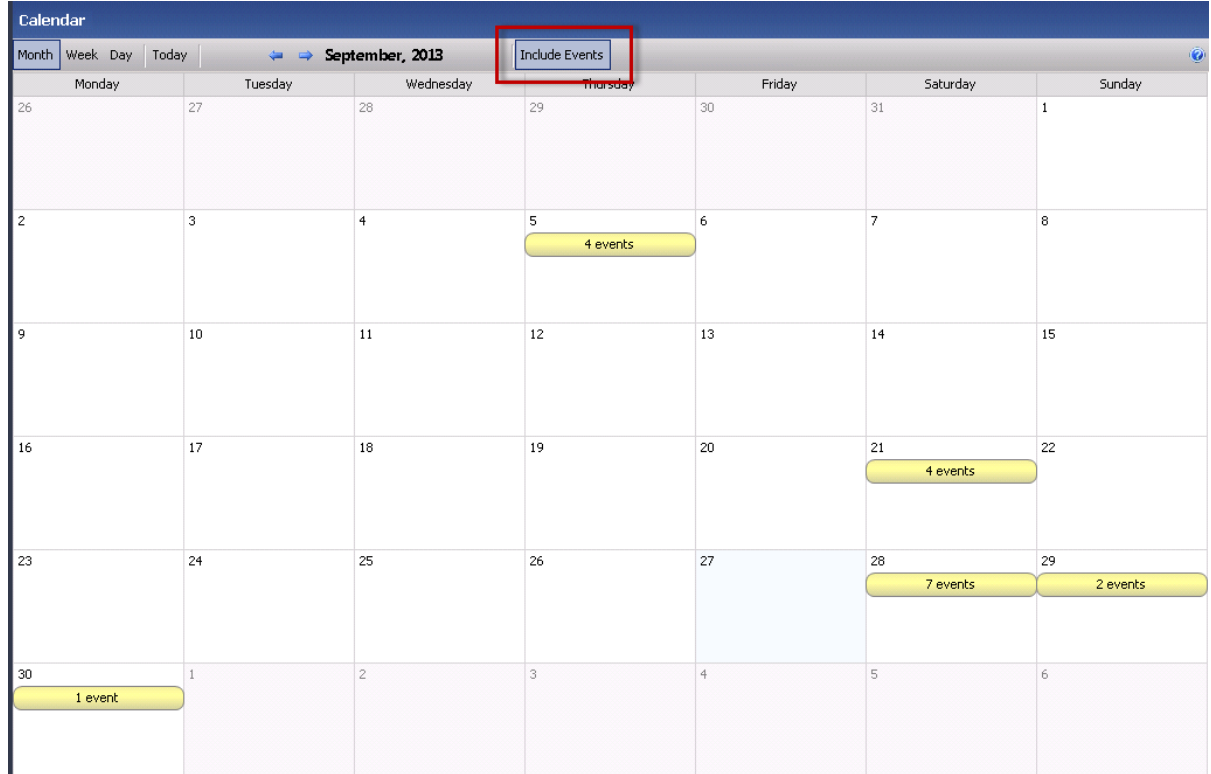
Email message

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.

5.8.1. 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 Administrator > 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. It can only be set as Read Only.

Name	Type	Visible	Required	Read Only	Order
Customer Name	Text	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1
VIN	Number	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	2
Notes	Text	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	3
Submission Date	Date	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	4
Claim #	Drill Do...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	5

5.8.2. 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 **System Admin > Global Settings > 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

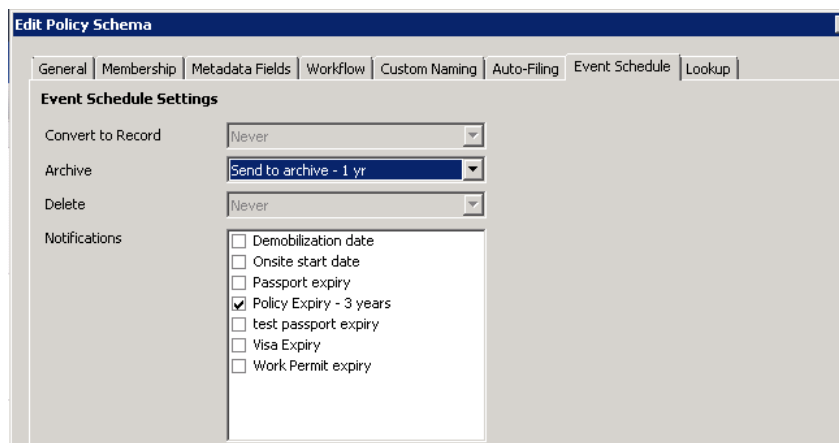
TO CREATE AN EVENT SCHEDULE

1. Do one of the following:

- In the Web Client, log in as **Library Administrator** and go to **Library Admin > Manage Schemas > 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 to 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. Log in as a Library Administrator. In the Web Client, go to [Document Schemas > Schema Name > 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**.

5.8.3. 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" />
```

5.9. 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.

TO CONFIGURE DATABASE LOOKUP FOR THE SCHEMA

1. In the Web Client, go to **Manage Schemas > Document Schemas > Schema Name > Step 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.

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
<input type="text" value="ModelName"/>	map to	Bike Model
<input type="text" value="Color"/>	map to	Colour
<input type="text" value="ListPrice"/>	map to	List Price
<input type="text" value="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 in the library. 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. Go to **Library Admin > Library Settings > General**.
2. Under General Settings, enter the number of days that a document can be permanently deleted after it has been soft deleted.
3. Click **Update**.

6.2. EMAIL ATTACHMENT SETTINGS

The email attachment setting allows you to specify if users are allowed to send documents from the library as attachments or as links when emailing documents from FileHold. If documents are emailed as links, only users with proper security membership can access the documents.

You can also specify the link type to allow users to use: FDA, Web Client, or both.

TIP: Links to the documents can be found in the version properties area of the metadata pane.

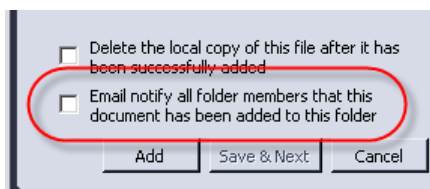
TO SET EMAIL ATTACHMENT SETTINGS

1. Go to **Library Admin > Library Settings > General**.
2. In the Email Attachment Settings area >Send Documents As field, select one of the following:
 - Either Attachments or Links
 - Attachments Only
 - Links Only
3. In the Link Type field, select one of the following:
 - Web Client links only — Allows you to send links from the Web Client.

- FDA links only — Allows you to send links from the FileHold Desktop.
 - Both Web Client and FDA links — Allows you to send links from both the FileHold Desktop and the Web Client.
4. Click **Update**.

6.3. 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.



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

1. Go to **Library Admin > Library Settings > 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.
 - To disallow email notifications, clear the check box.
3. Click **Update**.

6.4. 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 Auto-filing documents from the FDA Inbox check box.

6.5. 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 **Library Admin > Library Settings > 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.

6.6. DOCUMENT VIEWER CONFIGURATION

Viewers have many user features and many benefits that increase productivity and save companies money. Viewers are purchased on a per user basis and assigned to registered users by the IT administrator.

There are 2 viewer types available:

1. PDF/Image Viewer
2. Brava Viewer - The following are the three levels of Brava viewers available:
 - Enterprise Office Viewer
 - Enterprise Office Viewer with CAD support
 - Enterprise Office Viewer Engineering Edition

For a complete list of file formats that are supported, see [Appendix B](#).

You can configure the features of the viewer that is available to users when they are using the FileHold Desktop Application (FDA).

TO CONFIGURE THE VIEWER SETTINGS

1. Go to **Library Admin > Library Settings > General**.
2. Select a viewer type and select one or more of the following options. The type and level of viewer determines which settings are available. Not all settings are available in all viewer types.
 - Allow Users To Compare Documents
 - Allow Users To Publish Documents As Adobe PDF Files
 - Allow Users To Publish Documents As TIFF Files
 - Allow Users To Publish Documents As CSF Files
 - Allow Users To Save View In JPEG Format
 - Allow Users To Print / Print Regions Of Documents
 - Allow Users To Create ISO Banners / Watermarks For Printing
 - Allow Users To Copy Text and Markups In A Document To The Clipboard
 - Allow Users To Copy Regions Of Image Files To The Clipboard
 - Allow Users To View / Create / Edit Markups
 - Allow Users To Publish Documents As Dwf Files
 - Allow Users To Show Or Hide Layers

- Enable Measurement Tools For Users
 - CAD File Path References For Viewing Of CAD files
 - Enable Document Redaction (The redaction module is an optional feature. Contact sales@filehold.com for more information)
3. To select all the options, click **Check All**.
 4. To remove the selections, click **Uncheck All**.
 5. Click **Save**.

6.7. 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 Administrator > General page. See the [System Administration Guide](#) for more information.

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 maximum amount of time in which the server side OCR task runs can be configured in the web.config file located in *C:\Program Files\FileHold Systems\Application Server\LibraryManager*. The entry, under <appSettings>, is called <add key="OcrCommandTimeoutSec" value="270" />. 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" />.

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.

6.7.1. OCR Status

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

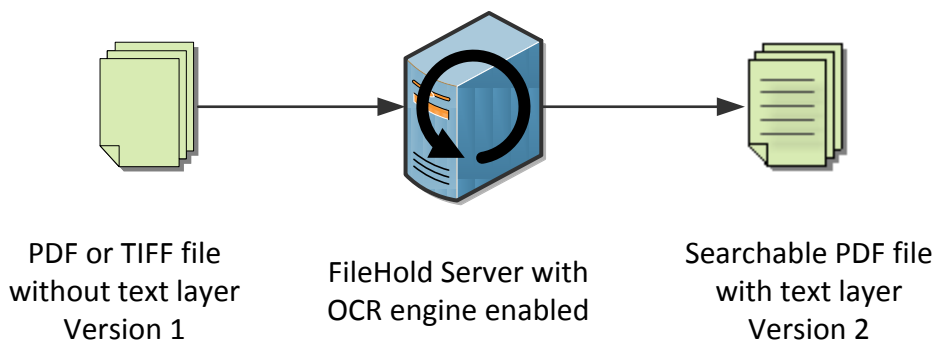
In the General area, the following information is displayed: the status of the OCR engine (enabled/disabled), if the higher priority of newly added documents or versions is enabled, the number of pending documents, and the number of processing errors as well as the list of errors.

When an error 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 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 **Web Client > Library Admin > Library Settings > OCR 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 Admin > 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 errors, the documents that triggered an error are displayed below. The list of errors displays:
 - FileHold ID of the document.
 - Date and time the OCR error occurred.
 - Details of the problem. Errors occur if the document is checked out, the document is under an active workflow, the document is encrypted, password protected, or corrupted, or the document does not have any valid text that can be recognized. The reason for the error is viewed in the Details tab.
 - 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, select the check box next to the FileHold ID and click **Re-add document(s) to OCR Queue**. To documents are re-added to the OCR queue for processing.

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

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	6

List of errors

From:
 To:

	FileHold Id	Date	Details
<input type="checkbox"/>	144	11/6/2013 11:36:07 AM	File has invalid extension.
<input type="checkbox"/>	144	11/6/2013 11:36:07 AM	A newer version of this document exists.
<input type="checkbox"/>	153	11/6/2013 11:26:04 AM	Document is encrypted.
<input type="checkbox"/>	150	11/6/2013 11:26:04 AM	Document is encrypted.
<input type="checkbox"/>	135	11/6/2013 11:21:10 AM	Document is encrypted.
<input type="checkbox"/>	32	11/6/2013 11:01:16 AM	Document is encrypted.

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 SETTINGS

Use the Search Engine settings to configure how you want the search feature to return data.

WARNING: Changing the search engine settings can dramatically affect system search performance. If you make any changes please note the previous settings and document your changes. Please read carefully all examples within this area. We recommend populating and using the system for a period of time before making major adjustments.

TO CONFIGURE SEARCH ENGINE SETTINGS

1. Go to **Library Admin > Search Engine > Settings**.
2. In the Search Result Metadata Weighting area, select the weighting of how strongly you want the metadata to influence the search results on a scale of 1 to 10. A selection of 1 puts more weighting on the content in the documents and a selection of 10 puts more weighting on the metadata. The suggested setting is 3 if you have strong metadata capture set in your schemas.

The screenshot displays the 'Search Engine Settings' interface. On the left is a navigation tree with 'Search Engine > Settings' highlighted. The main panel shows the following settings:

- Search Result Metadata Weighting:** A row of radio buttons from 1 to 10. The '3' radio button is selected, and the text 'Favour Document Metadata' is on the left and 'Favour Document Content' is on the right.
- Number of Files To Return:** A text input field containing '5,000' with the label 'Maximum number of Files to Return'.
- Stop Searching After:** A text input field containing '5,000' with the label 'files'.
- Search timeout:** A text input field containing '60' with the label 'Search timeout in seconds'.
- Stemmed Search:** A checkbox labeled 'Stemmed Search' that is checked, with a tooltip that reads 'Stemming finds other grammatical forms of the words in your search request. Example: A search for apples would also find apply.'

3. In the Number of Files to Return area, enter the number of files to return from a search. The default number is 5,000.
4. In the Stop Searching After area, enter the number of files to halt the search after the maximum number of files have been returned. For example, if the maximum number of files to return is set to 1,000 and the stop search is set to 5,000, the search will proceed until 5,000 files are found and the best matching of the 1,000 will be shown in the search results. The default number is 10,000. We recommend that you set this number to 500,000 if you have a very large collection of documents.
5. In the Search Timeout area, enter the time, in seconds, to terminate a search. This prevents server overload. The default is 60 seconds.

6. In the Stemmed Search area, select the check box if you want to use stemmed searching. Stemming finds other grammatical forms of the words in your search request. For example, a search for “applies” would also find “apply”.
7. In the Phonic Search area, select the check box if you want to use phonetically similar words. For example, Smith and Smythe.
8. In the Fuzzy Search Setting, select the check box if you want to enable fuzzy searching. Select a fuzzy search level from 1 to 10. Fuzzy search sifts through scanning and typographical errors. For example, a search for “alphabet” would find “alphaqet” with a fuzzy level of 1. A fuzzy level of 4 would find both “alphaqet” and “alpkaget.” Fuzzy search requires additional computational overhead so it is suggested to keep this setting less than 5 unless the documents in the library and metadata have frequent spelling errors. The recommended level is 2.

WARNING: We do not recommend using Stemmed Search, Phonic Search, Fuzzy Searching, nor Synonym searching for the vast majority of customers. They may change your search results wildly and should only be enabled in consultation with FileHold support support@filehold.com.

9. In the Synonym Searching area, select the check boxes to search for synonyms or related words.
10. In the Hyphen Searching area, you can set how hyphen characters are indexed and searched. Select from the following options:
 - Hyphen as ignore — Does not index the hyphen. For example, “first-class” will be indexed as “firstclass”.
 - Hyphen as a hyphen — Indexes the hyphen. For example, “first-class” will be indexed as “first-class”.
 - Hyphen as a space — Separates the hyphenated words into two words. For example, “first-class” will be indexed as “first” and “class”.
 - Hyphen all — Indexes a hyphen as all three of the above options.

WARNING: Changing hyphen settings will cause reinitialization of the full text search index and schedule reindexing of all documents. This should be done only after work hours as the search system will not function while this occurs.

11. In the Accent Support area, select the check box if you want indexing to be sensitive to accents. An accent-sensitive index converts characters, wherever possible, to a “base” character which is the letter A to Z or 0 to 9. Generally, accent-insensitive indexes are easier to use because they ensure that a document will be found even if the user omitted an accent when typing a word. In accent-sensitive indexes, each letter is converted to lower case where possible but otherwise characters re-indexed using their Unicode values. For example, e and é would be considered different letters and a search would not find the other.

WARNING: Changing accent settings will cause reinitialization of the full text search index and schedule reindexing of all documents. This should be done only after work hours as the search system will not function while this occurs. You generally do not need to use accent settings when managing English language documents.

12. In the Error Email Addresses area, select the groups of users that will receive a daily email with a summary of search engine warnings and errors.
13. In the Initialize Index area, click **Initialize Index** to start full-text search indexing.

WARNING: Use this feature only when absolutely necessary. This will wipe out the existing Full Text Search collection and create a queue for all documents in the system to be reindexed in the Microsoft SQL Databases. On large collections, this may also interfere

with documents being added to the system by FileHold users. This task takes considerable time and is only recommended if there are significant reasons for re-indexing the entire system. We recommend this be run over the weekend. Before doing this you should ensure an IT Administrator is available in case server changes are needed. The scheduled task runs this process, and an IT server administrator can disable this scheduled task (Update FTS index) during business hours. This process may take minutes or hours or longer - it depends on whether you have tens of thousands, hundreds of thousands or in millions of documents in your collection. Contact FileHold support if you have any questions.

14. Click **Update** to update the search engine settings.
15. Click **Restore Default** to revert the settings to their default values.

7.1.1. Rebuilding the Full Text Search Index

Rebuilding the index means that all documents stored in the library will be re-indexed along with the metadata tags associated with them.

WARNING: Rebuilding the index can take several hours to complete. Please initiate this during a time of low / zero user activity. Under normal operating conditions (and depending on the average size of the documents stored in the library) you can expect documents to be re-indexed at a rate of 5,000 (or more) per hour or more.

TO REBUILD THE RE-INDEX YOUR LIBRARY

1. Go to **Library Admin > Search Engine > Settings**.
2. In the Initialize Index area, click **Initialize Index** to start full-text search indexing.

WARNING: Use this feature only when absolutely necessary. This will wipe out the existing Full Text Search collection and create a queue for all documents in the system to be reindexed in the Microsoft SQL Databases. On large collections, this may also interfere with documents being added to the system by FileHold users. This task takes considerable time and is only recommended if there are significant reasons for re-indexing the entire system. We recommend this be run over the weekend. Before doing this you should ensure an IT Administrator is available in case server changes are needed. The scheduled task runs this process, and an IT server administrator can disable this scheduled task (Update FTS index) during business hours. This process may take minutes or hours or longer - it depends on whether you have tens of thousands, hundreds of thousands or in millions of documents in your collection. Contact FileHold support if you have any questions.

7.2. SEARCH ENGINE STATUS

You can view the status of the search engine. It shows information such as when the indexing last occurred, word count, state, document 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. Go to **Library Admin > Search Engine > Status**.

Full Text Search Index Status	
This shows the following status of the FileHold Full Text Search Engine. For more detailed information on how to re-build the full text search index go to the following help article. ?	
Fragmentation	122
DocCount	2006
CreateDate	10/6/2011 8:07:16 PM GMT
CompressedDate	Never
TaskQueueLength	0
PercentFull	0
ObsoleteCount	91
Flags	805306368
UpdatedDate	1/11/2012 4:59:21 PM GMT
IndexSize	74139109
WordCount	201987
StructureVersion	701
Fts Status	Idle
Fts Scheduled	No
Last Update State	Succeeded
<input type="button" value="Save Search Status"/>	

The key status indicators are:

- DocCount — Total files that have been indexed.
- Task Queue Length — How many documents are in the queue.
- Fts status — States if indexing process is currently running or disabled.
- Last Update — States if the FTS scheduled task and indexing system is running and current)

TO RUN THE FULL TEXT SEARCH STATUS REPORT

1. In the Search Engine > Status page, click **Save Search Status**.
2. You can open or save the search results in HTML format.

7.3. 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.

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 **Library Admin > Search Engine > Status**.
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.

List of Unindexed Files ?						
Document Name	Library Location	User Name	Date	Remove from the list	Replace	
<input type="checkbox"/> dvd - sys adm	Training and Support\FileHold 12\New Features	Renee Sauve	12/9/2011 8:27:19 AM	Checked Out	Replace	
<input type="checkbox"/> library book - editor	Training and Support\FileHold 12\New Features	Marvin Muffins	12/9/2011 8:02:07 AM	Checked Out	Replace	
<input type="checkbox"/> password_prot	Training and Support\FileHold 12\Alfonso	Joey Siopongco	10/6/2011 2:23:36 PM	Remove	Replace	

7.4. 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.
- 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 logins 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.

Time	EventType	ShortMessage
1/25/2011 11:38:21 PM	Add task	Index Job error(s). Index Job error(s) / SE 0001 Unable to access index C:\FileHoldData\FullTextSearch\DTIndex. The system cannot find the file speci...
1/25/2011 11:37:21 PM	Add task	Index Job error(s). Index Job error(s) / SE 0001 Unable to access index C:\FileHoldData\FullTextSearch\DTIndex. The system cannot find the file speci...
1/25/2011 11:36:20 PM	Add task	Index Job error(s). Index Job error(s) / SE 0001 Unable to access index C:\FileHoldData\FullTextSearch\DTIndex. The system cannot find the file speci...
1/25/2011 11:35:20 PM	Add task	Index Job error(s). Index Job error(s) / SE 0001 Unable to access index C:\FileHoldData\FullTextSearch\DTIndex. The system cannot find the file speci...
1/25/2011 11:34:19 PM	Add task	Index Job error(s). Index Job error(s) / SE 0001 Unable to access index C:\FileHoldData\FullTextSearch\DTIndex. The system cannot find the file speci...
1/25/2011 11:33:20 PM	Add task	Index Job error(s). Index Job error(s) / SE 0001 Unable to access index C:\FileHoldData\FullTextSearch\DTIndex. The system cannot find the file speci...
1/25/2011 11:32:19 PM	Add task	Index Job error(s). Index Job error(s) / SE 0001 Unable to access index C:\FileHoldData\FullTextSearch\DTIndex. The system cannot find the file speci...
1/25/2011 11:31:18 PM	Add task	Index Job error(s). Index Job error(s) / SE 0001 Unable to access index C:\FileHoldData\FullTextSearch\DTIndex. The system cannot find the file speci...
1/25/2011 11:30:18 PM	Add task	Index Job error(s). Index Job error(s) / SE 0001 Unable to access index C:\FileHoldData\FullTextSearch\DTIndex. The system cannot find the file speci...
1/25/2011 11:29:17 PM	Add task	Index Job error(s). Index Job error(s) / SE 0001 Unable to access index C:\FileHoldData\FullTextSearch\DTIndex. The system cannot find the file speci...
1/25/2011 11:28:16 PM	Add task	Index Job error(s). Index Job error(s) / SE 0001 Unable to access index C:\FileHoldData\FullTextSearch\DTIndex. The system cannot find the file speci...
1/25/2011 11:27:17 PM	Add task	Index Job error(s). Index Job error(s) / SE 0001 Unable to access index C:\FileHoldData\FullTextSearch\DTIndex. The system cannot find the file speci...
1/25/2011 11:26:16 PM	Add task	Index Job error(s). Index Job error(s) / SE 0001 Unable to access index C:\FileHoldData\FullTextSearch\DTIndex. The system cannot find the file speci...
1/25/2011 11:25:16 PM	Add task	Index Job error(s). Index Job error(s) / SE 0001 Unable to access index C:\FileHoldData\FullTextSearch\DTIndex. The system cannot find the file speci...
1/25/2011 11:24:16 PM	Add task	Index Job error(s). Index Job error(s) / SE 0001 Unable to access index C:\FileHoldData\FullTextSearch\DTIndex. The system cannot find the file speci...
1/25/2011 11:23:15 PM	Add task	Index Job error(s). Index Job error(s) / SE 0001 Unable to access index C:\FileHoldData\FullTextSearch\DTIndex. The system cannot find the file speci...
1/25/2011 11:22:15 PM	Add task	Index Job error(s). Index Job error(s) / SE 0001 Unable to access index C:\FileHoldData\FullTextSearch\DTIndex. The system cannot find the file speci...
1/25/2011 11:21:14 PM	Add task	Index Job error(s). Index Job error(s) / SE 0001 Unable to access index C:\FileHoldData\FullTextSearch\DTIndex. The system cannot find the file speci...
1/25/2011 11:20:14 PM	Add task	Index Job error(s). Index Job error(s) / SE 0001 Unable to access index C:\FileHoldData\FullTextSearch\DTIndex. The system cannot find the file speci...
1/25/2011 11:19:14 PM	Add task	Index Job error(s). Index Job error(s) / SE 0001 Unable to access index C:\FileHoldData\FullTextSearch\DTIndex. The system cannot find the file speci...
1/25/2011 11:18:14 PM	Add task	Index Job error(s). Index Job error(s) / SE 0001 Unable to access index C:\FileHoldData\FullTextSearch\DTIndex. The system cannot find the file speci...
1/25/2011 11:17:14 PM	Add task	Index Job error(s). Index Job error(s) / SE 0001 Unable to access index C:\FileHoldData\FullTextSearch\DTIndex. The system cannot find the file speci...
1/25/2011 11:16:14 PM	Add task	Index Job error(s). Index Job error(s) / SE 0001 Unable to access index C:\FileHoldData\FullTextSearch\DTIndex. The system cannot find the file speci...
1/25/2011 11:15:15 PM	Add task	Index Job error(s). Index Job error(s) / SE 0001 Unable to access index C:\FileHoldData\FullTextSearch\DTIndex. The system cannot find the file speci...
1/25/2011 11:14:15 PM	Add task	Index Job error(s). Index Job error(s) / SE 0001 Unable to access index C:\FileHoldData\FullTextSearch\DTIndex. The system cannot find the file speci...

TO MANAGE SEARCH ENGINE ERRORS

1. To hide known errors, click **Hide / Hide All**.
2. To show all errors, click **Show / Show All**.
3. 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.

7.5. 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* (Windows Server 2008). Modify the following section in the web.config file:

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

Where the list of file extensions that should be excluded in the search has a dot (.) in front of the extension and the extensions are separated with a semi-colon (;). For example:

```
<add key="FilteredFileTypes" value=".zip;.mdb;.rar" />
```

If at any time a file extension is removed from the list of excluded files in the web.config file, you will need to do a [manual re-index](#) of the files so that the excluded file types are indexed.

8. WORKFLOW REPORTS AND TEMPLATES

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.

Click the **View Details** link to 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.

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	
>	<input type="checkbox"/>	review, approve	2	Show Documents	Marvin Muffins	7/15/2013 10:56 AM	7/17/2013 10:56 AM	0%	View Details
>	<input type="checkbox"/>	review, approve	2	Show Documents	Marvin Muffins	7/12/2013 1:46 PM	7/16/2013 11:52 AM	50%	View Details
>	<input type="checkbox"/>	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
>	<input type="checkbox"/>	review, approve	2	Show Documents	Basie Pie	7/10/2013 3:16 PM	7/12/2013 3:16 PM	0%	View Details
>	<input type="checkbox"/>	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

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.

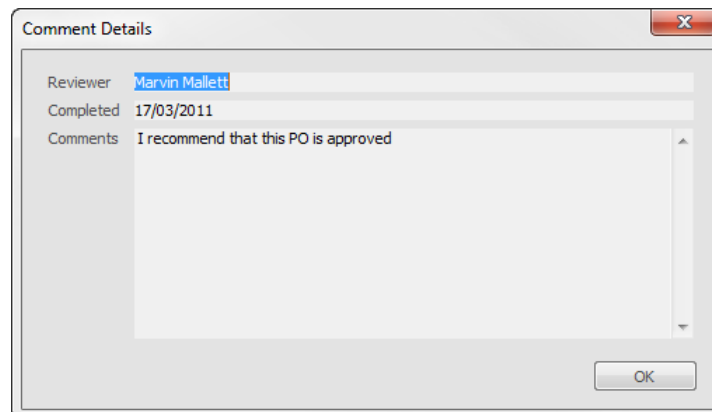
Cancel Workflow | Clear Completed | Clear Cancelled | Reserve/Undo Reservation | Override Task | Delegate Task

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			
	Activity	Type	Task	Participant	On Behalf of	Comments	Attachments	Started	Due	Completed	Status
	<input type="checkbox"/>	1	Review	1	sysadm*			7/12/2013 1:46 PM	7/13/2013 1:46 PM	7/15/2013 11:52 AM	Voided
	<input type="checkbox"/>	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
	<input type="checkbox"/>	2	Approval	1	Basie Pie*			7/15/2013 11:52 AM	7/16/2013 11:52 AM		
	<input type="checkbox"/>	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.



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.

TO RUN THE WORKFLOW STATUS REPORT

1. In Library Administrator, go to **Workflow > 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

1. 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** — Removes the completed workflows from the list.
 - **Clear Cancelled** — Removes the completed workflows from the list.
 - **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.
2. To expand the workflow details, click the **>** or **+** next to the workflow name. To contract the list, click **v** or **-**.

8.2. WORKFLOW TEMPLATES

You are able to view the list of all workflow templates. You can also create new workflow templates from this view.

Read how to [create workflow templates](#).

TO SEE A LIST OF WORKFLOW TEMPLATES

1. In Library Administrator, go to **Workflow > Templates**. The list of workflow templates is shown.
2. To create a new template, click **Add Workflow**. For more information on creating a workflow, see [To Create a Workflow Template](#).
3. To delete a workflow template, click **X**.

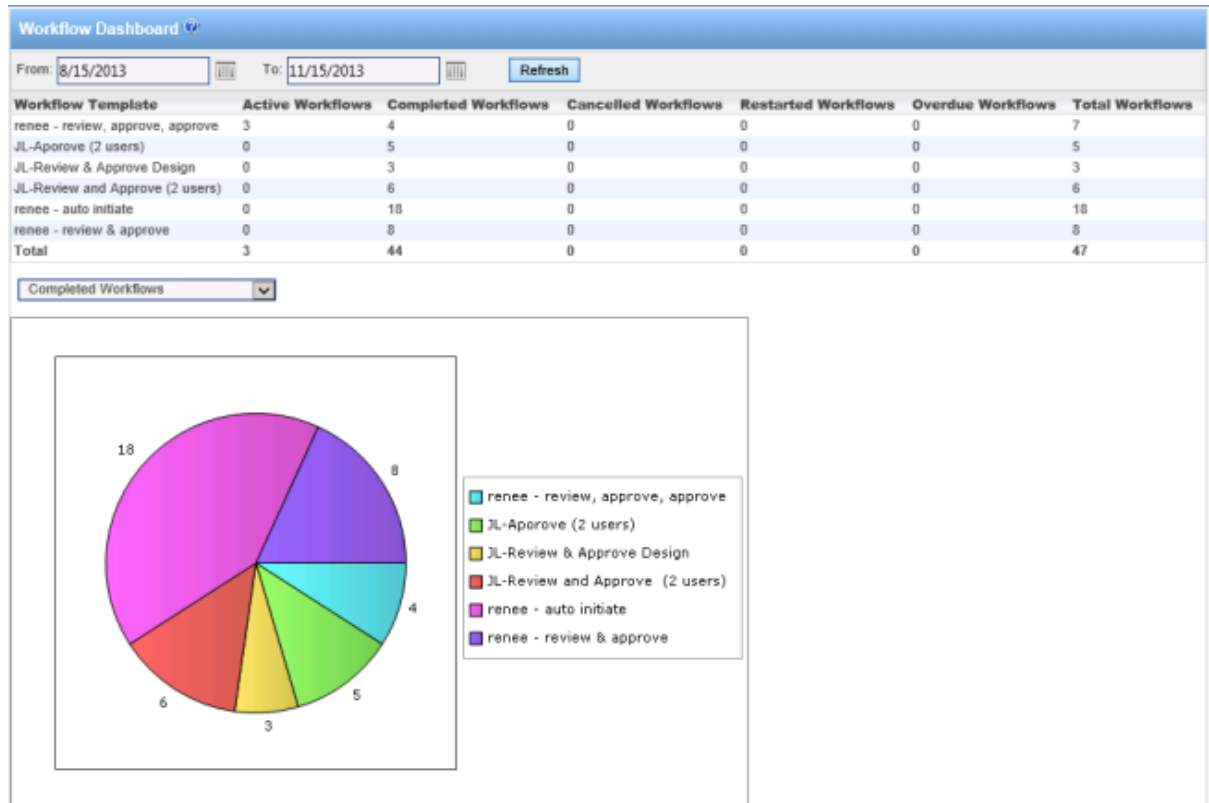
List of Workflow Templates					Add Workflow
Workflow Template Name	Activities	Description	Schemas Used In	Last Modified	
Purchase request approval over \$1000	Review, Approval	All purchase requests over \$1000 must be reviewed by Purchasing and approved by CFO.	Test, Purchase Order Request	12/9/2010 9:52:47 AM	✘
Send for Approval	Approval		Test, Cities	12/8/2010 2:18:50 PM	✘
Purchase request approval over \$5000	Review, Approval, Approval	All purchase requests over \$1000 must be reviewed by Purchasing and approved by CFO and President.	Purchase Order Request	12/9/2010 9:59:28 AM	✘

Click X to delete a workflow template

8.3. WORKFLOW DASHBOARD

The Workflow dashboard gives a high level overview of the 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.



TO USE THE WORKFLOW DASHBOARD

- Go to **Web Client > Library Administration area > Workflow > Dashboard**.
- 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.
- 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
- Click **Refresh** to update the information.

9. LIBRARY UTILITIES

Use the Library Utilities to:

- Check in documents for users
- Change document owners
- Change Cabinet or Folder owners
- Recover documents
- View the document usage log

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 check out 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.

TO CHECK IN A DOCUMENT FOR A USER

1. In Library Admin, go to **Library Utilities > Check in for User**.
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.

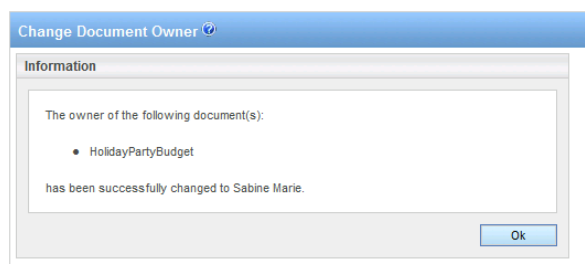
The Find People search results allows you to check in for a user that may have been deleted, disabled, or whose permissions have been changed (invalid) in the system. When changing

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.

TO CHANGE THE OWNER OF A DOCUMENT

1. In Library Admin, go to **Library Utilities > 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. 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.

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.

TO CHANGE THE OWNER OF A DOCUMENT

1. In Library Admin, go to **Library Utilities > 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**.



9.4. 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. Go to **Library Admin > Library Utilities > 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.

9.5. DOCUMENT USAGE LOG

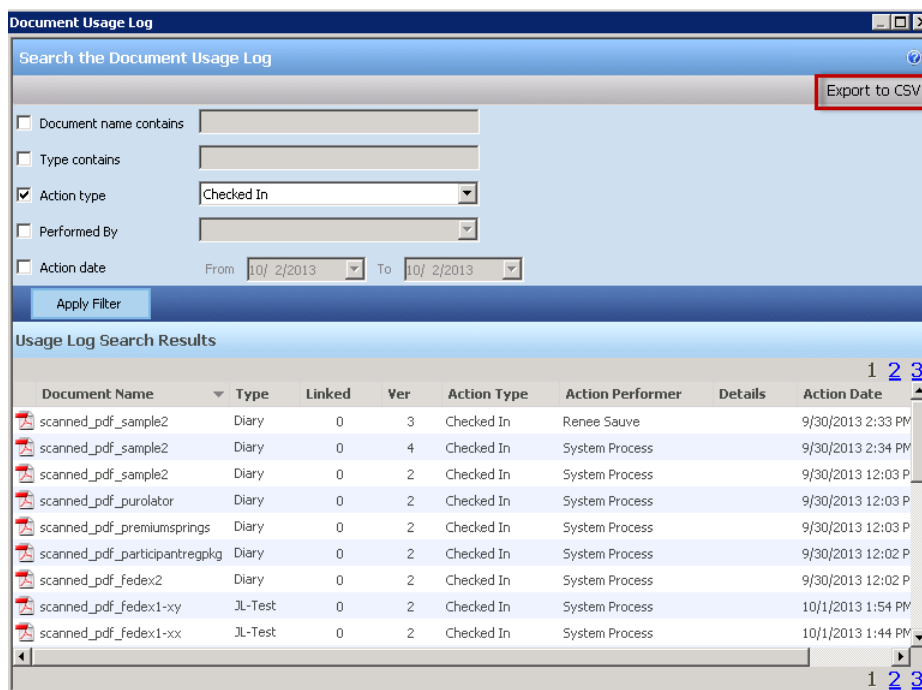
The document usage log provides a permanent record of all of the interactions that users have with individual versions of a file stored in the document management system. You can quickly search the entire database to reveal all interactions that any user has had with any document and when the interaction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

TO VIEW THE USAGE OF A DOCUMENT

1. In the Web Client, go to **Library Admin > Library Utilities > 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 list of search results will appear with all the actions that has been taken on the document.
 4. In the FDA, click **Export to CSV** to save all of the information in the view on the screen to a CSV file.



9.6. 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.

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 Library Administration area, go to [Library Utilities > Audit Log](#).
2. To filter by username, description, and/or date range, enter the information into the filter fields and click [Apply Filter](#). The results are displayed below.

10. SERVER SIDE DOCUMENT IMPORTATION

The Server Side Document Importation 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.

Several import “jobs” can be created by a Library Administrator or higher role. Each import “job” stores the configuration and status of the job. An administrator can configure the source type (Watched Folder 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.

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 fixed metadata field values. The files from the specified directory can be monitored and brought automatically into the system. The input files can also be deleted.

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.

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.

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

1. In the Web Client, go to **Library Admin > Automatic Document Importation > 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 a Source Type:

- **Watched Folder** – Documents are imported from a specified folder path. This folder can be on the server or in a network location; however, the folder **must have the FH Service account as a member and have full control permissions**.
 - **API** – Uses custom migration API code to add documents to the queue. See the [Knowledge Base for more information on API](#).
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 or API. 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 or API).
 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. If a Watched Folder source was selected, enter the **Source Folder Path**. This is the folder that is being “watched” for new documents and are brought into the queue.
 11. Select the **Delete Input Files** check box to delete the files from the source folder once they are imported into the library.
 12. 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.
 13. Click **Select** to set the Destination Folder from the library tree.
 14. Select the **Document Schema** from the list.
 15. Enter the values in the metadata fields. All fields marked with an asterisk (*) are required.
 16. Click **OK** to save the job. The job is added to the List of Import Jobs.

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 **Library Admin > Automatic Document Importation > 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 **Library Admin > Automatic Document Importation > 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 **Library Admin > Automatic Document Importation > 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 VIEW JOB DETAILS

1. In the Web Client, go to **Library Admin > Automatic Document Importation > 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 **Download 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. 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**.
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 **Library Admin > Automatic Document Importation > Import Jobs**.
2. In the List of Import Jobs, click **Enable** or **Disable** next to the job name.

11. REPORTING SERVICES

FileHold comes with some out-of-the-box standard reports. However, FileHold uses the Microsoft® SQL Server Reporting Services reporting tools that come standard with Microsoft SQL. This tool allows FileHold customers to generate their own reports using a standard supported reporting platform.

Customers are responsible for configuring, setting up, and maintaining SQL Reporting Services and integrating it with FileHold. FileHold technical support will only provide documentation on how to integrate them. Customers report that setting up this takes between 20 and 60 minutes. FileHold Systems limits support on this because this can be a very open ended process that involves creating custom reports and many things that are not part of product technical support. FileHold professional services can help write custom reports for customers requiring Microsoft SQL reports for a fee. Contact support@filehold.com for more information.

Microsoft® SQL Server™ Reporting Services is a complete platform for creating, managing, and delivering reports from a variety of data sources. Once the report is developed and tested, it can be deployed to the Microsoft® SQL Report Server and be viewed in the following different ways:

- In the FileHold Library under Reports.
- As a custom web page integrated into a web application.
- Via the SQL Server Reporting Services Home Page. Once on the home page users can navigate to the FH Reports folder and select a report to view.

Contact support@filehold.com if you require assistance in setting up the reporting services.

11.1. VIEWING FILEHOLD REPORTS

You are able to see the reports in the Library tree if the feature has been enabled and you have the correct permissions.

There are two standard reports that come with FileHold:

- Library List Report — Displays the contents of a Cabinet.
- System Activity Report — Displays all the logon activities of users.

TO VIEW REPORTS IN THE LIBRARY

1. In the Library, go to **Reports > FileHold Reports**.
2. Select a report from the list and click Show Report. The Report Manager opens.
3. Select or enter the parameters you want to be shown in the report and click View Report. The report results are shown.
4. You can now export the report into a XML, CSV, PDF, MHTML, Excel, Tiff, or Word file.

Client Type: FDA | User ID: | NULL | Last Name: | NULL | First Name: Basie | NULL | Login Time: | NULL | Logout Time: | NULL | View Report

Export | Select a format | Select an export format

FileHold Application Report

Client Type	Last Name	D	Login Time	Logout Time
FDA	McMarvin	Basie	12/8/2010 9:02:18 AM	12/8/2010 9:05:11 AM
FDA	McMarvin	Basie	12/8/2010 9:05:19 AM	12/8/2010 10:27:32 AM
FDA	McMarvin	Basie	12/8/2010 12:39:01 PM	12/8/2010 2:11:55 PM
FDA	McMarvin	Basie	12/8/2010 2:12:13 PM	12/8/2010 2:17:20 PM
FDA	McMarvin	Basie	12/8/2010 2:18:33 PM	12/8/2010 2:49:12 PM
FDA	McMarvin	Basie	12/8/2010 3:02:34 PM	12/8/2010 3:02:48 PM
FDA	McMarvin	Basie	12/8/2010 3:03:02 PM	12/8/2010 4:11:08 PM
FDA	McMarvin	Basie	12/9/2010 9:20:13 AM	12/9/2010 9:53:08 AM
FDA	McMarvin	Basie	12/9/2010 9:59:52 AM	12/9/2010 2:17:16 PM
FDA	McMarvin	Basie	12/9/2010 3:08:47 PM	12/9/2010 3:40:08 PM
FDA	McMarvin	Basie	12/13/2010 9:50:33 AM	12/13/2010 11:01:21 AM

Done

11.2. SETTING REPORT SECURITY

Library Administrators can configure and reassign the security (group and user access) to system reports. To use this feature you must first install, enable, and configure SQL Reporting Services.

TO SET REPORT SECURITY

1. Go to **Library Admin > Reporting Services > Security**.
2. In the Reporting Services Authorization window, click **Security**.
3. Select the Groups or Users that you want to allow access to the reports in the Library and click **Add Groups** or **Add Users**. The groups or users are added to the Current Members list.
4. Click **Save**.

12. MANAGE IMPORTS TOOL

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](#)
 - [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.

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 Type** 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.

Field	Description
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.

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.

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**. At the message prompt, click **OK**. 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, and Microsoft Office Word forms. Extraction rules only accessible in FDA by Library Administrators or higher permissions.

TO ACCESS THE EXTRACTION RULES

1. Go to **Tools > 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.

TIP: If the FileHold toolbar does not appear in the Add-Ins ribbon in Microsoft Outlook, refer to the Office Troubleshooting section.

NOTE: Email extraction rules do not work with 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
 - Create a date field for:
 - Date Sent:
3. Save the Email schema.

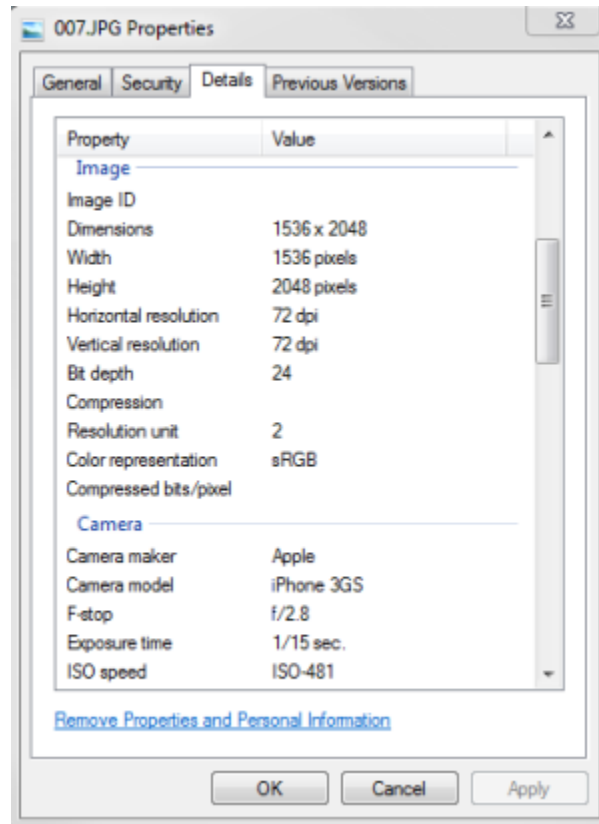
TO ENABLE THE EXTRACTION OF METADATA FROM EMAIL

1. In FileHold Desktop Application, go to **Tools > 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.

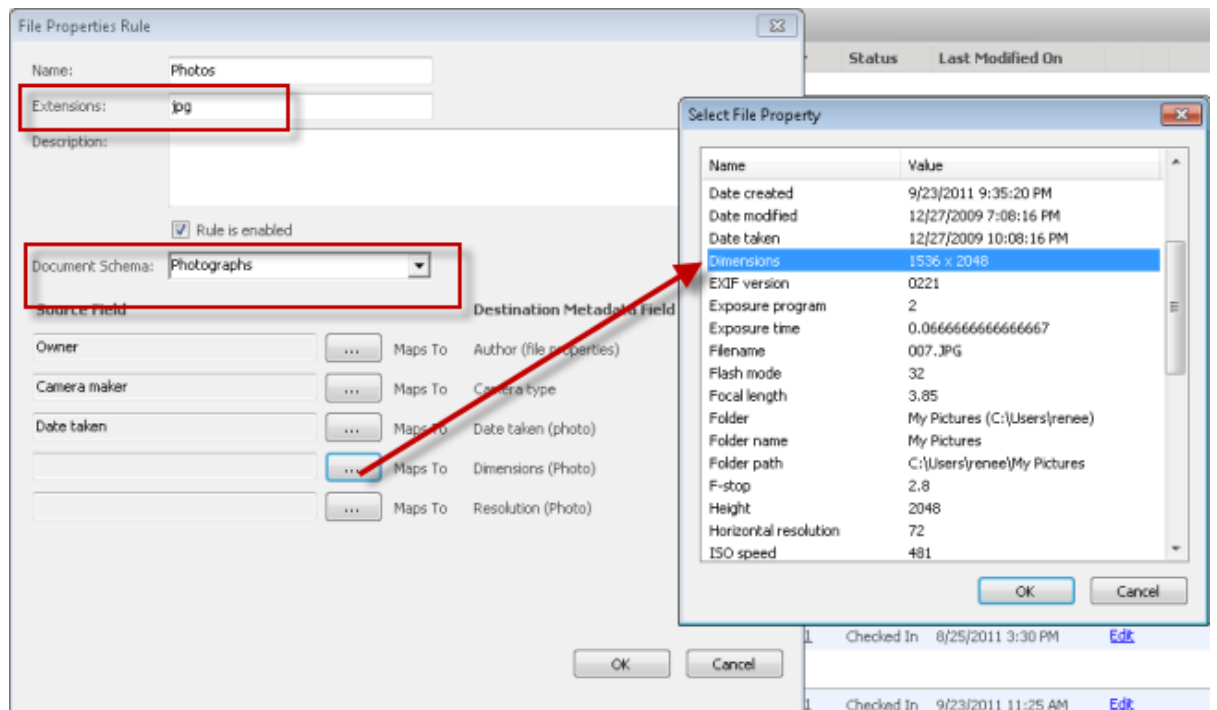
Only users with Library Administrator or higher permission can create extraction rules.

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. In FDA, go to **Tools > Extraction Rules > Add File Properties Rule**.
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 for the document type.
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 a 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.

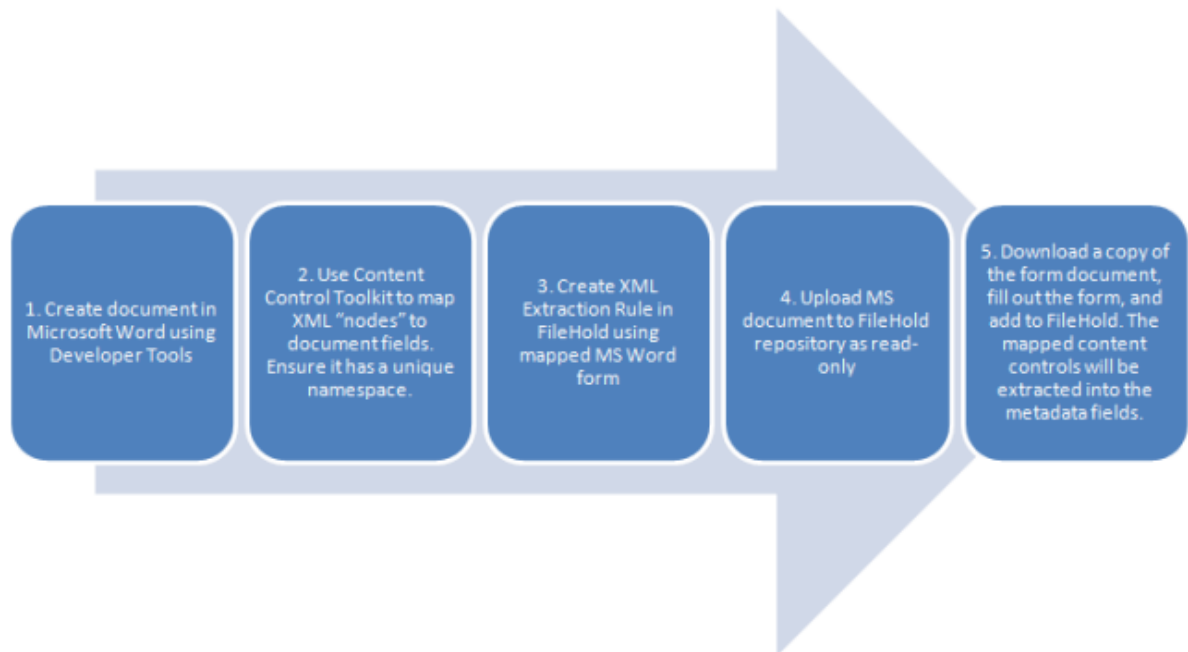
Once an e-Form is created in Microsoft Word, use the Word 2007 Content Control Toolkit to map the controls on the form to the custom XML parts. The free toolkit is made by Microsoft, is actively supported and available for download here: <http://dbe.codeplex.com/>

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.

Invoice

Pet Store Supply
Your cats and dogs love us!
250-4664 Laughed Hey
Burnaby BC V5C 3T5
1-877-833-1302

Invoice Number: Click here to enter text.
Date: Click here to enter a date.
Customer ID #: Click here to enter text.

To: Click here to enter text.
Click here to enter text.

Ship To: Click here to enter text.
Click here to enter text.

SALESPERSON	PO NUMBER	SHIPPING METHOD	SHIPPING TERMS	DELIVERY DATE	PAYMENT TERMS
Choose an item.	Click here to enter text.	Choose an item.		Click here to enter a date.	Due on receipt

QTY	ITEM #	DESCRIPTION	UNIT PRICE	LINE TOTAL
				SUBTOTAL
				SALES TAX
				TOTAL

Thank you for your business!

Invoice

Pet Store Supply
Your cats and dogs love us!
250-4664 Laughed Hey
Burnaby BC V5C 3T5
1-877-833-1302

Invoice Number: 12345
Date: 2/6/09/2011
Customer ID #: 45679

To: Basic Pie
Basic's Pet Store
111 Marinas Trench
Vancouver BC V6R 3T5

Ship To: Basic Pie
Basic's Pet Store
111 Marinas Trench
Vancouver BC V6R 3T5

SALESPERSON	PO NUMBER	SHIPPING METHOD	SHIPPING TERMS	DELIVERY DATE	PAYMENT TERMS
Tom Newton	895479	Ground		07/10/2011	Due on receipt

QTY	ITEM #	DESCRIPTION	UNIT PRICE	LINE TOTAL
1	4566-0455	Catnip	3.99	3.99
2	3244-9884	Kitty litter	5.99	11.98
				SUBTOTAL
				SALES TAX
				TOTAL

Thank you for your business!

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

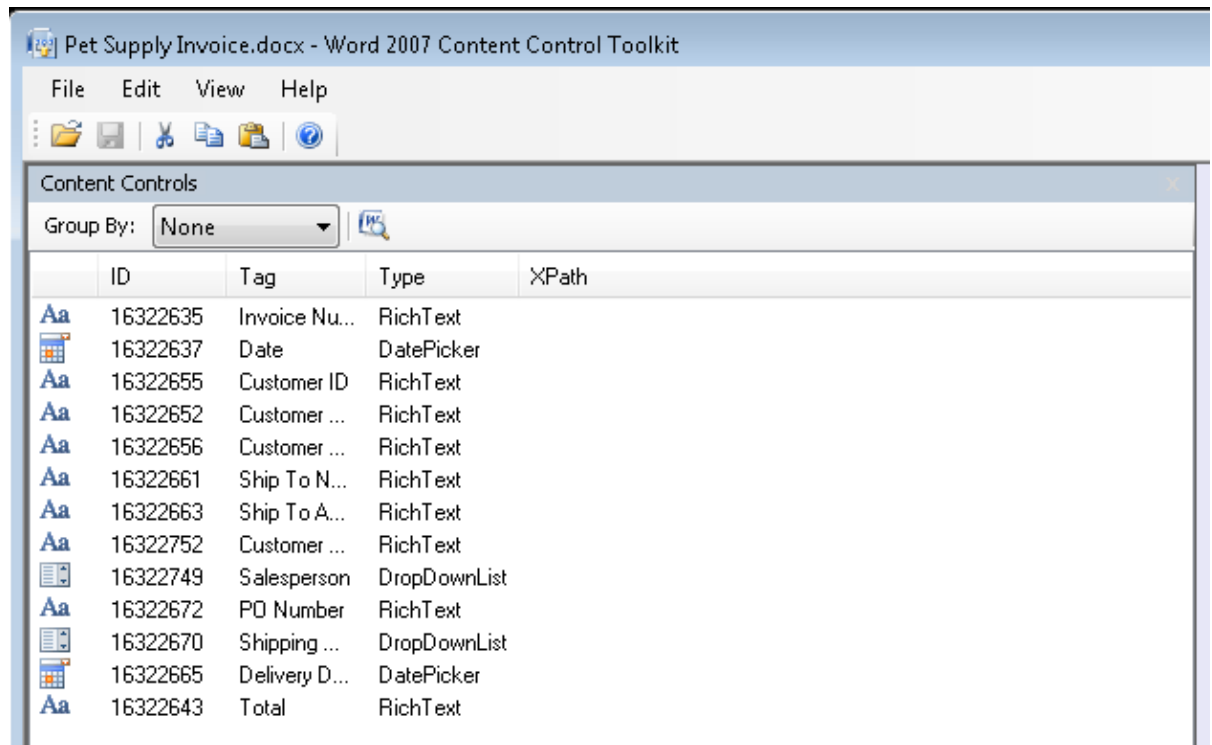
As previously mentioned, the Microsoft Word e-Form will require some additional configuration before the values from the content controls can be extracted. After the e-Form is created, the second step is to use the Word 2007 Content Control Toolkit to map the content controls in the e-Form to the custom 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/>.
2. 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.

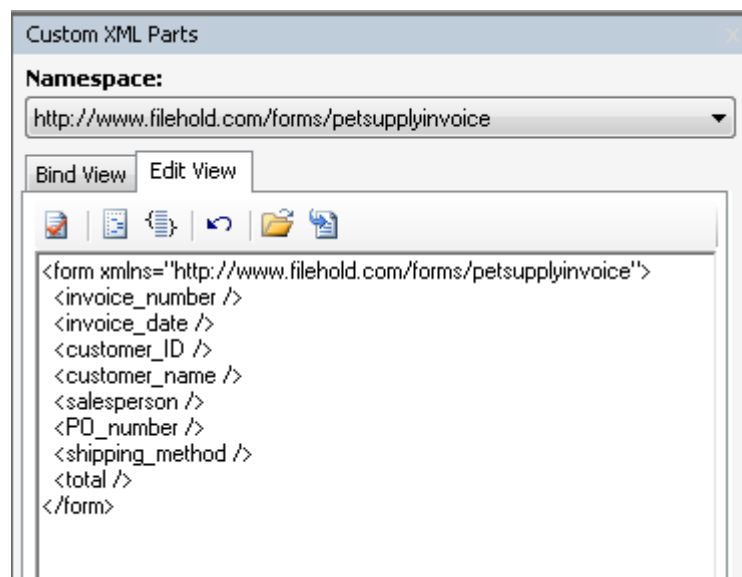


3. Create an XML file that contains a unique namespace and the XML nodes that you want to bind to the content controls. The unique namespace must be unique and written in a format of:

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

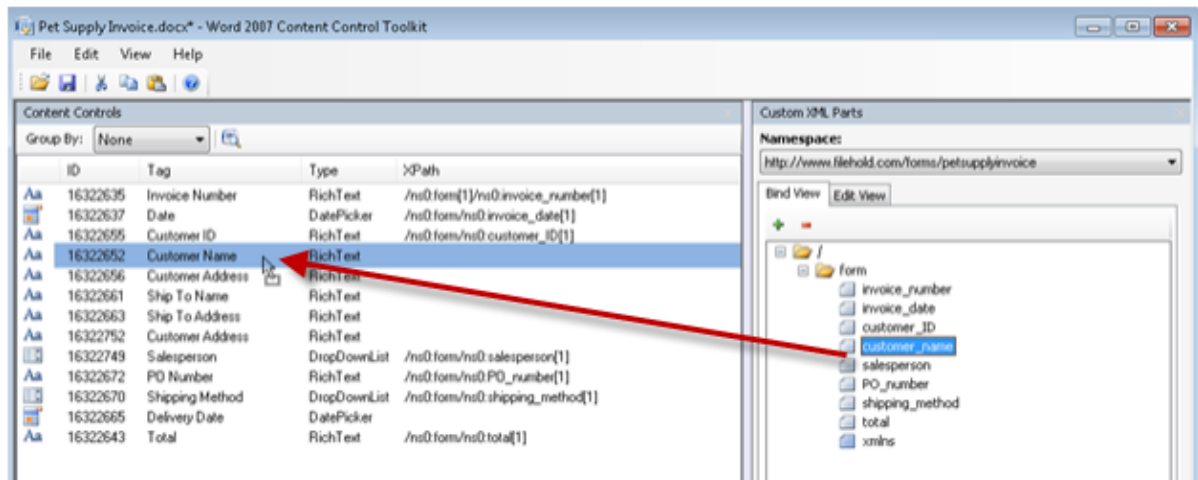
You can do this in the **Content Control Toolkit > Custom XML Parts > Edit View** tab or in another application such as Notepad and copy it over into the Edit View tab. For more information, see the Help in the Content Control Toolkit.

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.

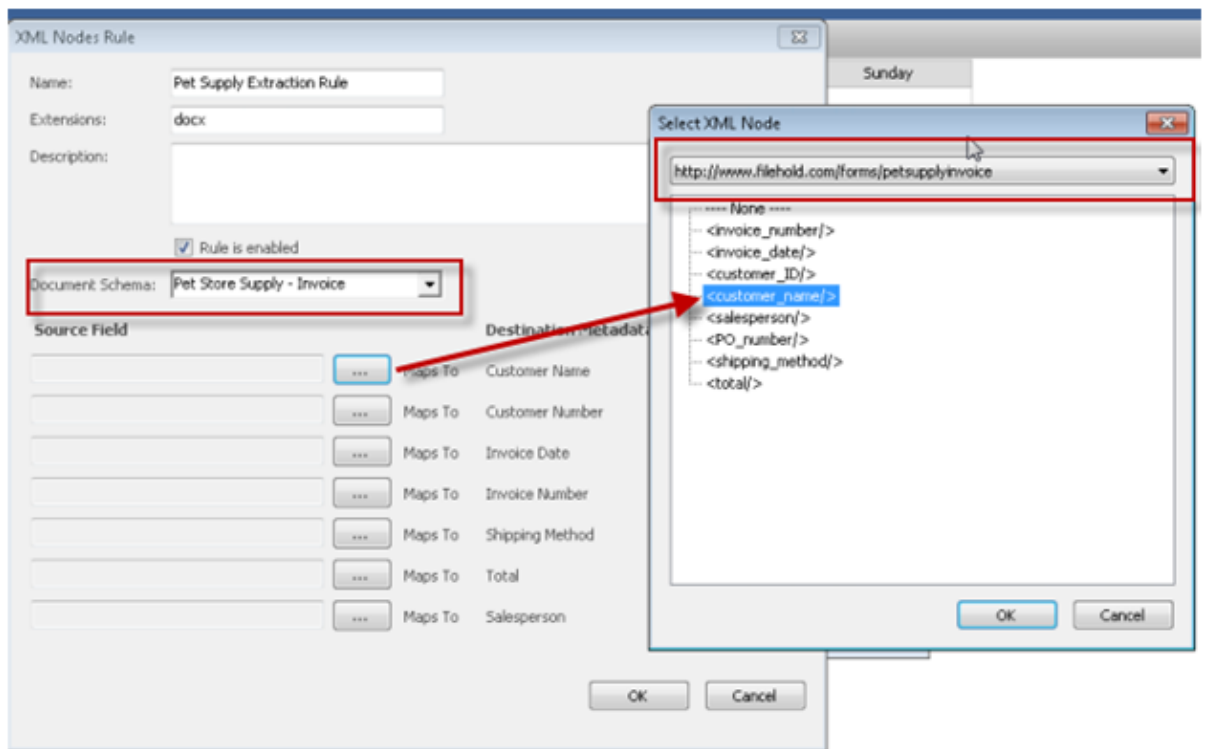
STEP 3: CREATE XML NODE EXTRACTION RULE IN FILEHOLD

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.

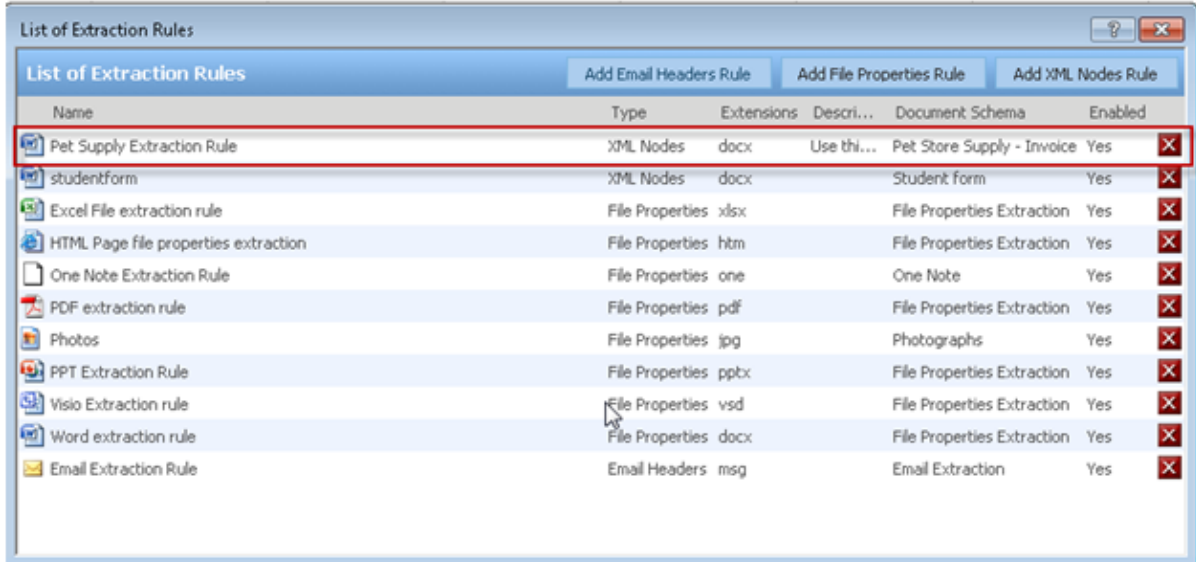
In the example, a specific schema called "Pet Store Supply – Invoice" was created to contain the metadata fields that will be extracted from the e-Form. When creating the XML Node extraction rule, you map the metadata field names in the schema to the "XML nodes" created in the Content Control Kit. Notice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

TO CREATE THE XML NODE EXTRACTION RULE

1. Open the FileHold Desktop Application (FDA) and go to Tools > 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 for the document type.
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.



Name	Type	Extensions	Descri...	Document Schema	Enabled
Pet Supply Extraction Rule	XML Nodes	docx	Use thi...	Pet Store Supply - Invoice	Yes
studentform	XML Nodes	docx		Student form	Yes
Excel File extraction rule	File Properties	xlsx		File Properties Extraction	Yes
HTML Page file properties extraction	File Properties	htm		File Properties Extraction	Yes
One Note Extraction Rule	File Properties	one		One Note	Yes
PDF extraction rule	File Properties	pdf		File Properties Extraction	Yes
Photos	File Properties	jpg		Photographs	Yes
PPT Extraction Rule	File Properties	pptx		File Properties Extraction	Yes
Visio Extraction rule	File Properties	vsd		File Properties Extraction	Yes
Word extraction rule	File Properties	docx		File Properties Extraction	Yes
Email Extraction Rule	Email Headers	msg		Email Extraction	Yes

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

Add Save & Next Cancel

Invoice

Pet Store Supply
four cats and dogs love us!
230-4664 Inglewood Hwy
Burnaby, BC V3C 3T3
6077433-1202

To:
Basie Pie
311 Marlmas Trnc h
Vancouver BC V4R 3T5

Ship To:
Basie's Pet Store
311 Marlmas Trnc h
Vancouver BC V4R 3T5

Invoice Number: 45639
Date: 21/09/2011
Customer ID #: 4587474

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

1. In FDA, go to **Tools > Extraction Rules > Add PDF Forms Rule**.
2. In the Select Template File window, select the PDF form "template" file from your computer and click **OK**.
3. In the PDF Forms Rule window, enter a name for the rule.
4. The Extensions field is automatically filled out with the type of PDF.
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 for the document type.
8. Map the metadata fields to the fields on the PDF form. Click **...** to select the PDF form field.

The screenshot shows the 'PDF Forms Rule' configuration window. The 'Name' field is set to 'Invoice', and the 'Extensions' field is set to 'pdf'. The 'Description' field is empty. The 'Rule is enabled' checkbox is checked. The 'Document Schema' is set to 'Invoice'. Below this, there are two columns: 'Source Field' and 'Destination Metadata Field'. The 'Source Field' column contains the following entries: 'form1/InvoiceNumber', 'form1/OrderNumber', 'form1/InvoiceDate', 'form1/Company', 'form1/Address', 'form1/StateProvince', and 'form1/ZipCode'. The 'Destination Metadata Field' column contains the following entries: 'Invoice Number', 'Order #', 'Date', 'Company (file properties)', 'Address', 'State', and 'ZIP'. Each source field is connected to its corresponding destination field via a 'Maps To' relationship. At the bottom right, there are 'OK' and 'Cancel' buttons.

9. Click **OK**.
10. ****Log off the FDA**** and log back in for the rule to take effect.
11. 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.
12. The values entered in the form and mapped in the extraction rule will appear in the metadata pane.

The screenshot shows the 'Metadata & File Properties' dialog box for the document 'Invoice_fillable_basie'. The 'Metadata' section is expanded, showing the following fields: '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), and 'Address' (678 Street). At the bottom, there are 'Save', 'Save & Next', and 'Cancel' buttons.

APPENDIX A: CONFIGURING THE XML FILE FOR AUTO-FILING

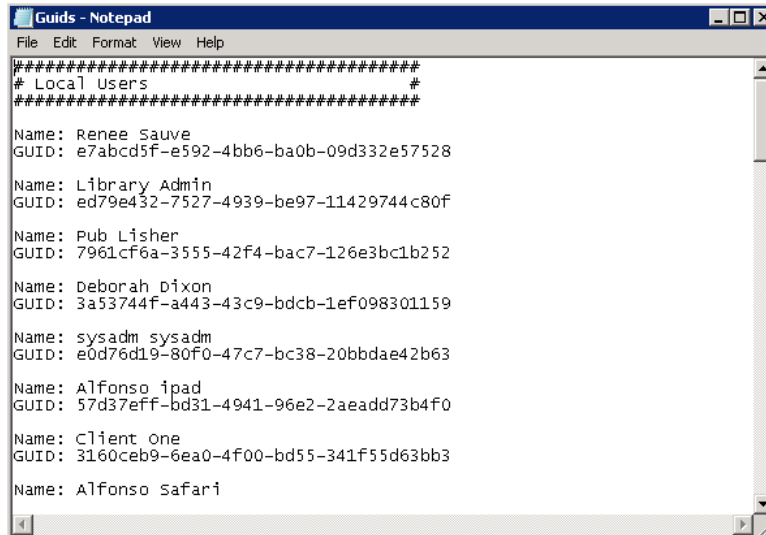
To set up Auto-filing in the FileHold system using the pre-configured scripts, you need to do the following:

- Get the list of GUIDs to assign membership to the automatically created Cabinets, Drawers, and Folders. A GUID is a unique ID number for each user and group.
- Edit the AutofilingMembership.xml file with the unique GUIDs.

A GUID is a unique ID number for each user and group in the FileHold system. You will need the GUID number in order to assign the automatically generated Cabinets/Drawers/Folders to a user or group. To get a list of the GUIDs for the users, you will need to run the ADAMDump application on the server.

TO RETRIEVE THE LIST OF GUIDS

1. On the FileHold server, run FH Instrumentation Tools (FHIT) in *C:\Program Files\FileHold Systems\Application Server\FHInstrumentation*.
2. In FHIT, go to Actions > ADAM objects management and select the Export GUIDs option.
3. Click **Start**.
4. In the Export GUIDs window, do the following:
 - Enter the name of the Microsoft SQL server that FileHold runs on.
 - Select an authentication option. Enter the username and password if required.
 - Set the destination to save the file on the server.
5. Click **Next**.
6. Click **Export**. You will receive a message that states that the export completed successfully.
7. Click **Finish**.
8. Open the GUIDs.txt file that was successfully exported.
9. Use the GUIDs in the file to assign membership to the Cabinets, Drawers, and Folders in the AutofilingMembership.xml file using the procedure below.



```

#####
# Local Users
#####
Name: Renee Sauve
GUID: e7abcd5f-e592-4bb6-ba0b-09d332e57528
Name: Library Admin
GUID: ed79e432-7527-4939-be97-11429744c80f
Name: Pub Lisher
GUID: 7961cf6a-3555-42f4-bac7-126e3bc1b252
Name: Deborah Dixon
GUID: 3a53744f-a443-43c9-bdcb-1ef098301159
Name: sysadm sysadm
GUID: e0d76d19-80f0-47c7-bc38-20bbdae42b63
Name: Alfonso ipad
GUID: 57d37eff-bd31-4941-96e2-2aeadd73b4f0
Name: Client One
GUID: 3160ceb9-6ea0-4f00-bd55-341f55d63bb3
Name: Alfonso safari

```

TO EDIT THE AUTOFILINGMEMEBERSHIP.XML FILE

1. On the FileHold server, go to *C:\Program Files\FileHold Systems\Application Server\LibraryManager\AutoFiling*
2. Open the XML file in Notepad or an XML editing tool.
3. Save the XML file once you have done editing the file with the GUIDs.

The following is an unedited AutofilingMembership.xml file:

```

<?xml version="1.0" encoding="utf-8"?>
<AutoFilingScripts xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <AutoFilingScript>
    <Name>Date-Based</Name>
    <Cabinet>
      <!--Here you can put a description of a member-->
      <Member>Please provide here a guid of a requested user in format dddddd-
ddd-dddd-dddd-dddddddddd</Member>
      <!--Here you can put a description of a member-->
      <Member>Please provide here a guid of a requested user in format dddddd-
ddd-dddd-dddd-dddddddddd</Member>
    </Cabinet>
    <Folder>
      <!--Here you can put a description of a member-->
      <Member>Please provide here a guid of a requested user in format dddddd-
ddd-dddd-dddd-dddddddddd</Member>
      <!--Alternatively uncomment this node to make folders inherit members from
cabinet-->
      <!--<Inherit />-->
    </Folder>
  </AutoFilingScript>
  <AutoFilingScript>
    <Name>SchemaName-Date-Based</Name>
    <Cabinet>

```



```

    <!--Here you can put a description of a member-->
    <Member>Please provide here a guid of a requested user in format dddddddd-
dddd-dddd-dddd-dddddddddddd</Member>
  </Cabinet>
  <Folder>
    <!--Here you can put a description of a member-->
    <Member>Please provide here a guid of a requested user in format dddddddd-
dddd-dddd-dddd-dddddddddddd</Member>
    <!--Alternatively uncomment this node to make folders inherit members from
cabinet-->
    <!--<Inherit />-->
  </Folder>
</AutoFilingScript>
<AutoFilingScript>
  <Name>FilePathFromMD</Name>
  <!-- Enter name of metadata field containing the destination location -->
  <MD_FieldName>Destination</MD_FieldName>
  <!-- Enter single character used as separator of location parts -->
  <Separator>/</Separator>
  <Cabinet>
    <!--Here you can put a description of a member-->
    <Member>Please provide here a guid of a requested user in format dddddddd-
dddd-dddd-dddd-dddddddddddd</Member>
  </Cabinet>
  <Folder>
    <!--Here you can put a description of a member-->
    <Member>Please provide here a guid of a requested user in format dddddddd-
dddd-dddd-dddd-dddddddddddd</Member>
    <!--Alternatively uncomment this node to make folders inherit members from
cabinet-->
    <!--<Inherit />-->
  </Folder>
</AutoFilingScript>
<AutoFilingScript>
  <Name>FixedDestination</Name>
  <Cabinet>
    <!--Sysadm group-->
    <Member>19da0d5b-69ee-4738-b790-394a0b689351</Member>
  <!--doc pub group-->
    <Member>b40240cd-1f52-4456-b347-ec0885570778</Member>
  </Cabinet>
  <Folder>
    <!--Sysadmin group-->
    <Member>19da0d5b-69ee-4738-b790-394a0b689351</Member>
    <!--doc pub group-->
    <Member>b40240cd-1f52-4456-b347-ec0885570778</Member>
    <!--Alternatively uncomment this node to make folders inherit members from
cabinet-->
    <!--<Inherit />-->
  </Folder>

```

```
</AutoFilingScript>
</AutoFilingScripts>
```

Here is a sample of an edited AutofilingMembership.xml file using the GUIDs:

```
-----
<?xml version="1.0" encoding="utf-8"?>
<AutoFilingScripts xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <AutoFilingScript>
    <Name>Date-Based</Name>
    <Cabinet>
      <!--Engineering Publishers-->
      <Member>00c92bd5-aaa5-468b-a1b0-9353961295da</Member>
      <!--Engineering group with editing rights-->
      <Member>3afc37c3-8ce6-49c4-97c3-77cd6e5b48da</Member>
    </Cabinet>
    <Folder>
      <!--Engineering - all-->
      <Member>ad56465b-73d9-4a4a-ac3d-59c3f23c5c4e</Member>
      <!--Alternatively uncomment this node to make folders inherit members
from cabinet-->
      <!--<Inherit />-->
    </Folder>
  </AutoFilingScript>
  <AutoFilingScript>
    <Name>SchemaName-Date-Based</Name>
    <Cabinet>
      <!--Basie McMarvin-->
      <Member>3afc37c3-8ce6-49c4-97c3-77cd6e5b48da</Member>
    </Cabinet>
    <Folder>
      <!--Sabine Marie-->
      <Member>d4290ff8-033e-4948-b4ed-05b6db1a337</Member>
      <!--Alternatively uncomment this node to make folders inherit members
from cabinet-->
      <!--<Inherit />-->
    </Folder>
  </AutoFilingScript>
  <AutoFilingScript>
    <Name>FilePathFromMD</Name>
    <!--Autofiling Destination location -->
    <MD_FieldName>AutofilingLocation</MD_FieldName>
    <!-- Enter single character used as separator of location parts -->
    <Separator>/</Separator>
    <Cabinet>
      <!--Library Admin-->
```

```
<Member>dd8d3baf-2c55-4f03-8e22-b511610c8a75</Member>
</Cabinet>
<Folder>
  <!--Document Publishers-->
  <Member>c2682088-d20e-4ef5-8603-c314ba5af238</Member>
  <!--Alternatively uncomment this node to make folders inherit members
from cabinet-->
  <!--<Inherit />-->
</Folder>
</AutoFilingScript>
</AutoFilingScripts>
```

APPENDIX B: DOCUMENT VIEWER SUPPORTED FILE FORMATS

Enterprise Office Viewer

Neutral Formats

Portable Document Format	PDF
Content Sealed Format	CSF
Tagged Image Format	TIFF/TIF

Imaging Formats (additional formats available*)

CALS (Group IV)	CAL, CG4, GP4, MIL
EDCARS	EDC
GIF	GIF
ISO 8613/CALS	ISO, CAL
JPEG Compressed Image	JPG, JPEG, JP2
Portable Network Graphic	PNG
Tagged Image File	TIF, TIFF
Windows Bitmap	BMP

Additional Document and Image Formats*

Corel Draw	CDR
Corel Presentations	SHW
DataBase Formats	DBF
DocuWorks	XDW
FAX CITT Group 3 Fax	FAX
Hangul Word Processor	HWP
Hyper Text Markup Language	HTML, HTM
Microsoft Email	MSG
Microsoft Excel	XLS, XLSX, XLSM, XLSB, XLTX, XLTMXLS
Microsoft PowerPoint	PPS, PPT, PPTX, PPTM, PPSX, PPSM, POTX, POTM
Microsoft Visio	VSD, VST, VDX, VSX, VTX
Microsoft Word	DOC, DOCX, DOCM, DOTX, DOTM
Microsoft Works	WDB, WPS, DOCX, XLSX
PageMaker	P65
QuattroPro	WB1, WB2, WQ1
Rich Text Format	RTF

Samna Word	SAM
Windows Write	WRI
WordPerfect	WP5, WP6, WPD, WPF
WordStar	WS

Enterprise Office Document View with CAD Support

AutoCAD Drawing (2D) (through version 2014)	DWG
AutoCAD DXF (through version 2014)	DXF
AutoCAD Web Format (through version 2014)	DWF

Enterprise Office Document Viewer – Engineering Edition

000 HPGL Plot File	000
906/907 Plot File	906/907
Auto-trol Raster	DX
Auto-trol Vector	DG
CADKEY	PRT
CAD Overlay	RLC
Computer Graphics Metafile	CGM
GTX Group III, IV	G3, G4, CG4
GTX Runlength	RNL
HP CAD ME10 (through version 13)	CMI, MI
HPGL Plot File	PLT
IGES (2D) (version 5.2)	IGS, IGES
Inventor (2D) (versions 5.3 - 2013) **	IDW
MicroStation Drawing (through version 8.11, including XM, V8i)	DGN
MicroStation Group IV	CIT
MicroStation Runlength	RLE
MYRIAD 3D View Sets	MVS
OrCad (version 10)	DSN
Solid Edge Drawings (2D) (versions 8 - ST5)	DFT
SolidWorks Drawings (2D) (versions 97 - 20011)	SLDDRW

*Some formats may require additional purchase

**Requires Free Inventor View

INDEX

- A**
- audit log
 - library administrator, 81
 - auto-filing, 23, 50, 61
 - autofilingmembership.xml file, 107
 - configuring xml file, 106
 - date-based, 50
 - enabling, 51
 - filepathfrommd, 50
 - fixed destination, 50
 - GUIDS, 106
 - schemaname-datebased, 51
 - setting, 51
 - Auto-Tagging, 16
- C**
- cabinet administrator role, 13
 - Cabinets
 - cloning, 18
 - copying, 17
 - creating, 14
 - deleting, 17
 - managing, 14
 - properties, 17
 - change cabinet/folder owner, 79
 - change document owner, 78
 - check in for user, 78
 - custom file naming, 47
 - custom file naming
 - setting, 48
 - custom naming, 23
- D**
- database lookup, 56
 - deleting
 - documents permanently, 60
 - document control fields
 - creating, 27
 - enabling, 27
 - document control numbers, 25, 27
 - document publisher + delete role, 12
 - document publisher role, 11
 - Document Schemas, 3
 - document usage log, 80
 - document viewer. *See* viewer
 - documents
 - permanently deleting, 60
 - Drawers
 - cloning, 20
 - copying, 19
 - creating, 18
 - deleting, 21
 - managing, 18
 - moving, 19
 - properties, 19
- E**
- electronic documents, 23
 - electronic records, 23
 - email attachments
 - settings, 60
 - email notifications
 - settings, 61
 - event schedule, 23, 51
 - adding to schemas, 56
 - archive, 51
 - convert to record, 52
 - creating, 54
 - delete, 52
 - email notifications, 53
 - enabling, 54
 - using custom metadata fields, 53
 - extraction rules, 92
 - email, 92
 - file properties, 93
 - Outlook, 92
 - PDF forms, 103
 - XML node, 96
- F**
- FileHold Library. *See* Library
 - FileHold Security, 5
 - folder groups
 - delete, 22
 - edit, 22
 - Folder Groups
 - assigning to a folder, 22
 - managing, 21
 - Folders
 - managing, 22
- G**
- guest user role, 11
- H**
- hard delete, 60
- L**
- Library
 - best practices, 6

- creating, 6
- creating the structure, 14
- general settings, 60
- overview, 6
- planning template, 6
- utilities. *See* utilities

Library Administrator

- security role, 1
- tasks, 1

library administrator role, 13

library audit log, 81

log in, 2

M

manage imports tool, 88

- importing files previously exported from FileHold, 90
- QuickScan Pro, 88

metadata, 23

- adding to schemas, 35
- checkbox field, 32
- creating, 30
- currency field, 31
- date field, 31
- drill down menu, 32
- drill drop down menu field, 31
- drop down menu, 33
- drop down menu - database lookup field, 31
- drop down menu-FileHold managed field, 31
- editing, 36
- importance, 29
- number field, 31
- text field, 30
- URL field, 32

O

offline documents, 24

- version 0 switch, 25

organizer + delete role, 12

organizer role, 12

P

publisher + delete role, 12

publisher role, 12

R

read-only role, 11

recover documents, 80

reporting services, 85

- report security, 87
- reports, 86

restricting access

- FileHold, 61

S

Schema membership, 23

schemas

- database lookup. *See* database lookup

Schemas, 23

- adding groups or users, 28
- adding workflows, 46
- creating, 23, 24
- metadata. *See* metadata
- offline documents, 24

search engine

- configuring, 66
- errors, 70
- rebuilding full-text search index, 68
- settings, 66
- status, 68
- unindexed files, 69

security

- problems, 5
- senior library administrator role, 13
- soft delete, 60
- system administrator role, 14

U

user roles, 11

utilities

- change cabinet/folder owner, 79
- change document owner, 78
- check in for user, 78
- document usage log, 80
- recover documents, 80

V

version control fields

- creating, 27
- enabling, 27

version control numbers, 25, 26

viewer

- Brava viewer, 62
- configuring, 62
- PDF/Image viewer, 62
- supported formats, 111

W

workflow, 23

- actions on status reports, 75
- adding to schemas, 46
- ad-hoc workflows, 37
- approvers, 37
- automatically starting, 46
- configuring, 36
- creating status reports, 74
- creating templates, 41
- dashboard, 76

diagram, 39, 40
editing templates, 47
examples, 38
initiator, 37
observers, 37

participants, 37
reviewers, 37
templates, 76
viewing templates list, 76
workflow status report, 73