



FileHold

Document & Record Lifecycle Software

SYSTEM 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 <http://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 support@filehold.com.

TABLE OF CONTENTS

1. OVERVIEW	1
1.1. SKILLS REQUIRED TO ADMINISTER THE SYSTEM	1
1.2. RESPONSIBILITIES OF THE SYSTEM ADMINISTRATOR.....	2
1.3. SETTING UP FILEHOLD SECURITY	3
2. LOG IN	3
3. SETTING UP USERS AND GROUPS	4
3.1. OVERVIEW	6
3.2. MANAGING ACCESS TO THE SYSTEM	6
3.3. CREATING LOCALLY MANAGED USERS	7
3.4. SYNCHRONIZING MICROSOFT ACTIVE DIRECTORY) USERS AND GROUPS (DOMAIN).....	9
3.4.1. ADDING A DOMAIN USER / GROUP TO FILEHOLD	10
3.5. CREATING FILEHOLD GROUPS.....	11
3.5.1. USER ROLES AND ACCESSING THE LIBRARY	12
3.6. ADDING USERS TO GROUPS	15
3.7. VIEWING USER PROPERTIES	18
3.8. VIEWING GROUP PROPERTIES.....	18
3.9. SEARCHING FOR USERS.....	19
3.10. DELETING USERS.....	19
3.11. DELETING GROUPS	20
3.12. GUARANTEED USER ACCESS	20
3.13. RESET USER PASSWORD	21
3.14. SET VIEWER LICENSE.....	22
3.15. ENABLING AND DISABLING ACCOUNTS	23
4. LOGON AND PASSWORD SECURITY	24
5. USER SELF-REGISTRATION.....	25
6. GLOBAL SETTINGS.....	26
6.1. SETTING THE DEFAULT DOMAIN.....	26
6.2. REMOVING LICENSES FROM DISABLED USERS IN THE DOMAIN.....	26
6.3. SETTING OUTBOUND EMAIL SETTINGS.....	27
6.4. ENABLING THE DOCUMENT AND VERSION CONTROL FIELDS.....	28
6.5. DOCUMENT SHORTCUTS.....	28
6.6. SETTING THE PERMISSION SETTINGS	28
6.7. EVENT SCHEDULE SETTINGS.....	30

6.8. INSUFFICIENT CAL NOTIFICATION SETTINGS	30
6.8.1. INSUFFICIENT CAL LOG.....	31
6.9. CENTRALIZED OPTIONS MANAGEMENT.....	31
6.10. SERVER SIDE OCR	31
7. REPOSITORY LOCATIONS	33
8. LICENSING	34
8.1. LICENSE EXPIRATION GRACE PERIOD	36
9. ACTIVITY LOG	36
10. SYSTEM AUDIT LOG	37
11. CENTRALIZED OPTIONS MANAGEMENT.....	37
11.1. ALERT PREFERENCES	37
11.2. WORKFLOW PREFERENCES.....	39
11.3. FASTFIND PREFERENCES	40
11.4. MISCELLANEOUS PREFERENCES.....	41
11.5. FDA ADVANCED SETTINGS.....	42
11.6. ADVANCED SEARCH OPTIONS	44

1. OVERVIEW

System Administrators have full control over the entire document management system. The System Administrator needs to have an understanding of not just the technical systems but also how the organization is structured so that they are able to set up system functionality and content for the various users, teams, groups, departments or other groups that may need to access the files. Optional qualifications for this role would include knowledge of Microsoft technologies like Active Directory.

The System Administrator provides for the creation and management of user groups, system permissions, individual user accounts, system security settings, as well as the management of the optional synchronization with Active Directory. This is in contrast to the Library Administrators who define and manage the files that are stored in document management system.

NOTE: The System Administrator may be the same person as the Library Administrator; however, we recommend that more than one individual take on these roles in order to cover vacations or other leaves of absences.

This guide describes the steps required to use the System Administration area of FileHold including:

- [Log in](#)
- Set up [locally managed](#) and [domain users](#)
- Set up [groups](#)
- Manage [logon and password security](#)
- Set up [user self-registration](#)
- Configure the [global settings](#)
- Manage [FileHold licenses](#)
- View logs and [activity reports](#)
- [Manage centralized options](#)

1.1. SKILLS REQUIRED TO ADMINISTER THE SYSTEM

Administering FileHold is not complex. The system is designed to be administered by fairly non-technical users who have a firm understanding of how their organization requires documents, records and other important files to be stored, organized, categorized and protected from unauthorized access.

A member of the IT team is often the System Administrator and provides IT expertise to assist the Library Administrator configure the document management system as well as more specific tasks such as synchronizing Active Directory users, the creation of managed users, and defining roles and groups.

It is important for System Administrators to understand their role and work together with the Library Administrator to organize the document management system so that users can find, search, browse for, update, and manage their files in an efficient and straightforward manner.

1.2. RESPONSIBILITIES OF THE SYSTEM ADMINISTRATOR

System Administrators create the roles, groups and security settings that define the system in terms of permissions, access, and user rights. Library Administrators use these foundational settings to build the file structure and document categorization system that provides users with highly configurable schemas for different types of documents.

In other words, Systems Administrators take care of the system security and provision users while Library Administrators are responsible for the management and security of the content held in the document management system.

In order to effectively accomplish this, the System Administrator should:

- Understand the document management system's System Administration by reading the System Administration guide and [Knowledge Base](#).
- Work with the Library Administrators on the creation of groups and permissions and roles these groups are assigned. Keep things simple at first. Remember it is easier to give users the minimum role required rather than retracting permissions in the future.

NOTE: The System Administrator may be the same person as the Library Administrator; however, we recommend that several trusted individuals take on these roles in order to cover vacations or other leaves of absences.

- Examine the list of users / employees that will be accessing the document management system, group these users into logical groups, and provide a descriptive name for the groups. A descriptive group name will make more sense to you or to other administrators months or years from now when they are adding new users or thinking of creating new groups.
- Security considerations:
 - What level of access (permissions) do the various groups need?
 - What roles do the various groups need to do their work in the system?
 - Are there places in the file structure that require a group to have their normal access restricted?

In some organizations (especially larger ones) there may be a desire or requirement to have different individuals acting as System and Library Administrators. In this case the IT group will be responsible for System Administration, while a separate group from either the records management department, information department or some other central department spearheads Library Administration management.

System Administrators create and manage user accounts and therefore controls who gets access to the document management system. FileHold supports two types of user accounts:

- Locally Managed User Accounts — User accounts (that are added directly to the document management system and are independent of any type of directory server (including Active Directory))
- Domain User Accounts — User accounts that are synchronized with a Microsoft Active Directory. These accounts definitely require the support of the organizations IT department

System Administrators also create user groups which are typically users that work together and require a specific type of access permission (role) in the Library. These groups are then used by the Library Administrator for both system permissions and membership of the cabinet, folder, and schema level.

1.3. SETTING UP FILEHOLD SECURITY

You will need to evaluate the users of the system and group them into logical groups, such as Accounting, Marketing, Sales, and so on. You will also need to decide what level of access that each group requires and assign the appropriate role to the group. For the list of security roles, see [User Roles and Accessing the Library](#).

FileHold has three levels of security:

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

Once you have created the users and groups in the system, the Library Administrator can apply group membership to the cabinets, folders, and schemas. This allows users to use the documents they need and restrict them from the ones they don't need access.

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. For more information on cabinets, folders, and schemas, see the [Library Administration Guide](#).

2. LOG IN

You can perform System Administration functions in both the FileHold Desktop Application (FDA) and the Web Client. The FDA has very limited System Administration functions whereas you can access all System Administration functions through the Web Client.

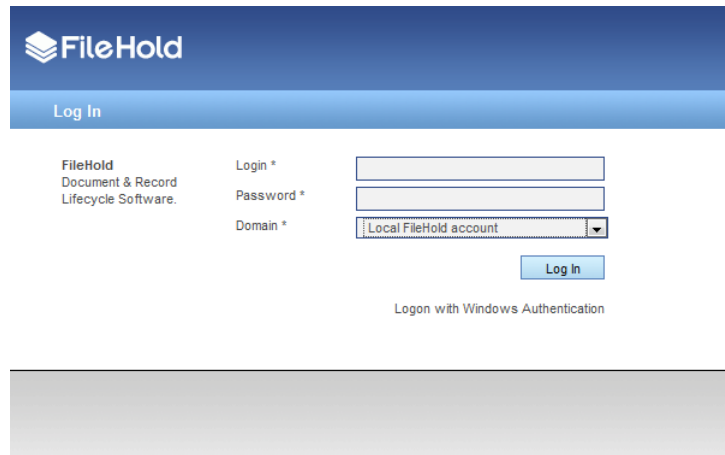
The System Administration features in FDA include:

- Users
- FileHold Groups

You will need to log in through the Web Client in order to gain access to all other System Administrator functions. All of the administration functions in FDA are performed almost exactly as they are in the Web Client.

TO LOGIN TO SYSTEM ADMINISTRATOR VIA THE WEB CLIENT

1. Open a Web Browser and enter the path to the FileHold server. This may be set up as link on your desktop or from the FileHold Desktop Application (FDA) by selecting [Administration > System Administration](#) from the menu bar.



The image shows the FileHold login page. At the top left is the FileHold logo. Below it is a blue bar with the text 'Log In'. The main content area contains the following fields and text:

FileHold
Document & Record
Lifecycle Software.

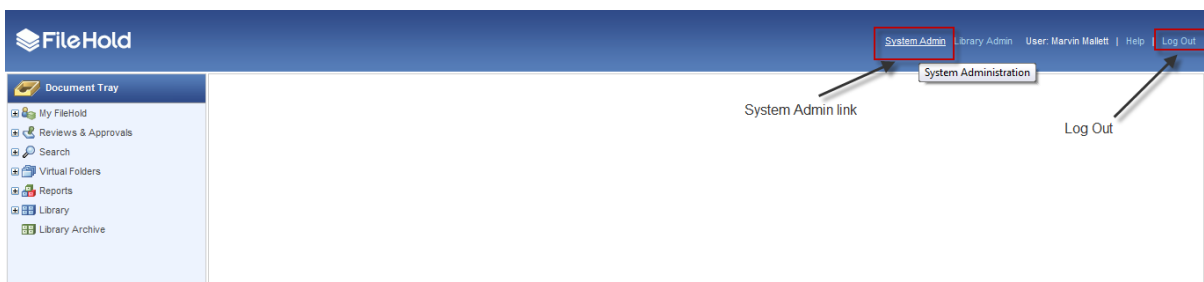
Login *

Password *

Domain *

Logon with Windows Authentication

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



Once logged in, the different areas of the system administration features will appear in the left sidebar menu.

NOTE: This System Administration section is only available to users designated as System Administrators. Non-administrator users will not see the link to the administration section.

TO LOG OUT FROM THE WEB CLIENT

1. Click **Log Out** in the top right hand of the screen.

TO LOGIN AS SYSTEM ADMINISTRATOR VIA THE FDA

1. Log into FDA using a System Administrator username and password.
2. Go to **Administration > System Administration** from the menu bar.

TO LOG OUT FROM THE FDA

1. Go to **File > Exit**.

3. SETTING UP USERS AND GROUPS

System Administrators are responsible for the setting up and configuring of the FileHold users and group memberships. They create the roles, groups and security settings that define the document management system in terms of permissions, access and user rights. Library

Administrators use these foundational settings to build the file structure and document categorization system that provides users with highly configurable schemas for different types of document.

The System Administrator should:

- Design and map out the user groups and permissions on a whiteboard or a spreadsheet. It is recommended that everything be considered up front before configuring the system.
- Create groups and assign permissions (roles) for each group.
- Create users or import users from active directory (if required).
- Assign users to groups.
- Document your planning work. It is suggested that you save this work to a folder restricted to administrator access within FileHold.

Here is an example of how you can set up a spreadsheet that contains all of the user groups and roles for your organization.

User Groups		
FileHold Group	Membership	Role
Call Center Team	Entire call center team	Document Publisher
Collections Team	Entire collections team	Document Publisher
Contracts	Entire Contracts Team	Document Publisher
HR (doc pubs)	HR team except for HR Director and HR Manager	Document Publisher
HR (admins)	HR Director and HR Manager	Library Administrator
IT Team	Entire IT team	System Administrators
Library Administrators	FileHold operations team. It might be desirable to setup library administrators for each operations team.	Senior Library Administrator
Risk Team - Admins	Entire risk team	Library Administrator
Risk Team - Read Only	Entire risk team	Document Publisher
Sales and Marketing Team	Entire sales and marketing operations team. Does not include F & I, area, or regional F & I managers.	Read Only
Settlement Team	Entire settlement team	Document Publisher
System Administrators	FileHold operations team	Document Publisher

WARNING: Systems Administrators should be very careful about which users/groups will receive delete permissions. Remember that it is easier to mark or flag files for deletion than it is to recover and restore them from the IT Enterprise backup system.

3.1. OVERVIEW

FileHold has multiple ways of ensuring user authentication and authorization of resources:

- Authentication identifies a user based on username and password.
- Authorization uses the authentication information to grant the appropriate level of access control to the content and other tools.

Granular roles-based security allows the System Administrator to quickly control the exact level of access a group of users will have to FileHold. For example, a group of users may be restricted to 'Read Only' access for one type of file yet have full access to another document type. Security can be configured at multiple levels so documents can even be stored in the same folder yet carry differing permissions of access.

There are two types of user accounts: Locally Managed Users and Active Directory Synchronized Users. Both types of accounts can co-exist on the same FileHold Server.

- A locally managed user is an account that does not authenticate or synchronize against Microsoft Active Directory systems. This allows System Administrators to setup and manage users without involving complex IT deployment scenarios. This is suited for a non-technical System Administrator in a smaller organizational environment. The FileHold Locally Managed User account leverages two Microsoft based components for application developers called AzMan (Authorization Manager) and ADAM. (Active Directory Application Mode). These components provide security and standard management functionality without needing to authenticate or synchronize against Active Directory.

Administrators can quickly create user accounts in mere minutes OR activate [user self-registration](#).

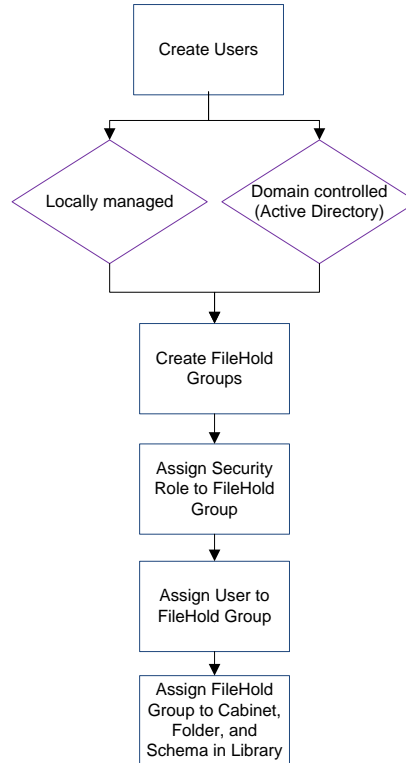
- Microsoft Active Directory Synchronized Users are users that called FileHold Domain Users. Groups synchronized with Microsoft Active Directory are called FileHold Domain Groups. The users and groups behave the same way as locally managed users when interacting FileHold. The difference is that the properties (contact information, passwords etc.) associated with domain user/groups are managed externally in Active Directory and not through the user properties of the document management system.

3.2. MANAGING ACCESS TO THE SYSTEM

Users are placed within FileHold Groups. FileHold Groups are created by System Administrators and given a specific name and permissions (roles) to system functionality. Roles give users specific functionality throughout the system, however, groups can have their roles restricted at the cabinet and folder levels.

Groups and users are given access via membership to FileHold cabinets, folders and schemas. These permissions provide control down to the document level. The degree of access users have to content is determined by their role.

The following flowchart depicts how security is set up in the system.



3.3. CREATING LOCALLY MANAGED USERS

A locally managed user is a user account that is created and managed directly in FileHold.

This is in contrast to a domain user. A domain user is a user account obtained through synchronization of FileHold with a Microsoft Active Directory server. For more information on domain users, see [Synchronizing Domain \(Active Directory\) Users and Groups](#).

In the FileHold user list, other than the list of users, you can see the number of registered users, the number of concurrent sessions, the number of Insufficient CALs events in the last 24 hours, the number of viewer licenses (if purchased), the number guest user licenses (if purchased), and the number of Microsoft SharePoint sessions (if purchased). You can also view the number of enabled, remaining, and total number of licenses, the number of guaranteed and shared sessions, the number of assigned and remaining viewer licenses, and the available number of Guest User and Microsoft SharePoint sessions.

A registered user is someone who has a FileHold account that is registered and can access the system if the account is enabled. Concurrent sessions are the total number of people allowed to use FileHold at the same time. For example, you may have purchased 250 registered user licenses and 100 concurrent sessions. This means that only 100 out of the 250 registered users can log into FileHold at the same time.

The screenshot shows the 'Users Management' window with a 'List of all FileHold users' header. A red arrow points to the alphabetical filter letters (A-Z) with the text 'Click on letter to filter by last name'. Below this is a 'License summary area' with a table of license usage. At the bottom is a 'List of registered users' table.

Name	FileHold Account	Guaranteed Access	Viewer License	Scanning Inbox License	Source	FileHold Group
<input type="checkbox"/> Library Admin	Enabled	Yes	No Viewer	No	Locally managed...	Library Administr...
<input type="checkbox"/> alfonso AND	Enabled	Yes	No Viewer	No	Locally managed...	
<input type="checkbox"/> alfonso basic user	Enabled	No	No Viewer	No	Locally managed...	
<input type="checkbox"/> Pub Delete	Enabled	No	No Viewer	No	Locally managed...	
<input type="checkbox"/> Deborah Dixon	Enabled	No	No Viewer	No	Locally managed...	Cabinet Administr...
<input type="checkbox"/> Boris Godunov	Enabled	No	No Viewer	No	Locally managed...	
<input type="checkbox"/> User Guest2	Enabled	No	No Viewer	No	Locally managed...	
<input type="checkbox"/> Alfonso Ipad	Enabled	Yes	No Viewer	No	Locally managed...	
<input type="checkbox"/> Senior Libadmin	Enabled	Yes	No Viewer	No	Locally managed...	
<input type="checkbox"/> Puh Iisher	Fnahler!	Yes	Nn Viewer	Nn	Locally managed...	

TO CREATE A LOCALLY MANAGED USER

- In the Web client, log into System Admin and select **User and Group Management > Users**.
 - Alternatively, in FDA, log in with System Administrator rights and go to **Administration > User & Group Management > Users**.
- Click **Add Users**.
- Select **Locally Managed User** and click **Next**.
- Fill in the following information and click **OK**:
 - First Name
 - Last Name
 - User Logon Name
 - Email
 - Default Language
 - Source — Locally managed user account
 - Initials

The screenshot shows the 'Add Locally Managed User' form. The 'General' tab is active, showing the following fields:

- First Name *: Deborah
- Last Name *: Dixon
- User Logon Name *: ddixon
- E-mail *: ddixon@filehold.com
- Default Language: English (dropdown menu)
- Source: This is a locally managed user account.
- Initials: DD

Buttons for 'OK' and 'Cancel' are visible at the bottom right.

- Enter the password for the user twice and click **OK**.

6. Select **Account Settings** and enter the following information under FileHold Account Options:
 - FileHold account is enabled for this user — Select this check box if the user account should be enabled.
 - User has guaranteed system access — Select this check box if the user should have access to the system at all times. See [Access](#) for more information.
 - User must change password at next logon — Select this option if the user is to set their own password the next time they log into the system. This option is recommended.
7. In the FileHold Desktop Application Viewer Options area, select the viewer license (if purchased) for the user. For detailed information about the viewers, see the [FileHold Knowledge Base](#).
 - A viewer is not licensed for this user.
 - PDF/Image Viewer
 - Enterprise Office Viewer (includes PDF/Image Viewer)
 - Enterprise Office Viewer with CAD Support (includes PDF/Image Viewer)
 - Enterprise Office Viewer (Engineering Edition)(includes PDF/Image Viewer)
8. In the FileHold Scanning Inbox License area, select the **Scanning Inbox License Assigned** check box if the user is to be assigned a WebCap scanning license. For more information about WebCap, see the [Knowledge Base](#).
9. In the Account Expiration area, select a date for the user account to expire or leave the default **Never** for the account to remain active indefinitely. An account expiration date is good to use when you have contractors or temporary workers.
10. Click **OK**.
11. In the Member Of window, you will need to add the user to a group. See [Adding Users to Groups](#) for more information.
12. Select Contact Information and enter the user's contact information such as addresses, phone numbers, and company information. This information is optional.
13. Click **OK**. The user is added to the list of registered users.

3.4. SYNCHRONIZING MICROSOFT ACTIVE DIRECTORY) USERS AND GROUPS (DOMAIN)

With the optional Microsoft Active Directory Toolkit, FileHold can synchronize domain users and groups that reside in Active Directory with the FileHold users. The benefits of synchronization of user / group objects with Active Directory include: centralized control of system users, single sign on authentication support, and the ability to quickly rollout new users to FileHold from Active Directory.

Active Directory synchronized users are called FileHold Domain Users within the FileHold system. Groups synchronized with Active Directory are called FileHold Domain Groups. The users and groups behave the same way as locally managed users when interacting FileHold. The difference is that the properties (contact information, passwords etc) associated with domain user/groups are managed externally in Active Directory and not in FileHold.

Domain groups can be assigned to FileHold Groups that can in turn be given access (membership) to specific content located throughout the Library. Synchronization of a domain group will allow a new user added to the domain group at the Active Directory level to be

automatically provisioned to all areas of FileHold based on the pre-defined permissions of their FileHold groups.

NOTE: It is important to keep in mind that some Active Directory deployments can be complex as they employ custom schemas and objects that may not be industry standard and can require additional effort to synchronize.

If you did not purchase the Active Directory option, you will need to create [locally managed users](#). You will not be able to synchronize FileHold with Active Directory. To purchase the Active Directory Toolkit, contact sales@filehold.com. This toolkit includes additional support resources to ensure a successful synchronization.

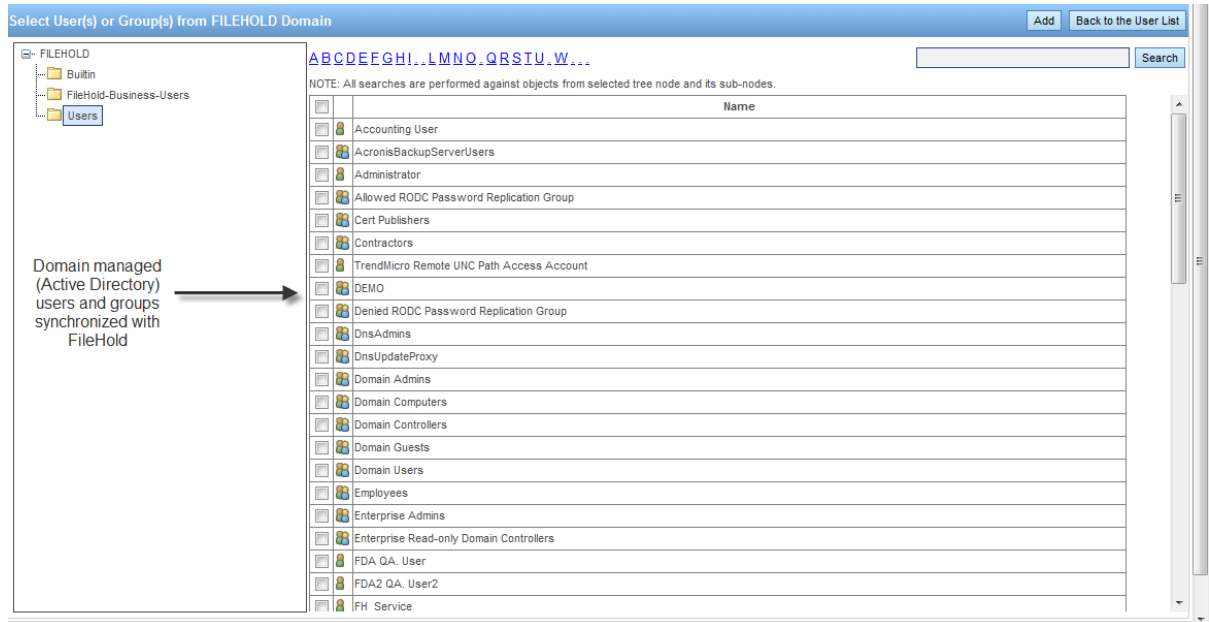
3.4.1. Adding a Domain User / Group to FileHold

Complete the following steps to add a domain-managed (Active Directory) user account to FileHold.

WARNING: You must ensure that FileHold has been successfully synchronized with Microsoft Active Directory prior to completing these steps. If you have purchased the Active Directory module, please contact support@filehold.com to start the process of domain synchronization.

TO ADD A DOMAIN USER OR GROUP TO FILEHOLD

1. In the Web Client, log in to the System Admin section of FileHold and select **User and Group Management > Users**.
 - Alternatively, in FDA, log in with System Administrator rights and go to **Administration > User & Group Management > Users**.
2. Click **Add User(s)**.
3. Select **Add a user(s) or group(s) from a domain/directory server** and select the domain name from the list.
4. Click **Next**.
5. Select the check boxes for the users or groups you want to add and click **Add**.
6. To search for a domain user or group in the list, enter the name in the search field and click **Search**.



7. In the Add Domain Group Options, select one of the following and click **OK**:
 - Add the group and the group members. Keep both synchronized with the domain.
 - Add just the group members and do not add the group. Only the user accounts will still be synchronized with the domain.
8. At the Add User(s) and Group(s) Confirmation, click **OK**.
9. Continue to add more users and groups to FileHold.
10. To return to the user list, click **Back to the User List**.
11. To set viewer, guaranteed access, and scanning inbox (Web Cap) licenses, select Properties next to the user name and go to Account Settings. See [Creating Locally Managed users](#) for more information.

3.5. CREATING FILEHOLD GROUPS

A FileHold Group is a collection of users that share specific membership and permissions for the purposes of providing an appropriate level of access to the system and its functionality.

Groups are created by the System Administrator. It is highly recommended that the Library Administrator help with the planning of FileHold groups since access to the documents via the groups is set by the Library Administrator and not the System Administrator.

Groups are assigned a role from the set list of [user roles](#) in FileHold. In many organizations, groups are associated by department or function within the organization. These groups typically have entire cabinets in the Library for their documents. For more information on assigning group membership to Cabinets, Folders, and Schemas, see the [Library Administration Guide](#).

TO CREATE A FILEHOLD GROUP

1. In the Web Client, log in to the System Admin area and select **User and Group Management > FileHold Groups**.

- Alternatively, in FDA, log in with System Administrator rights and go to **Administration > User & Group Management > FileHold Groups**.
2. Click **Add Group**. The list of FileHold groups that come standard with the product are shown. See the [table below](#) for a list of user roles and descriptions. It is recommended that you create your own groups that are meaningful to your organization, such as Accounting Group, Engineering Group, HR Group, and so on. The standard FileHold groups can be renamed or deleted once your own groups are created.
 3. Enter the following information:
 - Group Name — Enter a name for the group.
 - Description — Enter a description for the group.
 - Role — Select a role from the list. See User Roles and Accessing the Library for descriptions.
 - Notes — Enter any additional information about the group.
 - FileHold Group Members — Select **Display all members on one page** check box to display all the members on a single page. Click **Add Members** to add user to the group. See [Adding Users to Groups](#) for more information.
 - Restrictions — Select the **Disable emailing documents** check box if users will not be able to email documents from FileHold.
 4. Click **OK**. The group is added to the list.

3.5.1. 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 two 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>

Role Name	Description
Read Only	A Read-Only user role may only download or open and read documents from FileHold. They cannot edit, delete, or create documents. They can email documents if given this functionality by System Administrators.
Document Publisher	Document Publisher user role can read, get a copy, add, check-in/check-out, edit documents, and metadata. They can move documents that are owned by them. They cannot delete any documents including those which they have added to the system.
Document 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

Role Name	Description
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>
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. • Move documents between cabinets as long as they are owners of the Cabinet. If users need to move documents between Cabinets that they do not own, then use an organizer role instead. • Have access to all document schemas. • Change document owner for documents in the cabinets that they own. • Convert electronic documents to electronic records and vice versa for cabinets that they own. • Convert electronic documents to offline documents for cabinets that they own. • Manually move document to and from the library archive as long as they are the Cabinet owner in the library archive.
Library Administration	<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.

Role Name	Description
Senior Library Administration	Senior Library Administrators have full control of the FileHold library itself and Library Administration area. Senior Library Administrators can create cabinets to be managed by any Library Administrator or Cabinet Administrator.
System 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.

3.6. ADDING USERS TO GROUPS

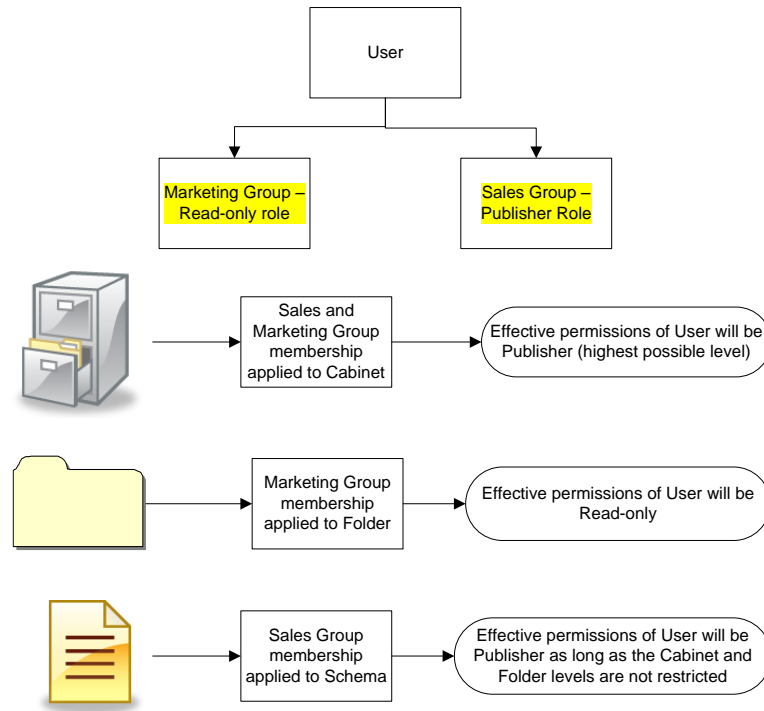
Once the users are in the system, you can add them to FileHold groups. Users can be assigned to an unlimited number of groups and groups can contain one or more users.

It is recommended that users access the Library as a member of a group instead of an individual user. This makes it easier to control access and maintain security. For example, you should add groups to Cabinet, Folder, and Schema memberships instead of users because it is easier to add and remove users from groups than it is to locate the Cabinets, Folders, and Schemas of individual users.

There are several ways that users can be added to groups:

- [Selecting a user from the User list and clicking Add to FileHold Group.](#)
- [Selecting a user from the Users list and selecting Properties > Member of.](#)
- [Selecting a group from the FileHold Group list and selecting Add Members.](#)
- [Selecting a group from the FileHold Group list and selecting Properties > Add Members.](#)

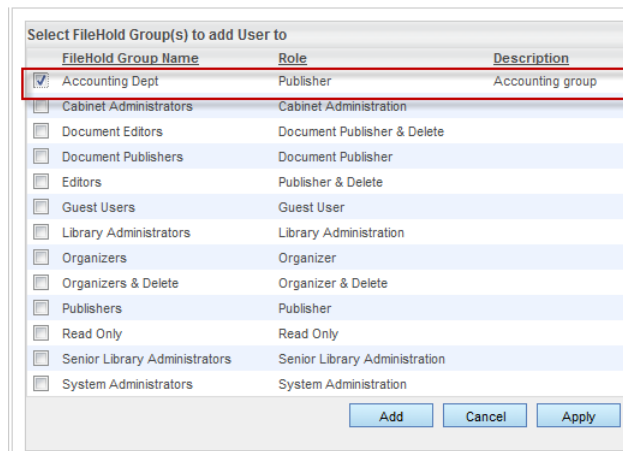
When users belong to more than one FileHold group they will inherit the access level of the highest group of which they are a member. For example if a user is assigned to the Marketing group (associated with a read-only role) and the Sales group (associated with the publisher role) they will have full publisher rights if both groups are assigned to a cabinet, folder, or schema. If only the Marketing group is assigned to a folder, then the user will have only read-only rights. If only the Sales group is assigned to folder, then the user will have publisher rights. See the diagram below.



NOTE: The Library Administrator can restrict access to these users at the folder or schema level in order to preserve the security of the system.

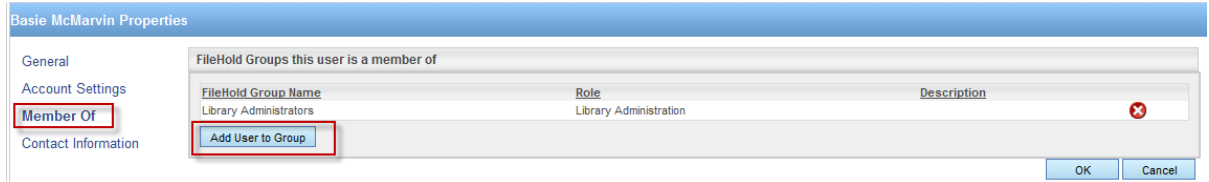
To ADD A USER TO A GROUP FROM THE USER LIST USING ADD TO FILEHOLD GROUP BUTTON

1. In the System Admin area, go to **User and Group Management > Users** and select the check box of one or more user names.
2. Click **Add to FileHold Group**.
3. Select the check box of the group you want to add the user(s) to and click **Add**. The user is now a part of the group.



TO ADD A USER TO A GROUP FROM THE USER LIST USING THE USER PROPERTIES

1. In the System Administration area, go to **User and Group Management > Users** and select properties from the drop-down menu on a user name.
2. In the User Properties, click **Member Of**.
3. In the FileHold Groups this user is a member of list, click **Add User to Group**.



4. Select the check box of the group you want to add the user(s) to and click **Add**. The user is now a part of the group.

TO ADD USERS TO A GROUP FROM THE GROUP LIST

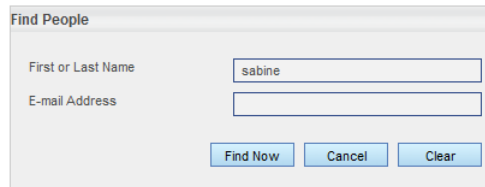
1. In the Web Client, in the System Administration area, go to **User and Group Management > FileHold Groups** and select **Add Members** from the drop-down menu on the group name.



2. In the Find People window, enter the first or last name of the user and/or the email address and click **Find Now**.
3. In the Results of People Search area, select the check box next to the user name(s) and click **Select User(s)**. The user is added to the group.

TO ADD USERS TO GROUP USING THE GROUP PROPERTIES

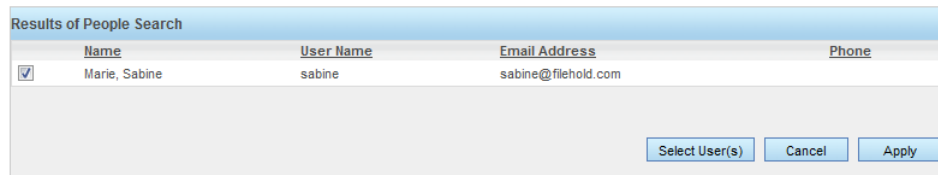
1. In the System Administration area, go to **User and Group Management > FileHold Groups** and select **Properties** from the drop-down menu on the group name.
 2. Alternatively, in FDA, log in with System Administrator rights and go to **Administration > User & Group Management > FileHold Groups**. Click on the Group Name and click **Add Members**.
3. In the FileHold Group Members area, click **Add Members**.
4. In the Find People window, enter the first or last name of the user and/or the email address and click **Find Now**.
5. In the Results of People Search area, select the check box next to the user name(s) and click **Select User(s)**. The user is added to the group.



Find People

First or Last Name

E-mail Address



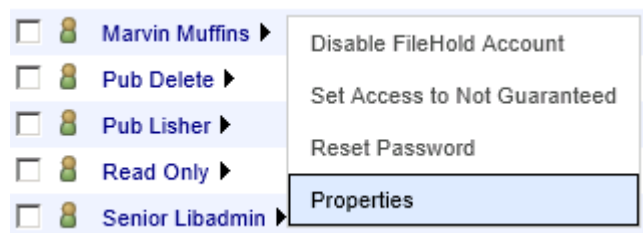
Results of People Search				
	Name	User Name	Email Address	Phone
<input checked="" type="checkbox"/>	Marie, Sabine	sabine	sabine@filehold.com	

3.7. VIEWING USER PROPERTIES

You can view and edit user properties such as email addresses, account settings, group membership, and contact information.

TO VIEW USER PROPERTIES

- In the System Administration area, go to **User and Group Management > Users** and click on a user name.
 - Alternatively, in the Web Client, you can select **Properties** from the context-sensitive menu next to the user name. Click on the arrow ► next to the user name for the context sensitive menu to appear.



- Update or view the General, Account Settings, Member Of, or Contact Information for the user and click **OK**.

3.8. VIEWING GROUP PROPERTIES

You can view and edit group properties such as the group name, role, and group members.

TO VIEW GROUP PROPERTIES

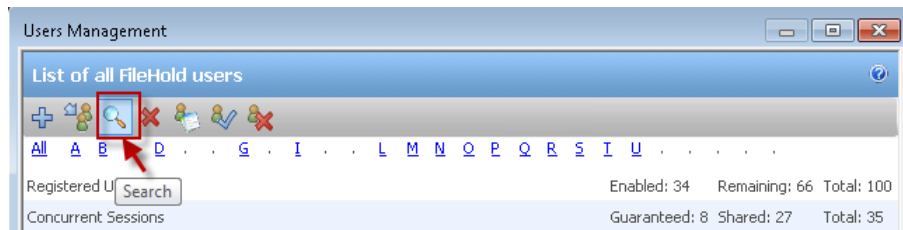
- In the System Administration area, go to **User and Group Management > FileHold Groups** and click on a group name.
 - Alternatively, in the Web Client, select **Properties** from the context-sensitive menu next to the group name. Click on the arrow ► next to the group name for the context sensitive menu to appear...
- Update or view the group name, description, role, notes, group members and restrictions for the user and click **OK**.

3.9. SEARCHING FOR USERS

You can search for users by first or last name, or by email. After you have found the user you are searching for, you can modify their properties, group membership, licenses, and accounts.

TO SEARCH FOR A USER

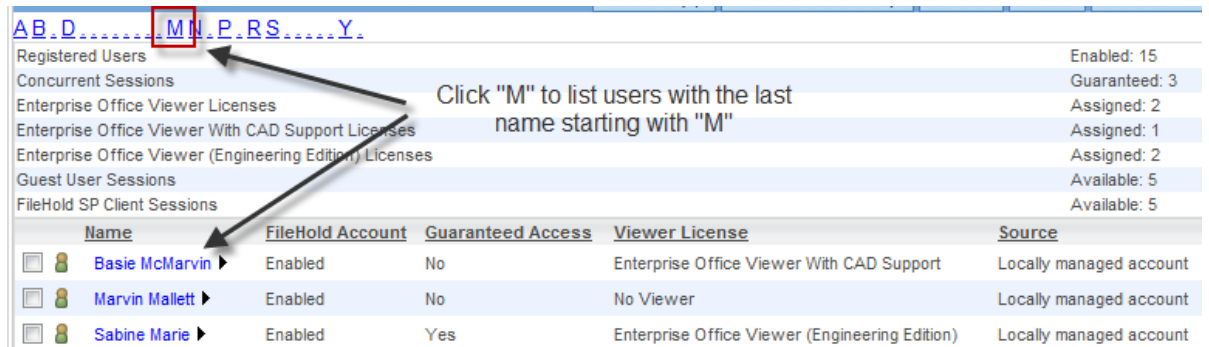
1. In System Administration area in both the Web Client and FDA, go to **User and Group Management > Users** and click **Search**.



2. In the Find People window, enter the first name, last name or email address of the person you are searching for and click **Find Now**.
3. From the Search Results window, you can now modify the user account.

TO SEARCH BY LAST NAME

1. In the System Admin area of both the Web Client and FDA, go to **User and Group Management > Users** and click on a letter in the alphabet at the top of the screen. The list of users with the last name starting with that letter is shown.



3.10. DELETING USERS

Deleting a user from the system removes any ownership of the deleted user's documents, folders or cabinet ownership. It is recommended to not delete a user if you wish to maintain the account in case the user ever will need access to FileHold again. Instead, you should [disable](#) a user account. This way the account can be re-enabled in the future. The actual user account is never deleted - the user name is internally represented by a GUID that exists perpetually in the system.

Deleting a user action cannot be undone.

If you must delete the user account, be sure to use the Change Document Owner and Change Cabinet/Folder Owner features in the Library Administration area to give the cabinets, folders, and documents a new owner. See the [Library Administration Guide](#) for more information.

NOTE: The actual user account is never deleted - the user name is internally represented by a GUID that lives forever. Before deleting a user, we suggest you change the last name of the user to indicate the user is deleted. This way, if a user with the same name is added in the future, there will be no confusion in the document usage log. For example, if you will delete the user John Smith, change the last name to Smith(deleted20130820) before deleting it. The name displayed in the usage log will clearly distinguish between the old and the new John Smith.

TO DELETE A USER ACCOUNT

1. Go to **User and Group Management > Users** and select the check box for user account you want to delete. You can use the [Search](#) feature to find a user.
2. Click **Delete**.
3. You will receive a warning message that you are about to delete a user. Click **OK** to delete the user. The user account is removed from the list of FileHold users.

3.11. DELETING GROUPS

Deleting a group will delete the group from all cabinet, folder, and document schema memberships. This action cannot be undone.

TO DELETE A GROUP

1. Go to **User and Group Management > FileHold Groups**
2. In the Web Client, click the arrow ► next to the group name and select **Delete**.
 - Alternatively, in FDA, right-click on the group name and select **Delete**.
3. You will receive a warning message about deleting the group. Click **OK** to delete the group.

3.12. GUARANTEED USER ACCESS

A guaranteed user has guaranteed access to FileHold regardless of how many other users are logged onto the system. Normally, a user can only connect when a concurrent user license is available. This setting is usually reserved for users like library administrators that frequently access the server.

For example, a company with 40 total (named) users and 20 concurrent licenses means that all 40 people share the same pool of 20 concurrent connections. If two of the named users are given guaranteed access then they will each have a dedicated concurrent license ensuring they always be able to get into the document management system. This means that the other 38 named users now draw from a pool of 18 concurrent user licenses.

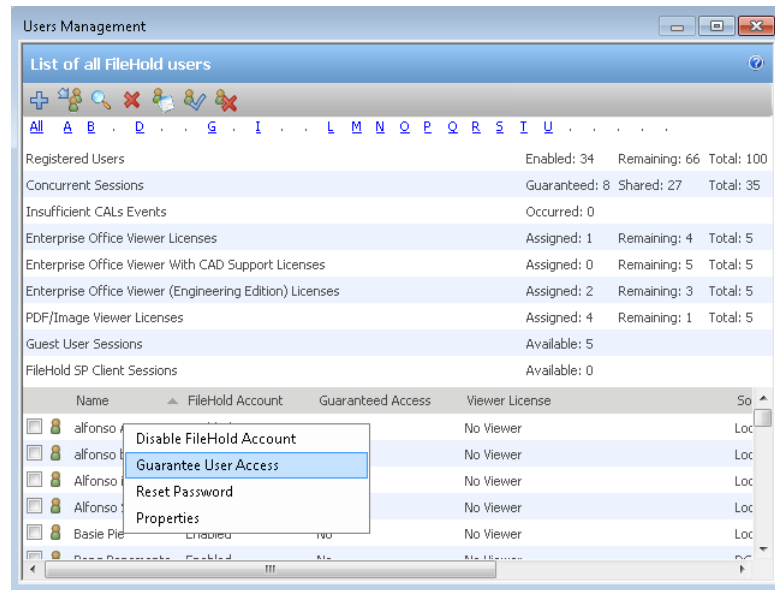
TO GUARANTEE A USER ACCOUNT

1. In the Web Client, go to **User and Group Management > Users** and click the ► next to the user name.
 - In FDA, go to **Administration > User and Group Management > Users**.
2. Select **Guarantee User Access**. The Guaranteed Access status is now set to Yes.

Name	FileHold Account	Guaranteed Access
Administrator ▶	Enabled	No
Basie McMarvin ▶	Enabled	No
Cabinet Administrator ▶	Enabled	No
Cameron Siguenza ▶	Enabled	No
Deborah Dixon ▶	Disable FileHold Account	No
Guest Portal ▶	Guarantee User Access	No
Guest Read Only ▶	Reset Password	No
Joey Siopongco ▶	Properties	No
Leszek Brykajlo ▶		No

Status will change to Yes

- In FDA, right-click on a user name and select **Guarantee User Access**.



TO REMOVE GUARANTEED USER ACCOUNT ACCESS

1. In the Web Client, go to **User and Group Management > Users** and click the ▶ next to the user name.
 - In FDA, go to **Administration > User & Group Management > Users** and right-click on the user name.
2. Select **Set Access to Not Guaranteed**. The Guaranteed Access status is now set to No.

Name	FileHold Account	Guaranteed Access
Deborah Dixon ▶	Disable FileHold Account	Yes
	Set Access to Not Guaranteed	
	Reset Password	
	Properties	

Status will change to No

3.13. RESET USER PASSWORD

You can reset a user password if they have lost or forgotten it. This is only for locally managed users. You cannot reset a password for a domain user in FileHold.

TO RESET A USER PASSWORD

1. Go to **User and Group Management > Users** and click the ► next to the user name.
 - In FDA, go to **Administration > User & Group Management > Users** and right-click on the user name.
2. Select **Reset Password**.
3. In the Reset Password for User Name window, enter the password twice and click **Update**. Reusing the same password may not be allowed. See [Logon and Password Security](#) for more information about the **Allow password re-use** option.

3.14. SET VIEWER LICENSE

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 System Administrator. Two different viewers are available for purchase to use with the FileHold Desktop Application (FDA):

- Brava Viewer (3 levels)
- PDF/Image Viewer

The Brava viewer and the PDF/Image viewer do not support viewing documents via the web browser (Web Client). However, there are a wide variety of free viewers that can be used with the web client if the native application is not available. These viewers can be installed on the computer running the Web Client to view files downloaded from the document management system. Read a summary of the [viewers work with the Web Client](#).

If the Brava viewer is purchased (any level), customers receive the PDF/Image viewer at no additional cost. If a user is assigned a Brava viewer license, they can also use the PDF/Image viewer with the Brava viewer, with the Brava viewer being the default viewer. The Brava viewer has three levels of viewers available:

- Enterprise Office Viewer (includes PDF/Image Viewer)
- Enterprise Office Viewer with CAD support (includes PDF/Image Viewer)
- Enterprise Office Viewer Engineering Edition (includes PDF/Image Viewer)


See the [complete list of file formats that are supported by the Brava viewer](#).


The PDF/Image Viewer supports the following file formats only:

- PDF
- TIFF (single or multi-page)
- Image files (jpg, png, gif, bmp)

CAUTION: The Brava Viewer MUST be installed when installing the FileHold Desktop Application in order to use the viewer.

TO SET A VIEWER LICENSE FOR A USER

1. In Web Client, go to **User and Group Management > Users** and do one of the following:
 - Click the ► next to the user name and select **Properties > Account Settings**.
 - Select the check box next to a user name and click **Set Viewer License** .

2. In FDA, go to **Administration > User & Group Management > Users**. Select the check box next to the user name and click **Set Viewer License** .
3. Select one of the license options from the list:
 - A viewer is not licensed for this user.
 - PDF/Image Viewer
 - Enterprise Office Viewer (includes PDF/Image Viewer)
 - Enterprise Office Viewer with CAD support (includes PDF/Image Viewer)
 - Enterprise Office Viewer Engineering Edition (includes PDF/Image Viewer)
4. Click **OK**.

3.15. ENABLING AND DISABLING ACCOUNTS

When an employee joins or leaves an organization they will need to have a user account enabled or disabled. In other situations, users may continue to work for an organization but simply no longer need access to FileHold. Enabling and disabling user accounts lets the Systems Administrator create and disable user access to the system without having to [delete user accounts](#).



When a user no longer requires access to the system the user account can be easily disabled. Disabling idle user accounts frees up a license for another user.

By default, when a user is created in the system, the account is enabled.

NOTE: If you need to [delete the user account](#), be sure to use the Change Document Owner and Change Cabinet/Folder Owner features in the Library Administration area to give the cabinets, folders, and documents a new owner. See the [Library Administration Guide](#) for more information.



TO ENABLE A USER ACCOUNT

1. In the Web Client, go to **User and Group Management > Users** and do one of the following:
 - Click the ► next to the disabled user name and select **Enable FileHold account**.
- OR

- Select the check box next to a disabled user name and click **Enable Account** .
2. FDA, go to **Administration > User & Group Management > Users** and do one of the following:
 - Select the check box next to the user name and click **Enable Account** .
- OR
- Right-click on a user name and select **Enable Account**.
3. The FileHold account status changes to Enabled.

TO DISABLE USER ACCOUNT

1. In the Web Client, go to **User and Group Management > Users** and do one of the following:

- Click the ► next to the enabled user name and select **Disable FileHold account**.
- OR
- Select the check box next to an enabled user name and click **Disable Account** .
2. In FDA, go to **Administration > User & Group Management > Users** and do one of the following:
- Right-click on a user name and select **Disable Account**.
- OR
- Select the check box next to a disabled user name and click **Disable Account** .
3. The FileHold account status changes to Disabled.

4. LOGON AND PASSWORD SECURITY

The logon settings allow the System Administrator to manage the number of logon attempts allowed and the time-out settings for user sessions. If users exceed the number of login attempts, the user account is disabled and an email alert is sent to all system administrators. The system administrator will need to [enable the account](#) in the Users area and if the user is a local user, [reset their password](#).

The password settings only apply to FileHold locally managed users and not domain users synchronized with Active Directory. Domain user policies are defined by the Active Directory security policy defined by your organizations IT group.

TO SET THE LOGON AND PASSWORD SECURITY SETTINGS

1. Go to **User and Group Management > Logon and Password Security**.
2. Enter the number of logon attempts allowed. The user will be locked out of the system after the number of login attempts has been exceeded. The system administrator will receive an email stating that the user account has been disabled due to the exceeded number of login attempts.
3. Enter the amount of time, in minutes, that the system automatically logs off inactive users. This is the amount of time that the system is idle and not in use. This frees up a concurrent session for other users.
4. In the Password Settings for Locally Managed Users area, enter the minimum number of characters for the password. This applies only to locally managed users.
5. Select one or more of the following options:
 - Must contain a number
 - Must contain a special character
 - Must contain at least one upper case letter
 - Must contain at least one lower case letter
 - Allow password re-use

6. Enter the number of days that the password expires. Enter 0 if the password is not to expire. This applies only to locally managed users.

Logon & Password Security Settings

Logon attempts allowed: 10 times

Log inactive users off after: 200 minutes

Password Settings for Locally Managed Users

Minimum number of characters: 5

Must contain a number

Must contain a special character

Must contain at least one upper case letter

Must contain at least one lower case letter

Allow password re-use

Password expires after: 0 days
Please enter 0 (zero) in this field if you want the password to Never Expire

Note: password settings only apply to users that are not managed by a directory server (users of type locally managed).

Update Cancel

7. Click **Update**.

5. USER SELF-REGISTRATION

System Administrators can allow users to self-register an account in the FileHold system. This allows users to register themselves in FileHold for an initial period of time. These users can enter their full name, user name, and other contact details (which is optional). Unlike regularly registered users, self-registered users are placed into a temporary area where they are assigned to a group that has no permissions or rights. The administrator re-assigns these users to a group that provides them with the access they need. Self-registered users are considered locally managed users and are managed as such after they have created an account.

The following are reasons for allowing self-registered accounts:

- The system is being deployed for the general public and user registration needs to be self-serve.
- The system is being used by an organization that does not have or plan to use Active Directory to manage the users. This provides access while limiting administrator burden to create user accounts.
- The system is occasionally accessed by casual users who may only logon a few times per year. On-demand access can be provided for these users who may spontaneously decide to access the system.

You will need to assign self-registered users to a group. This will control what the user has access to in the system. Groups, permissions, and roles can be modified by the System and Library Administrators once the user has registered.

Once you have enabled self-registration, a Register button will appear on the main log in page of the FileHold web client.

TO SET UP SELF-REGISTERED USERS

1. Go to User and Group Management > FileHold Groups.
2. Create a new group for the self-registered users. See Creating FileHold Groups for more information.
3. Go to **User and Group Management > User Self-Registration**.

4. Select the Allow User Self-Registration check box.
5. Select the FileHold Group to apply to the self-registered user.
6. Click **Update**. A register button will be visible on the logon page of the Web Client. You cannot self-register from the FileHold Desktop Application (FDA).

6. GLOBAL SETTINGS

In the Global Settings for FileHold, you can set the storage path, default domain, set email settings, enable document and version control, set permissions, and enable schedule settings.

6.1. SETTING THE DEFAULT DOMAIN

When a domain user (user account is synchronized with Active Directory) logs into FileHold, a domain needs to be selected so the system can check with the domain server (Active Directory) to verify your username and password. The default domain is automatically selected for a user at the login screen.

TO SET THE DEFAULT DOMAIN

1. Go to **Global Settings > General**.
2. In the Select Default Domain area, select a domain from the list or leave the setting at “none selected” if Active Directory synchronization is not being used.
3. Click **Update**.

6.2. REMOVING LICENSES FROM DISABLED USERS IN THE DOMAIN

If a domain user (user account is synchronized with Active Directory) is disabled in Active Directory, then the FileHold license can be removed from the user.

TO REMOVE A LICENSE FROM A DISABLED DOMAIN USER

1. Go to [Global Settings > General](#).
2. In the Remove License from Users Disabled in the Domain area, select **Yes** to automatically remove a FileHold license from disabled Active Directory domain users.

6.3. SETTING OUTBOUND EMAIL SETTINGS

Setting the outbound email settings allows administrators to be notified of potential issues and users to receive alerts, reminders and workflow tasks via email. FileHold requires access to a SMTP server which is part of an Email server. FileHold uses the SMTP port / service to relay messages.

You may need to create an email account on your email server in order for FileHold to use this feature.

NOTE: SMTP ports are generally assigned to port 25. Please check with your email server, internal firewall and network system administrator(s) for more details.

TO SET THE OUTBOUND EMAIL SETTINGS

1. Go to [Global Settings > General](#).
2. In the Outbound Email Settings area, enter the **Reply-to email address**. This is the email account that FileHold uses to send outbound emails. This name has to be in the format of an email address such as filehold_alerts@yourcompanyname.com. Your email administrators may need to create an email account for this if your email server requires authentication.
3. Enter the outgoing SMTP server address. Please check with your email administrator for this address.
4. Enter the SMTP server port number. The default is 25. Please check with your email server, internal firewall and network system administrator(s) for more details.
5. Select the SMTP Server Requires Authentication check box, if applicable. This is the username and password created for on the email server to use to send out alerts.
6. Enter the username for the server.
7. Enter the password twice.
8. Select the SMTP server requires an encrypted connection check box, if applicable.
9. Click **Update**.
10. To send a test email, enter the test email address and click **Send Test Email**.
 - If the outbound email settings are correct, a "*Test email message sent successfully*" message appears and an email is delivered to the recipient.
 - If the outbound email settings are not configured correctly, you will receive the message "*Failure sending mail. Check the mail account settings*".
11. Click **Update** at the bottom of the page.

NOTE: You may need to authorize the FileHold server to send SMTP to the email server by changing SMTP security settings on your email server.

6.4. ENABLING THE DOCUMENT AND VERSION CONTROL FIELDS

Document and Version Control Numbers are essentially special metadata fields that allow you to create a 3 letter prefix followed by a range of values. 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.

In order for the Library Administrator to set up document and version control numbers on document schemas, it first must be enabled by the System Administrator. See the [Library Administration Guide](#) for more information.

TO ENABLE CONTROL FIELDS

1. Go to **Global Settings > 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**.

6.5. DOCUMENT SHORTCUTS

Shortcuts to documents can be created but can slow down the Search performance in FileHold. When you have several million documents with several shortcuts, it impacts the performance of the system.

The option of creating document shortcuts can be disabled in order to improve Search performance. Shortcuts will be automatically disabled in FileHold 12 for all new installations (but can be enabled if necessary). If you have existing shortcuts from previous versions of FileHold, this will still be active and enabled when you upgrade. Once shortcuts are created, they cannot be disabled again.

There are several workarounds for shortcuts such as:

- Virtual folders
- Document tray
- My Favorites
- Saved searches
- Linked documents

To read more about these features, see the [User Guide](#) or the [Knowledge Base](#).

TO DISABLE/ENABLE DOCUMENT SHORTCUTS

1. In the **Web Client > System Administration**, go to **General > Document Shortcuts** area.
2. To enable document shortcuts, select the check box.
3. To disable document shortcuts, clear the check box.

6.6. SETTING THE PERMISSION SETTINGS

Permission settings allow certain users to do various functions such as convert between electronic documents and records, covert offline documents to electronic documents, archive

and remove documents from the archive, and allow non-document owners to initialize workflows.

To learn more about converting to different types of records, archiving documents, and workflows, see the *User Guide*.

TO SET USER PERMISSION SETTINGS

1. Go to **Global Settings > General > Permission Settings** area.
2. Select the following options:
 - Enable converting between electronic documents and records – Allows Library Administrators or higher permissions to convert electronic records to electronic documents and vice versa in the metadata pane.
 - Enable converting offline documents to electronic documents – For Library Administrators or higher permissions to convert offline documents to electronic documents using the Check-In window. See the [Knowledge Base](#) for more information.
 - Enable converting electronic documents to offline documents – For Library Administrators or higher permissions to convert electronic documents to offline documents using the “convert to offline” function in the context sensitive menu. See the [Knowledge Base](#) for more information.
 - Enable manually archiving documents – For Library Administrators or higher permissions only. Manually send entire cabinets, drawers, folders, or document(s) to the Library Archive using the “send to archive” function in the context sensitive menu. See the [Knowledge Base](#) for more information.
 - Enable manually unarchiving documents – For Library Administrators or higher permissions only. Manually move documents back to the Library using the “move” function. See the [Knowledge Base](#) for more information.
 - Allow non document version owners to initialize workflows – Allows users that are not owners of a document to initiate a workflow. This permission setting is useful when the person who is adding the document, such as a scanning station worker, is not the person who is initiating the workflow, such as a user on the accounting team.
 - Enable editing document metadata when workflow is active - Allows metadata to be edited for a document that is under the workflow process. This permission setting is useful when a metadata field, such as a status field, needs to be changed during the workflow process.
 - Enable checking out documents when workflow is active — When enabled, the “Allow Check Out” option is available on the workflow template. This allows participants in a workflow to check out a document under the workflow. If disabled, users will not have the option to check out a document that is under the workflow process. See the *Library Administration Guide* for more information on workflow templates.
 - Allow the creator of a document to modify the initial value of read-only fields – Allows the document creator (owner) to modify a read-only custom date or blank date metadata field after the document has been added to the Library. For more information, see the *Library Administration Guide* or the [Knowledge Base](#).
3. Click **Update**.

6.7. EVENT SCHEDULE SETTINGS

You can configure the system to automatically delete, archive, or convert documents to records for a particular schema. Users can also receive alerts and/or email notifications based on an important date which are called user defined events.

- Delete — “Soft” deletes a document based on the event schedule date. The document can still be recovered in the “soft” deletion state.
- Archive — The document is moved to the Library Archive in the hierarchy.
- Convert to Record — The document is no longer editable but remains in the library.
- User Defined Events — Allows email and/or document alerts to be sent to specific administrative groups or document owners to notify them of an important document date or event.

In order to use the events features, the System Administrator must enable them. Library Administrators can then create and apply events to schemas. For more information on events, see the *Library Administration Guide*.

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 — Allow documents to be automatically converted to a record after a specified period of time.
 - Enable Archive Events — Allow documents to be automatically sent to the archive after a specified period of time.
 - Enable Delete Events — Allow documents to be automatically “soft” deleted after a specified period of time.
 - Enable User Defined Events — Allow email and/or document alerts to be sent to specific administrative groups or document owners to notify them of an important document date or event.
3. Click **Update**.

6.8. INSUFFICIENT CAL NOTIFICATION SETTINGS

Concurrent access licenses (CALs) determine how many users can log into the document management system at the same time. This number varies depending upon how many concurrent user licenses your organization has purchased. To see how many CALs you have, you can look at the User page or the License Information page. The User page also displays the number of insufficient CAL events for the last 24 hours in the License Information Area.

List of all FileHold users

	Add User(s)	Add to FileHold Group	Search	Delete	Set Viewer License	Enable Account	Disable Account
A B . D . . G . I . . L M N O P Q R S T U							
Registered Users	Enabled: 34	Remaining: 66	Total: 100				
Concurrent Sessions	Guaranteed: 9	Shared: 26	Total: 35				
Insufficient CALs Events	Occurred: 0						
Enterprise Office Viewer Licenses	Assigned: 1	Remaining: 4	Total: 5				
Enterprise Office Viewer With CAD Support Licenses	Assigned: 0	Remaining: 5	Total: 5				
Enterprise Office Viewer (Engineering Edition) Licenses	Assigned: 2	Remaining: 3	Total: 5				
PDF/Image Viewer Licenses	Assigned: 4	Remaining: 1	Total: 5				
Guest User Sessions	Available: 5						
FileHold SP Client Sessions	Available: 5						

An email notification can be sent to System Administrators and/or Library Administrators when there are insufficient concurrent access licenses. The frequency of the emails can be sent daily or weekly.

TO SET THE EMAIL NOTIFICATION OF INSUFFICIENT CALS

1. Go to **System Administration > Global Settings > General > Insufficient CAL Notification Settings**.
2. In the Notification Interval field, select **Daily** or **Weekly**.
3. In the Recipients field, select **None**, **System Administrators Only**, or **Library and System Administrators**. “None” indicates that no emails will be sent.

6.8.1. Insufficient CAL Log

To determine if there are enough concurrent user licenses for FileHold, you can run the Insufficient CAL Log to view which users were not able to log into the system due to there not being enough concurrent licenses.

TO RUN THE INSUFFICIENT CAL LOG

1. Go to **System Administrator > Logs and Reports > Insufficient CAL**.
2. Enter a username and a date range, if applicable, and click **Apply Filter**. The results of the report are shown below.

6.9. CENTRALIZED OPTIONS MANAGEMENT

The Centralized Options Management area allows System Administrators to globally manage alert preferences, workflow preferences, FastFind preferences, FDA advanced settings, advanced search settings and other miscellaneous preferences for all users of the document management system.

To allow users with a role of Library Administration or higher to bypass the enforcement of the [centralized management options](#), select the **Exclude Administrators** check box.

When enabled, Administrators can set their own preferences regardless of what options are enforced in the global settings. See [Centralized Options Management](#) for more information.

6.10. 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. The OCR mechanism is located on the FileHold server. 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.

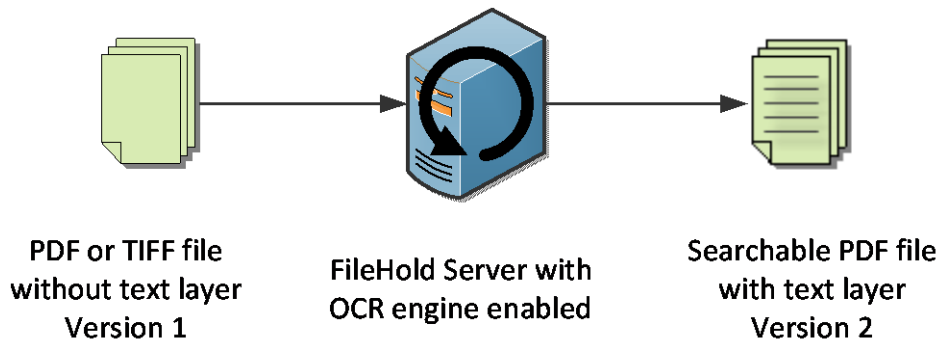
Server side OCR can be a time consuming mechanism; therefore, documents are added to a queue to be processed. All new documents, new versions, manually added or through an automatic import mechanism (such as watched folders or managed imports), are automatically added to the queue. Existing repository documents can be added manually to the queue.

You can enforce the priority for newly added documents or versions so that they will take a higher priority in the queue via a setting. They will be processed before any existing documents in the queue. If the setting is not enforced, documents are taken from the queue in the order they are added without taking priority into account.

The criteria for adding a document to OCR processing queue are:

- The document must be an “Electronic Document” format. Electronic records and offline documents will not be processed.
- Only PDF and TIF/TIFF type documents are processed. TIFF images are converted to searchable PDF documents.
- Only the latest version of the documents can be processed. This is because a new version is created once the document has been OCR’d. The owner of the original document remains the owner for the new OCR’d version.

If a document already contains searchable text, then it is removed from the queue.



The scheduled task “FH OCR documents” can be modified for the frequency and time frame for when the OCR’ing occurs in the Task Scheduler. 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* in the entry 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" />`.

The languages supported by the OCR engine are:

- German
- English
- French
- Spanish

The default configuration is:

- DPI resolution is 300.
- Language is English

The language configuration for OCR 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" />
```

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. In order to use this feature, it must be enabled in the **System Administrator > General** page.

TO ENABLE SERVER SIDE OCR

1. Go to [System Administration > Global Settings > General > Server Side OCR](#).
2. Select the [Enable Server Side OCR](#) check box.
3. To enforce the priority for newly added documents or versions so that they take a higher priority in the queue, select the [Enforce a higher priority for newly added or checked in documents](#) check box. If the setting is not enforced, documents are taken from the queue in the order they are added without taking priority into account.
4. Click [Update](#).

TO ADD EXISTING DOCUMENTS IN THE REPOSITORY TO THE QUEUE

1. Go to [System Administration > Global Settings > General > Server Side OCR](#).
2. Click [Add existing documents to OCR queue](#).
3. At the message prompt, click [OK](#) to continue with the process. This adds existing PDF and TIFF documents in the repository to the queue for processing. Only the last version of the document will be processed. They are added to the queue with a low priority and do not affect the position of existing documents in the queue.

7. REPOSITORY LOCATIONS

The document repository can be split into multiple physical locations to improve scalability. This feature is controlled by a licensing option. If this optional feature has not been purchased, the Add Repository button will be disabled.

In order to balance the load of adding/downloading files between multiple locations and ensure that files are distributed in a sensible way between locations with different level of free space, a semi-random algorithm will be used to select the location for a new file. Repositories that have been marked as read only will not have files added to them; files can only be downloaded.

Once a repository location has been added, new files will be added to it immediately. Repositories containing files cannot be deleted.

When all locations reach the threshold, it is not possible to add any files to the system and all uploads fail with an error message. The system administrator will receive an email notification when the maximum storage space is reached in the repository. A new location should be added to the system or increase the amount of free space on one of the disk if using a virtual server environment.

WARNING: Contact FileHold support prior to moving the file storage path. Moving the file storage path location initiates a re-indexing of the entire Full Text Search feature.

WARNING: The FH_Service account must have full access to this location. If your collection is large, use Robocopy or another method to move the collection to the new location. Using Windows Explorer and "Move" is a recipe for disaster as files can be lost in the process. Always use the copy function. When the copy is complete, compare the original and new locations for an exact/identical File/Folder count. Check and double-check this before doing anything else.

TO ACCESS THE REPOSITORY LOCATIONS

1. Log in to the System Administration area of the Web Client and go to [Global Settings > Repository Locations](#).

TO ADD A REPOSITORY LOCATION

1. Click **Add Repository**.
2. Enter the following information and click **OK** when finished:

Field Name	Description
Path	The path of the physical location.
Capacity	The total size of the disk in TB, GB, or MB. This will be automatically calculated by the system.
Free Space	The amount of free space on the disk in TB, GB, or MB. This will be automatically calculated by the system.
Threshold	The amount of reserved free space on the disk. The default value is 15% of the total disk capacity. You cannot set this limit to less than 10% of the remaining free space on the disk. This value needs to be in MB (1024 MB = 1 GB).
Read Only	When selected, documents cannot be added to this physical location. This option can be selected when the disk has reached its threshold. When clear, documents can be added to this physical location. You cannot mark all locations as read only. There must be at least one disk that is writable for the addition of files into the system

3. In the Repository Locations main page, you need to finalize the addition of the repository location by clicking **OK** or **Apply**. If necessary, the Full Text Search index is re-initialized after applying any changes such as a change in repository path.

NOTE: In versions prior to FileHold 12, only one document repository was able to be used. Storing the repository in a single location limited the repository size to a single disk drive which is about 2 TB. The storage location was set in the **System Administration area > Global Settings > General Settings** page.

TO CHANGE THE THRESHOLD OF THE REPOSITORY

1. Go to **Web Client > System Admin > Global Settings > Repository Locations**.
2. Click on the repository path link.
3. Enter a new amount in the **Threshold** field. This cannot be less than 10% of the total space of the repository and must be set in megabytes (1 GB= 1024 MB). The default is set to 15% of the total capacity. For example: For a repository that has the capacity of 39.90 GB, you can set the threshold to 4084 MB (1024 MB x 4 = 4 GB) which is approximately 10% of the total capacity.
4. Click **Refresh**. This will increase the amount of free space.
5. Click **OK**.

8. LICENSING

The license information area displays a summary of all the enabled features, number of registered user licenses, number of concurrent sessions, number of viewers, the software version, hardware key, and other information pertaining to the license. The date the license

was issued and the license time limit is also shown. If the FileHold license has been fully paid, then the time limit will be “unlimited”.

In order to receive a new license key, copy and paste your FileHold server's unique hardware key into the body of an email and send to licensing@filehold.com. You will receive a license file and can upload the key in the License Information area.

You can add additional user licenses or [optional features](#) after purchasing them from FileHold. To purchase additional licenses or features such as workflow, FastFind, Print-to-FileHold, or Microsoft SharePoint integration, contact sales@filehold.com.

System information Add CALs

How to request a new or replacement licence

1. Copy hardware key from below into the text of an email message
2. Attach a screenshot of this licensing page
3. Write a short note with your contact details, organization page
4. Send email to licensing@filehold.com

For more information on how to license - please visit the [how to license support page](#)

System Details

Is system activated	True
System Version	FileHold 13.00.00
Build	FileHold13_20130821.1
Hardware key	155205241831012094521081 Launch Email to Send Hardware Key
Machine name	QA-ENT2008R2
Domain name	DC2008.QA

License Details

Registered to	Alfonso TEST
Concurrent Sessions	50
Registered Users	50
Guest user sessions	3
FileHold SP Client sessions	disabled
Workflow module	enabled
Active Directory module	disabled
Redaction module	enabled
FastFind module	enabled
Print-to-FileHold	enabled
Multi Document Repository	enabled
Web Scanning	disabled

NOTE: You do not need to reboot or restart the web server after a new license is added.

TO REQUEST A NEW LICENSE KEY

1. In the Web Client, go to **Global Settings > License Information**. The System Information displays your current license information.
 - From the FDA, go to **Administration > License Information**.
2. Click **Launch Email to Send Hardware Key**. Note that a default email application will need to be configured in order for this function to work.
3. The default email application opens with an email addressed to licensing@filehold.com with the system version, build, and hardware key in the body of the email. Type any other pertinent information into the body of the email and click **Send**.

TO ADD A LICENSE KEY

1. In the Web Client, go to **Global Settings > License Information**. The System Information displays your current license information.
 - From the FDA, go to **Administration > License Information**. You are directed to the Web Client login page.

2. Click **Add CALs**.
3. Click **Browse** and select the new license file provided by FileHold.
4. Once the license file is located, click **Upload and Show License Information**.
5. The new license key information appears and a message will indicate the license is valid. Click **Update System License** to complete the process.

8.1. LICENSE EXPIRATION GRACE PERIOD

When a license expires or the hardware key is changed and does not match, an email entitled “*Attention Required: Your FileHold License has Expired*” will be sent automatically to the email addresses of the System Administrators of FileHold. The content of the email includes the when the 7 day grace period ends. The system continues to work normally until the grace period expires.

Once the grace period expires, the system becomes deactivated unless a new license key is uploaded. If you receive the email, use the [License Request](#) procedure to get a new license key.

If you experience a lot of hardware key changes and run a virtual machine environment that is set to automatically recover from hardware failures, please contact FileHold support.

9. ACTIVITY LOG

The Activity log displays the user name, which client they logged into (FDA or Web Client), and the time and date they logged in and out of the system. This log is never deleted or overwritten.

For more detailed reporting, FileHold uses Microsoft SQL Reporting Services integration. See the [Library Administration Guide](#) for more information.

TO VIEW THE ACTIVITY LOG

1. Go to **Logs and Reports > Activity**. The Activity Log is shown.
2. Click **Refresh** to update the log information.
3. Click the page numbers to scroll through the log.

Activity Log							Refresh
Last Name	First Name	User Name	Client	Version	Last Logon	Logout	
Siopongco	Joey	Joey Siopongco	WebClient		2/18/2011 11:26:01 AM	2/18/2011 2:46:18 PM	
Siopongco	Joey	Joey Siopongco	WebClient		2/18/2011 11:14:09 AM	2/18/2011 11:17:28 AM	
sysadm	sysadm	sysadm sysadm	FDA	9.0	2/16/2011 4:04:51 PM	2/16/2011 4:50:23 PM	
Siopongco	Joey	Joey Siopongco	FDA	9.0	2/16/2011 3:54:10 PM	2/16/2011 3:57:35 PM	
Siopongco	Joey	Joey Siopongco	FDA		2/16/2011 3:54:06 PM	2/16/2011 3:54:06 PM	
Siopongco	Joey	Joey Siopongco	WebClient		2/16/2011 3:46:13 PM	2/16/2011 8:32:09 PM	
Mallett	Marvin	Marvin Mallett	WebClient		2/16/2011 2:48:40 PM	2/16/2011 6:14:10 PM	
Mallett	Marvin	Marvin Mallett	WebClient		2/16/2011 2:45:53 PM	2/16/2011 2:46:46 PM	
sysadm	sysadm	sysadm sysadm	WebClient		2/16/2011 2:40:28 PM	2/16/2011 2:45:46 PM	
McMarvin	Basie	Basie McMarvin	WebClient		2/16/2011 2:40:12 PM	2/16/2011 2:40:22 PM	
Marie	Sabine	Sabine Marie	WebClient		2/16/2011 2:39:58 PM	2/16/2011 6:00:09 PM	
sysadm	sysadm	sysadm sysadm	WebClient		2/16/2011 2:32:27 PM	2/16/2011 2:39:38 PM	
sysadm	sysadm	sysadm sysadm	FDA		2/16/2011 2:31:06 PM	2/16/2011 2:31:06 PM	
sysadm	sysadm	sysadm sysadm	FDA	9.0	2/16/2011 11:32:15 AM	2/16/2011 11:32:39 AM	
sysadm	sysadm	sysadm sysadm	FDA	9.0	2/16/2011 11:20:13 AM	2/16/2011 11:32:12 AM	
sysadm	sysadm	sysadm sysadm	FDA		2/16/2011 11:20:08 AM	2/16/2011 11:20:08 AM	
Siopongco	Joey	Joey Siopongco	WebClient		2/11/2011 11:24:40 AM	2/11/2011 12:04:09 PM	
Siopongco	Joey	Joey Siopongco	FDA	9.0	2/11/2011 11:23:29 AM	2/11/2011 11:47:49 AM	
Siopongco	Joey	Joey Siopongco	FDA	9.0	2/11/2011 11:12:23 AM	2/11/2011 11:23:26 AM	
Siopongco	Joey	Joey Siopongco	WebClient		2/11/2011 11:06:10 AM	2/11/2011 11:23:21 AM	
Siopongco	Joey	Joey Siopongco	WebClient		2/11/2011 10:47:22 AM	2/11/2011 11:08:04 AM	
Siopongco	Joey	Joey Siopongco	FDA	9.0	2/10/2011 11:51:30 AM	2/10/2011 12:22:09 PM	
sysadm	sysadm	sysadm sysadm	WebClient		2/10/2011 11:49:58 AM	2/10/2011 12:36:12 PM	
Siopongco	Joey	Joey Siopongco	FDA	9.0	2/10/2011 11:49:14 AM	2/10/2011 11:51:28 AM	
Siopongco	Joey	Joey Siopongco	WebClient		2/10/2011 11:46:38 AM	2/10/2011 11:49:49 AM	

1 2 3 4 5 6 7 8 9 10 ... >>

10. SYSTEM AUDIT LOG

The System Audit Log logs activities performed by a System Administrator. It is accessible in the System Administration area in the Web Client. This log is never deleted or overwritten.

The following information is recorded in the log:

- Adding local and domain users
- Deleting local users
- Adding and deleting FileHold groups
- Enable and disabling licenses
- Resetting passwords
- Adding and removing users to and from FileHold groups

The audit log can be filtered by user name, description, and to and from dates.

TO ACCESS THE SYSTEM AUDIT LOG:

1. Log into the [Web Client > System Admin](#) and go to [Logs and Reports > 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.

11. CENTRALIZED OPTIONS MANAGEMENT

The Centralized Options Management area allows System Administrators to globally manage alert preferences, workflow preferences, FastFind preferences, FDA advanced settings, advanced search settings and other miscellaneous preferences for all users of the document management system.

When the options are set globally by the administrator:

- They can be set as the default value and then changed by the end user if desired.
- They can be set and then “enforced” meaning that the end users cannot modify the option.

Administrators can set the default option values and update them at any time. Once the default options are set and saved, they will be pushed out to the end users if the option is enforced or if they have not have been already set by the end user. If end users have their own preferences set, they will not be overwritten upon saving the settings, unless the option is set to enforced.

Any changes made in the centralized options management area will be recorded in the System Administrator [Audit Log](#).

NOTE: If any of the options are “enforced”, they can be enforced only for anyone who has a lower role than Library Administrators. Library and System Administrators can still modify preferences even if they are enforced if enabled in the System Admin > [General settings](#) page.

11.1. ALERT PREFERENCES

Set the alert preferences for all users of the document management system to determine when they receive email and alert notifications under the Document Alerts area of My FileHold. Notifications can be sent when:

- Changes are made to documents or metadata

- Changes to documents within specific folders
- Specific date based events (user defined events)
- A reminder is set on a document

TO SET THE GLOBAL ALERT PREFERENCES

1. In the Web Client, go to [System Admin > Centralized Options Management > Alert Preferences](#).
2. Use the following table to set the global alert preferences for the document management software:

Option	Values	Default Value
Notification when new documents/versions are Added to folders user has subscribed to	Enabled Disabled	Enabled
Notification when documents are Transferred To folders user has subscribed to	Enabled Disabled	Disabled
Notification when documents are Deleted from folders user has subscribed to	Enabled Disabled	Disabled
Notification when a new version of a document user has subscribed to is Checked-in	Enabled Disabled	Enabled
Notification when metadata values are updated for a document user has subscribed to.	Enabled Disabled	Disabled
In addition to notifying user on My FileHold send an email of the notification	Disabled Immediately Daily Weekly	Immediately
Send email when a document reminder is activated	Enabled Disabled	Disabled

3. Select the **Enforce** check box next to the preference you want to be imposed on all users. Users will not be able to modify this setting in their personal alert preferences. Administrators may be able to modify their personal alert preferences which are dependent upon the setting in [System Admin > Global Settings > General](#).
4. To reset the value for all users, click the **Reset** button next to the option name. At the prompt message, click **OK**. The settings will take effect the next time the user logs into FileHold.
5. To reset all alert preference options to their original default values, click **Reset All Settings**.
6. Click **Save**. The changes will be pushed out to all end users unless their alert preferences have been previously modified. If the option is set to “enforced” then their alert preferences will be changed and locked down (meaning they cannot be modified by the end user) except for [possibly Library Administrators or higher](#).

11.2. WORKFLOW PREFERENCES

Set the workflow preferences for users to determine when they receive emails notification about tasks and workflow changes.

TO SET THE GLOBAL WORKFLOW PREFERENCES

1. In the Web Client, go to **System Admin > Centralized Options Management > Workflow Preferences**.
2. Use the following table to set the global workflow preferences for the document management software:

Option	Values	Default Value
Notification when a task is assigned or delegated to user	Enabled Disabled	Enabled
Notification when a task assigned to user is overdue	Enabled Disabled	Enabled
Notification when a task assigned to user is overridden	Enabled Disabled	Enabled
Notification when a task assigned to me is reserved by another participant	Enabled Disabled	Enabled
Notification when a task assigned to user is cancelled	Enabled Disabled	Enabled
Notification when a task assigned to user is restarted	Enabled Disabled	Enabled
Notification when a document associated with a task assigned to user is added or removed	Enabled Disabled	Enabled
Notification when a document associated with a task assigned to user is checked out or checked in	Enabled Disabled	Enabled
Notification if tasks in workflow user is the initiator of are overdue	Enabled Disabled	Enabled
Notification when activity is completed for a workflow user initiated	Enabled Disabled	Enabled
Notification when workflow is restarted for a workflow user initiated	Enabled Disabled	Enabled
Notification when document is added or removed from a workflow user initiated	Enabled Disabled	Enabled
Notification when workflow is completed for a workflow user is an observer of	Enabled Disabled	Enabled

Option	Values	Default Value
Notification when workflow is restarted for a workflow user is an observer of	Enabled Disabled	Enabled
Notification when document is added or removed from a workflow user is an observer of	Enabled Disabled	Enabled
Notification when activity is completed for a document that user owns	Enabled Disabled	Enabled
Email Alerts Frequency	Immediately Daily Weekly	Immediately

3. Select the **Enforce** check box next to the preference you want to be imposed on all users. Users will not be able to modify this setting in their personal workflow preferences. Administrators may be able to modify their personal workflow preferences which are dependent upon the setting in [System Admin > Global Settings > General](#).
4. To reset the value for all users, click the **Reset** button next to the option name. At the prompt message, click **OK**. The settings will take effect the next time the user logs into FileHold.
5. To reset all workflow preference options to their original default values, click **Reset All Settings**.
6. Click **Save**. The changes will be pushed out to all end users unless their workflow preferences have been previously modified. If the option is set to “enforced” then their preferences will be changed and locked down (meaning they cannot be modified by the end user) except for [possibly Library Administrators or higher](#).

11.3. FASTFIND PREFERENCES

FastFind provides search capability from third party windows-based forms applications such as Windows applications such as accounting or GIS software. FastFind works in conjunction with the FileHold Desktop Application (FDA). Users can use keyboard shortcut shortcuts that perform searches directly from the chosen application in the document management system to find relevant data instantly.

The options for FastFind settings can be globally enabled through the centralized options management.

TO SET THE GLOBAL FASTFIND PREFERENCES

1. In the Web Client, go to [System Admin > Centralized Options Management > FastFind Preferences](#).
2. Use the following table to set the global FastFind preferences for the document management software:

Option	Values	Default Value
Enable FastFind	Enabled Disabled	Disabled

Option	Values	Default Value
Update FastFind templates when user logs in to FileHold	Enabled Disabled	Disabled
Enable mouse search	Enabled Disabled	Disabled
Enable selection search	Enabled Disabled	Disabled
Enable clipboard search	Enabled Disabled	Disabled
Enable screen OCR search	Enabled Disabled	Disabled

3. Select the **Enforce** check box next to the preference you want to be imposed on all users. Users will not be able to modify this setting in their personal FastFind preferences. Administrators may be able to modify their personal FastFind preferences which are dependent upon the setting in [System Admin > Global Settings > General](#).
4. To reset the value for all users, click the **Reset** button next to the option name. At the prompt message, click **OK**. The settings will take effect the next time the user logs into FileHold.
5. To reset all FastFind preference options to their original default values, click **Reset All Settings**.
6. Click **Save**. The changes will be pushed out to all end users unless their FastFind preferences have been previously modified. If the option is set to “enforced” then their preferences will be changed and locked down (meaning they cannot be modified by the end user) except for [possibly Library Administrators or higher](#).

11.4. MISCELLANEOUS PREFERENCES

There are some miscellaneous settings which can be configured globally. They are described in the table below.

TO SET THE GLOBAL MISCELLANEOUS PREFERENCES

1. In the Web Client, go to [System Admin > Centralized Options Management > Misc Preferences](#).
2. Use the following table to set the global miscellaneous preferences for the document management software:

Option	Description	Values	Default Value
Default page in Web Client after log in	Sets the default screen for the Web Client only after a user logs in. To the default screen in the FDA, see User Preferences.	Blank Simple Search Advanced Search Tasks	Blank

Option	Description	Values	Default Value
Edit metadata upon Check In action	When enabled, the metadata pane is displayed in edit mode after a new version is checked in. This allows the user to enter new metadata. If disabled, the user can check the document back in without editing metadata.	Enabled Disabled	Disabled
Clear required metadata fields upon Check In	When enabled, any required fields in the schema are automatically blanked out (current value is deleted) when checking in a new version of a document. The users are forced to fill in the required field prior to checking in the document.	Enabled Disabled	Disabled
Number of expanded drawers	The number of drawers that can be simultaneously expanded in the library tree. The last number of drawers opened is preserved when the library is refreshed. The lower number of expanded drawers allows for a faster page loading time since the lower number of permissions that needs to be calculated before displaying the library structure to the user.	1, 2, 3, 4, or 5	3

3. Select the **Enforce** check box next to the preference you want to be imposed on all users. Users will not be able to modify this setting in their User preferences. Administrators may be able to modify their personal User preferences which are dependent upon the setting in [System Admin > Global Settings > General](#).
4. To reset the value for all users, click the **Reset** button next to the option name. At the prompt message, click **OK**. The settings will take effect the next time the user logs into FileHold.
5. To reset all Misc preference options to their original default values, click **Reset All Settings**.
6. Click **Save**. The changes will be pushed out to all end users unless their User preferences have been previously modified. If the option is set to “enforced” then their preferences will be changed and locked down (meaning they cannot be modified by the end user) except for [possibly Library Administrators or higher](#).

11.5. FDA ADVANCED SETTINGS

The FDA Advanced settings area is some of the options that are set in the User Preferences in the FileHold Desktop Application (FDA). These are only for the FDA.

TO SET THE GLOBAL FDA ADVANCED SETTINGS PREFERENCES

1. In the Web Client, go to [System Admin > Centralized Options Management > FDA Advanced Settings](#).
2. Use the following table to set the global FDA Advanced Settings preferences for the document management software:

Option	Values	Default Value
Show Welcome Screen at Startup	Enabled Disabled	Enabled
Default screen at startup	Blank Simple Search Advanced Search Inbox Tasks Calendar	Blank
Maximum simultaneous transfers (This is the number of documents that can be uploaded or downloaded at a time)	This number can be any value but it is recommended to keep it at 1.	1
By default delete documents that a user Adds to FileHold	Enabled Disabled	Disabled
By default delete documents that a user Checks In to FileHold	Enabled Disabled	Disabled
Prompt for Download Location when a user Makes Copies of Files	Enabled Disabled	Enabled
Prompt for Download Location when a user Checks Out Files	Enabled Disabled	Enabled
Prompt user to remove files when sending them from the Inbox	Enabled Disabled	Enabled
Prompt to clean up the FileHold Working Folder when a user closes the FileHold Desktop Application	Enabled Disabled	Enabled
By default close documents that a user Adds/Checks In to FileHold	Enabled Disabled	Disabled
Auto-Send documents to Auto-Tagged folders	Enabled Disabled	Disabled
Auto-Send documents after completing metadata	Enabled Disabled	Disabled
Move to recycle bin instead of permanently deleting	Enabled Disabled	Disabled

Option	Values	Default Value
Automatically open in the Viewer selected document in Inbox	Enabled Disabled	Disabled
Automatically open in the Viewer selected document in folders and search results	Enabled Disabled	Disabled
Open documents in the Document Viewer using separate tabs	Enabled Disabled	Disabled
Allow opening one document in multiple tabs	Enabled Disabled	Disabled
Enable Smart Check In and Smart Check Out messages	Enabled Disabled	Enabled
Enable Click to Tag	Enabled Disabled	Disabled

3. Select the **Enforce** check box next to the preference you want to be imposed on all users. Users will not be able to modify this setting in their personal User preferences. Administrators may be able to modify their personal User preferences which are dependent upon the setting in [System Admin > Global Settings > General](#).
4. To reset the value for all users, click the **Reset** button next to the option name. At the prompt message, click **OK**. The settings will take effect the next time the user logs into FileHold.
5. To reset all User preference options to their original default values, click **Reset All Settings**.
6. Click **Save**. The changes will be pushed out to all end users unless their preferences have been previously modified. If the option is set to “enforced” then their preferences will be changed and locked down (meaning they cannot be modified by the end user) except for [possibly Library Administrators or higher](#).

11.6. ADVANCED SEARCH OPTIONS

The Advanced Search options management allows you to set the advanced search options so that they persist and can be enforced for each advanced search. These are the check box options that show in the Advanced search page.

The screenshot shows the 'Advanced Search' interface. At the top, there are two dropdown menus: 'File or Metadata' and 'Contains', followed by a search input field and a 'Search' button. Below the search bar, there are four checkboxes: 'Search Metadata Only', 'Include Archive in Search', 'Include All Document Versions', and 'Search Using Historical Metadata Fields'. A red box highlights these checkboxes.

TO SET THE GLOBAL ADVANCED SEARCH OPTIONS

1. In the Web Client, go to [System Admin > Centralized Options Management > Advanced Search Options](#).
2. Use the following table to set the global Advanced Search options for the document management software:

Option	Description	Values	Default Value
Search Metadata Only	Searches the metadata only and not the contents of a document (full-text search).	Enabled Disabled	Disabled
Include Archive in Search	Searches the documents in the Library archive and includes any matches in the results. FileHold will search only the Library (current documents) if this option is not selected.	Enabled Disabled	Disabled
Include All Document Versions	Searches all versions of the document. FileHold will only search the latest version if this option is not selected.	Enabled Disabled	Disabled
Search Using Historical Metadata Fields	If metadata field names and values have been changed over time, you can still search these "historical" items as FileHold keeps track of any changes that have been made.	Enabled Disabled	Disabled

3. Select the **Enforce** check box next to the preference you want to be imposed on all users. Users will not be able to modify this setting in their personal Advanced Search options. Administrators may be able to modify their personal Advanced Search options which are dependent upon the setting in [System Admin > Global Settings > General](#).
4. To reset the value for all users, click the **Reset** button next to the option name. At the prompt message, click **OK**. The settings will take effect the next time the user logs into FileHold.
5. To reset all advanced preference options to their original default values, click **Reset All Settings**.
6. Click **Save**. The changes will be pushed out to all end users unless their Advanced Search options have been previously modified. If the option is set to "enforced" then their options will be changed and locked down (meaning they cannot be modified by the end user) except for [possibly Library Administrators or higher](#).

INDEX

- A**
- Active Directory, 1, 9, 10, 26
 - activity log, 36
 - Allow non document version owners to initialize workflows, 29
 - Allow the creator of a document to modify the initial value of read-only fields, 29
 - audit log. *See* system audit log
- C**
- cabinet administrator role, 14
 - CALs, 30, *See* licenses
 - centralized options management, 31, 37
 - advanced search options, 44
 - alert preferences, 37
 - exclude administrators, 31
 - FastFind preferences, 40
 - FDA advanced settings, 42
 - miscellaneous settings, 41
 - workflow preferences, 39
 - check out
 - checking out documents when workflow is active, 29
 - concurrent sessions, 7
 - convert between electronic documents and records, 29
 - convert electronic documents to offline documents, 29
 - convert offline documents to electronic documents, 29
- D**
- default domain
 - setting, 26
 - document control fields
 - enabling, 28
 - document publisher + delete role, 13
 - document publisher role, 13
 - document shortcuts, 28
 - domain groups, 9
 - domain users, 2, 6, 9
 - adding, 10
- E**
- email
 - outbound mail settings, 27
 - event schedule, 30
 - archive, 30
 - convert to record, 30
 - delete, 30
 - enabling, 30
 - user defined events, 30
- F**
- FDA, 3
 - FileHold Domain Groups, 9
 - FileHold Domain Users, 9
 - FileHold groups. *See* groups
- G**
- global settings, 26
 - groups, 11
 - adding users, 15
 - creating, 11
 - deleting, 20
 - permissions diagram, 16
 - user roles, 12
 - viewing properties, 18
 - guaranteed access, 20
 - guest user role, 12
- I**
- insufficient CALs, 30
 - log, 31
 - notification settings, 31
- L**
- Library Administrator, 1, 16
 - library administrator role, 14
 - licenses
 - adding additional licenses, 35
 - removing from disabled domain users, 26
 - viewers, 22
 - locally managed users, 2, 6, 7
 - creating, 8
 - log in, 3
 - log out
 - FDA, 4
 - Web Client, 4
 - logon security, 24
- M**
- manually archiving documents, 29
 - manually unarchiving documents, 29
 - Microsoft Active Directory, 9
 - Microsoft SQL Reporting Services, 36
- O**
- OCR, 31
 - languages supported, 32
 - organizer + delete role, 14

organizer role, 13

P

password security, 24
passwords
 resetting, 21
permission settings, 28
publisher + delete role, 13
publisher role, 13

R

read-only role, 13
registered users, 7
repository locations, 33
 add repository, 34
reset passwords, 21
responsibilities, 2

S

scheduled task
 FH OCR documents, 32
security, 3
 problems, 3
self-registered users, 25
 setting up, 26
senior library administrator role, 15
server side OCR. *See* OCR
shortcuts, 28
skills required, 1
synchronizing
 domain users, 9
System Administrator
 responsibilities, 2
 skills required, 1
system administrator role, 15
system audit log, 37

T

time-out settings, 24

U

user roles, 12
user self-registration, 6
users
 adding to groups, 15
 deleting, 19
 disabling accounts, 23
 enabling accounts, 23
 reset password, 21
 searching for, 19
 viewing properties, 18
users and groups
 example plan, 5
 flowchart, 7
 managing access, 6
 overview, 6
 setting up, 4

V

version control fields
 enabling, 28
viewers
 licenses, 9, 22

W

WebCap scanning license, 9
workflows
 editing document metadata when workflow is active,
 29