FileHold

Document & Record Lifecycle Software

System Administration Guide

version 14.2

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.

Proprietary Notice

TABLE OF CONTENTS

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
- Enable viewer features
- Set Microsoft® SQL Report permissions

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, system 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 in the Administration panel.

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 (Firefox and Internet Explorer are supported) and enter the path to the FileHold server. This may be set up as link on your desktop.
2. Enter your Login, Password, and select the domain (if required) and click **Log In**.
3. Click the **Administration Panel** link at the top of the screen. Once logged in, the different areas of the system administration and Library Administration features will appear in the left panel.

TO LOGIN AS SYSTEM ADMINISTRATOR VIA THE FDA

1. Log into FDA using a system administrator username and password.
2. Go to **Administration** menu in the menu bar.

TO LOG OUT FROM THE WEB CLIENT

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

To log out from the FDA

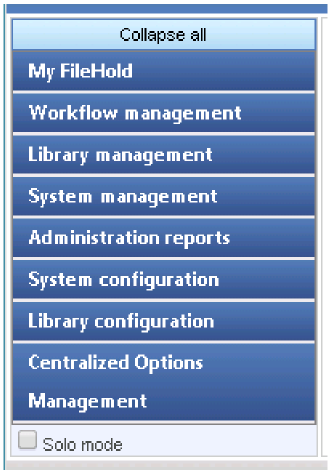
1. Go to **File > Exit**.

3. WEB CLIENT ADMINISTRATION PANEL

The system administration and library administration areas can be found combined in the area called the Administration panel. Some end user preferences and settings (user, view, alert) are also available in the Administration panel. This is in addition to the FileHold library area where end user preferences can also be set.

Depending upon the role used to log into the Web Client, only the functionality that the user is able to access is shown. As a system administrator, you have access to everything in the Administration panel.

If Solo Mode is enabled, then only one section of the Administration Panel will expand at a time. If Solo Mode is disabled, then all of the sections can be expanded and the Collapse All button is available.



The following list describes the areas that are available to only system administrators in the Administration panel:

- Administration reports > Effective Permissions
- Administration reports > Insufficient sessions
- Administration reports > System audit log
- Administration reports > User activity
- Centralized options management > Advanced search preferences
- Centralized options management > Alert preferences
- Centralized options management > FastFind preferences
- Centralized options management > FDA preferences
- Centralized options management > Miscellaneous preferences
- Centralized options management > Workflow preferences
- System configuration > Document repository locations
- System configuration > General

- System configuration > Security > Logon
- System configuration > Security > Self registration
- System management > License information
- System management > Permissions > Group
- System management > Permissions > User
- System management > Permissions > Custom reports
- System configuration > Document viewers (FDA)

4. USERS AND GROUP PERMISSIONS

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.

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

FileHold Group	Membership	Role
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

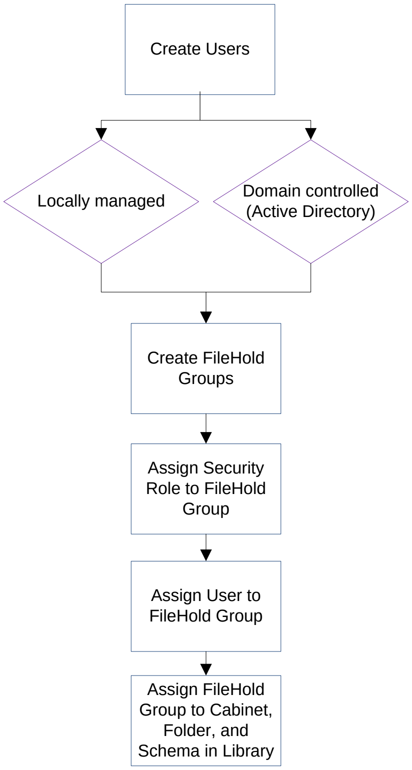
WARNING: System administrators should be very careful about which users/groups will receive delete permissions. Remember that it is easier to mark or flag files for deletion than it is to recover and restore them from the IT Enterprise backup system.

4.1. 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.


Create Users
Locally managed
Domain controlled (Active Directory)
Create FileHold Groups
Assign Security Role to FileHold Group
Assign User to FileHold Group
Assign FileHold Group to Cabinet, Folder, and Schema in Library

4.2. CREATING USERS

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.

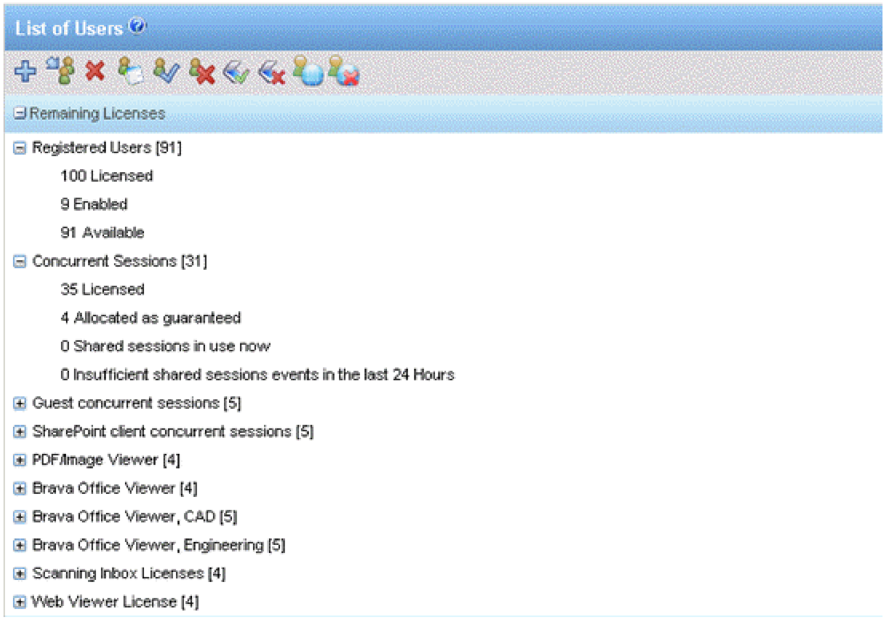
  Administrators can quickly create user accounts in mere minutes OR activate user self-registration.

- 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.

4.2.1. Users list

The list of users is accessible in the Administration Panel in the Web Client under System Management > Permissions > Users. The Users list includes the remaining licenses panel and a filter panel.

The Remaining Licenses area contains a summary of the purchased licenses: registered users, concurrent sessions, viewers, WebCap scanning licenses, and web viewers, SharePoint sessions and guest portal sessions. The various licensing options can be expanded or collapsed by clicking on the + or -. The number of licenses remaining is shown in brackets.



List of Users

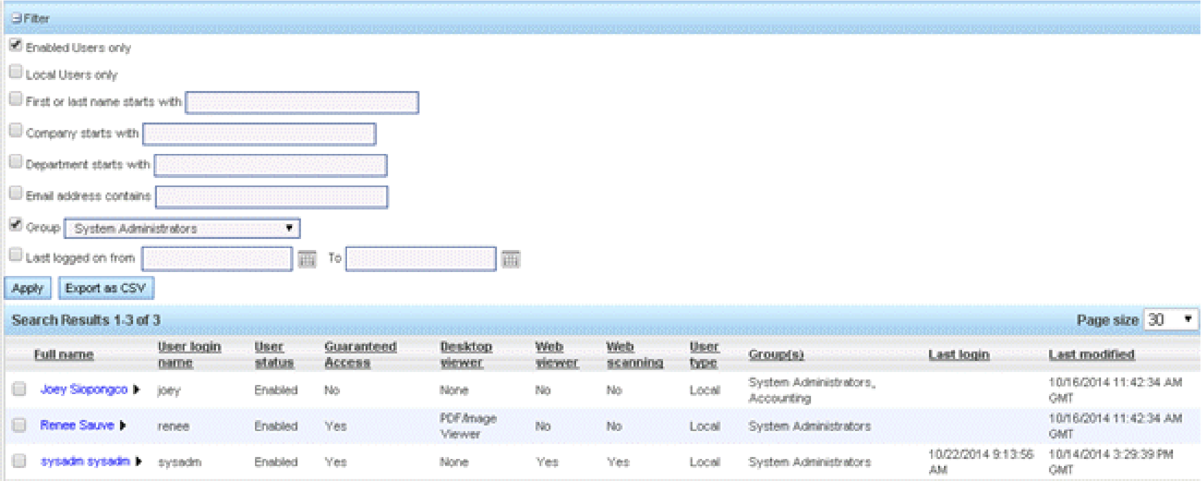
⊟ Remaining Licenses

- ⊟ Registered Users [91]
  - 100 Licensed
  - 9 Enabled
  - 91 Available
- ⊟ Concurrent Sessions [31]
  - 35 Licensed
  - 4 Allocated as guaranteed
  - 0 Shared sessions in use now
  - 0 Insufficient shared sessions events in the last 24 Hours
- ⊞ Guest concurrent sessions [5]
- ⊞ SharePoint client concurrent sessions [5]
- ⊞ PDF/Image Viewer [4]
- ⊞ Brava Office Viewer [4]
- ⊞ Brava Office Viewer, CAD [5]
- ⊞ Brava Office Viewer, Engineering [5]
- ⊞ Scanning Inbox Licenses [4]
- ⊞ Web Viewer License [4]

A Registered User is someone who has a FileHold account 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 number of concurrent sessions in use is shown.

The Filter area can be used to narrow down the users displayed in the search results below. Enabled users only, local users (non-Active Directory users) first or last name, company, department, email address, group name, and logged in dates are the filter criteria that can be used. Search results can be exported as a csv file. If no filter criteria are used then all users are displayed in the search results.

The number of users is shown in the search results list. The number of rows that are displayed in the report view can be adjusted to show 15, 30, or 60 rows at a time. Click on the column to sort in ascending or descending order.



⊟ Filter

☑ Enabled Users only
☐ Local Users only
☐ First or last name starts with
☐ Company starts with
☐ Department starts with
☐ Email address contains
☑ Group: System Administrators
☐ Last logged on from … To …

Search Results 1-3 of 3 — Page size: 30

	Full name	User login name	User status	Guaranteed Access	Desktop viewer	Web viewer	Web scanning	User type	Group(s)	Last login	Last modified
☐	Joey Siopongco	joey	Enabled	No	None	No	No	Local	System Administrators, Accounting		10/16/2014 11:42:34 AM GMT
☐	Renee Sauve	renee	Enabled	Yes	PDF/Image Viewer	No	No	Local	System Administrators		10/16/2014 11:42:34 AM GMT
☐	sysadm sysadm	sysadm	Enabled	Yes	None	Yes	Yes	Local	System Administrators	10/22/2014 9:13:56 AM	10/14/2014 3:29:39 PM GMT

A unique ID number is given to each user. In the event that users have exactly the same name, the unique ID number can be used to differentiate between the same named users. This unique ID is used in the various logs and reports.

The information displayed in the results is:

Icon	Column Header	Description
👤		Enabled domain user.
👤⊗		A domain user that has been disabled in the domain.
👥		Domain group.
	Full name	First and last name of the user.
	User login name	The login name of the user.
	User status	Enabled or disabled.
	Guaranteed access	A concurrent session is dedicated to a user Yes or No
	Desktop viewer	A PDF/Image or Brava viewer or None.
	Web viewer	Web client viewer is assigned Yes/No.
	Web scanning	WebCap scanning license is assigned Yes/No.
	User type	Local or domain user.
	Group(s)	The name of the groups the user is assigned to.
	Last login	The last time the user logged in.
	Last modified date	The last time the user profile was updated.

4.2.2. 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 Active Directory server. For more information on domain users, see Synchronizing Domain (Active Directory) Users and Groups.

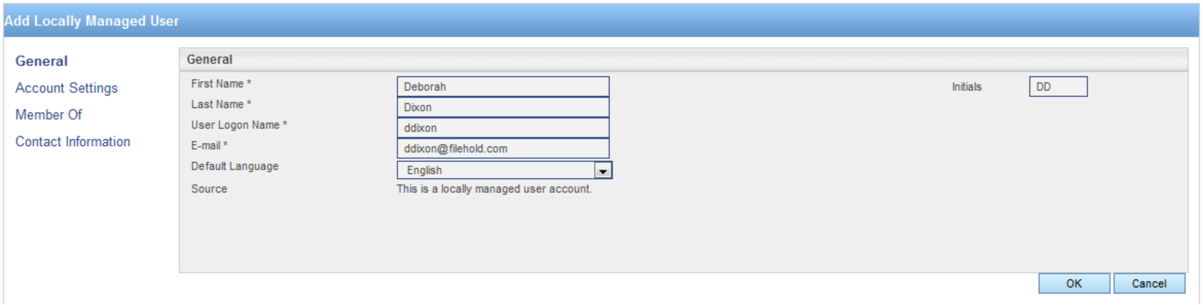
TO CREATE A LOCALLY MANAGED USER

1. From the Web Client, go to **Administration Panel > System Management > Permissions > Users.** .

- Alternatively, in FDA, log in with system administrator rights and go to **Administration > User & Group Management > Users**.

2. Click **Add Users**.
3. Select **Locally Managed User** and click **Next**.
4. Fill in the following information and click **OK**:
   - First Name
   - Last Name
   - User Logon Name
   - Email
   - Default Language
   - Source — Locally managed user account

- Initials



Add Locally Managed User

General
Account Settings
Member Of
Contact Information

General

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

5. 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
   - Brava Office Viewer
   - Brava Office Viewer, CAD (includes PDF/Image Viewer)
   - Brava Office Viewer, Engineering (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 Web Viewer License Association area, select the Web Viewer License Assigned check box if the user is to be assigned a web viewer license.
10. In the Account Expiration area, select at 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.
11. Click **OK**.
12. In the Member Of window, you will need to add the user to a group. See Adding Users to Groups for more information.
13. Select Contact Information and enter the user's contact information such as addresses, phone numbers, and company information. This information is optional.
14. Click **OK**. The user is added to the list of registered users.

4.2.3. 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.

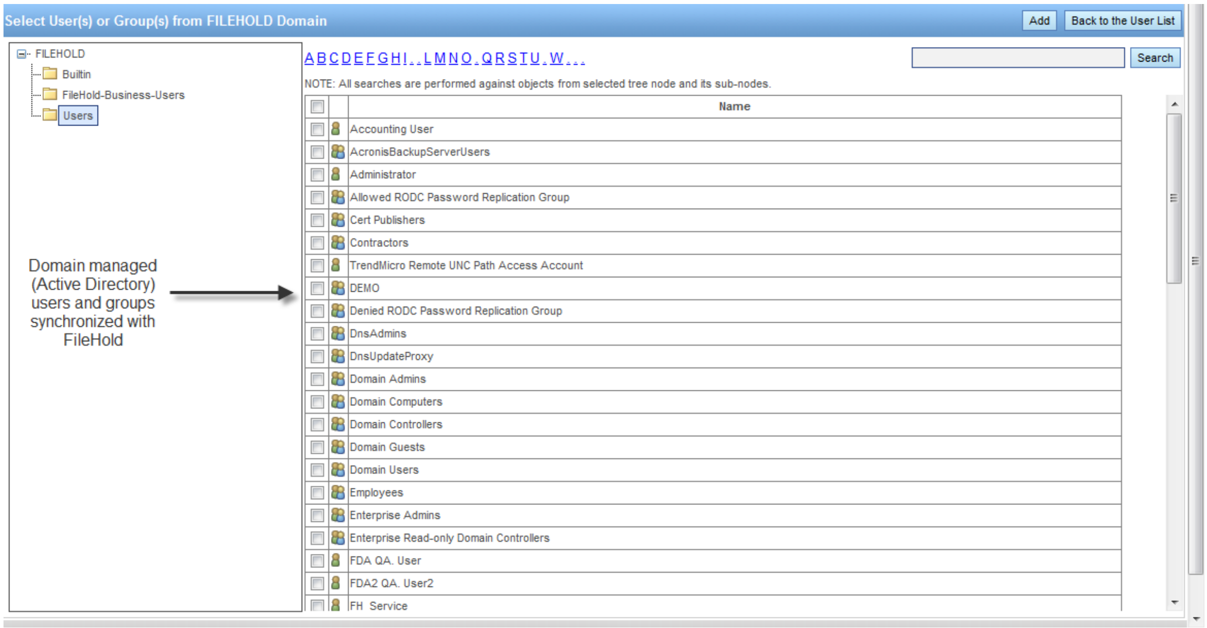
NOTE: It is important to keep in mind that some Active Directory deployments can be complex as they employ custom schemas and objects that may not be industry standard and can require additional effort to synchronize.

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.

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, go to **Administration Panel > System Management > Permissions > Users** and click **Add User(s).**
    - 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**.


Select User(s) or Group(s) from FILEHOLD Domain
Add
Back to the User List
FILEHOLD
Builtin
FileHold-Business-Users
Users
A B C D E F G H I . . L M N O . Q R S T U . W . . .
Search

NOTE: All searches are performed against objects from selected tree node and its sub-nodes.

☐		Name
☐	👤	Accounting User
☐	👥	AcronisBackupServerUsers
☐	👤	Administrator
☐	👥	Allowed RODC Password Replication Group
☐	👥	Cert Publishers
☐	👥	Contractors
☐	👤	TrendMicro Remote UNC Path Access Account
☐	👥	DEMO
☐	👥	Denied RODC Password Replication Group
☐	👥	DnsAdmins
☐	👥	DnsUpdateProxy
☐	👥	Domain Admins
☐	👥	Domain Computers
☐	👥	Domain Controllers
☐	👥	Domain Guests
☐	👥	Domain Users
☐	👥	Employees
☐	👥	Enterprise Admins
☐	👥	Enterprise Read-only Domain Controllers
☐	👤	FDA QA. User
☐	👤	FDA2 QA. User2
☐	👤	FH Service

Domain managed (Active Directory) users and groups synchronized with FileHold

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.

4.3. CREATING FILEHOLD GROUPS

A FileHold Group 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

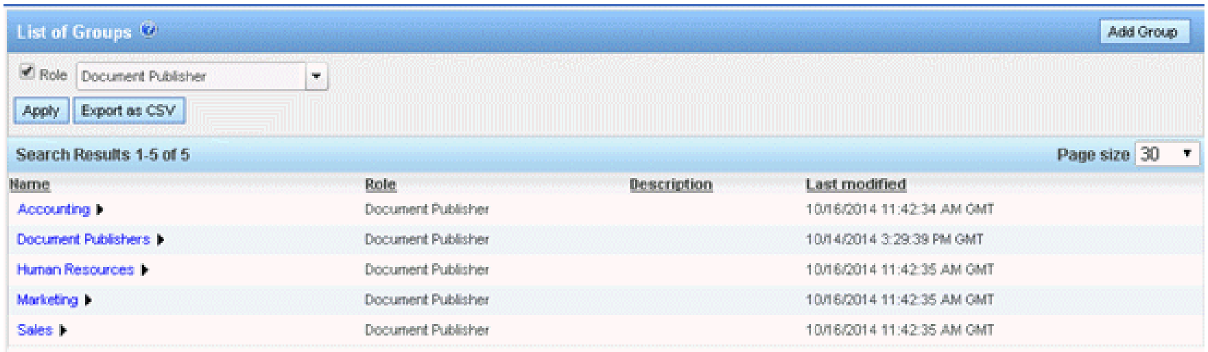
1. In the Web Client, go to **Administration Panel > System Management > Permissions > Groups**.

- 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.

To filter the Group list

1. Select the **Role** check box and select a role from the drop down list.
2. Click **Apply**. The number of results is shown below. The number of rows that are displayed in the report view can be adjusted to show 15, 30, or 60 rows at a time. Click on the column to sort in ascending or descending order.
3. Click **Export to CSV** to export to a CSV file.



Search Results 1-5 of 5

Name	Role	Description	Last modified
Accounting	Document Publisher		10/16/2014 11:42:34 AM GMT
Document Publishers	Document Publisher		10/14/2014 3:29:39 PM GMT
Human Resources	Document Publisher		10/16/2014 11:42:35 AM GMT
Marketing	Document Publisher		10/16/2014 11:42:35 AM GMT
Sales	Document Publisher		10/16/2014 11:42:35 AM GMT

4.3.1. 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	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. With the guest user role you can optionally bypass the login process entirely by setting up a Self-Service Portal with a guest user account. The Self-Service Portal is an optional module that allows users to access FileHold with a special URL. The portal does not require a login as this is done programmatically. The user simply visits the URL and the portal page appears. For more information about guest user licenses, contact sales@filehold.com.
Read Only	A Read-Only user role may only download or open and read documents from FileHold. They cannot edit, delete, or create documents. They can email documents if given this functionality by system administrators.
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	Publisher user role can do everything a Document Publisher can do plus: • Create new folders and folder groups. • Copy or move folders that they have already created. • Clone folders and folder groups created by other users and become the owners of the folders / folder groups. • Publishers cannot delete existing documents, folders or folder groups including those which they have added /created. All documents and folders created by the Publisher will be owned by them and they cannot change the ownership.
Publisher + Delete	Publisher plus Delete user role can do everything that a Publisher can do plus delete documents, folders and folders group owned (created) by them.

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

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

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

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.

4.4. ADDING USERS TO GROUPS

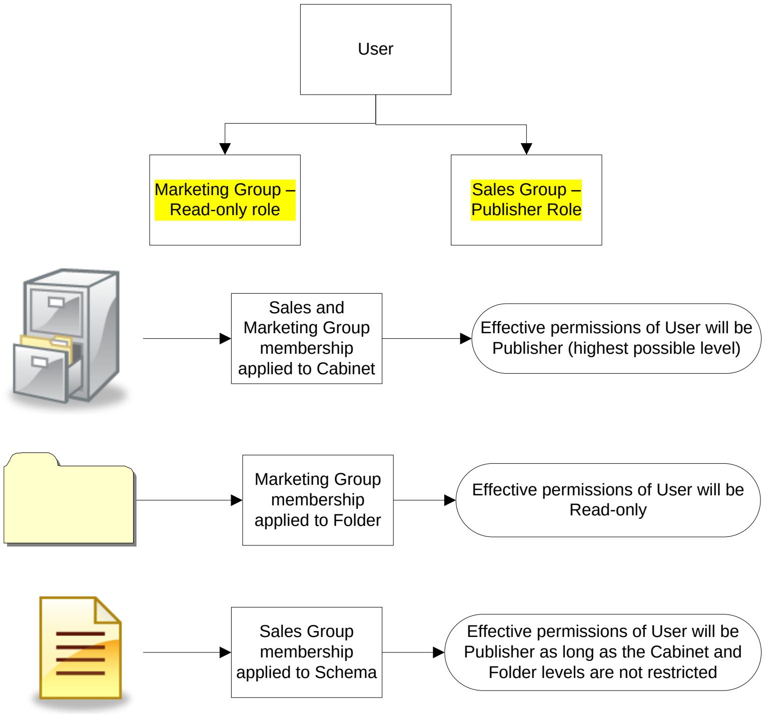
Once the users are in the system, you can add them to FileHold groups. Users can be assigned to an unlimited number of groups and groups can contain one or more users.

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.

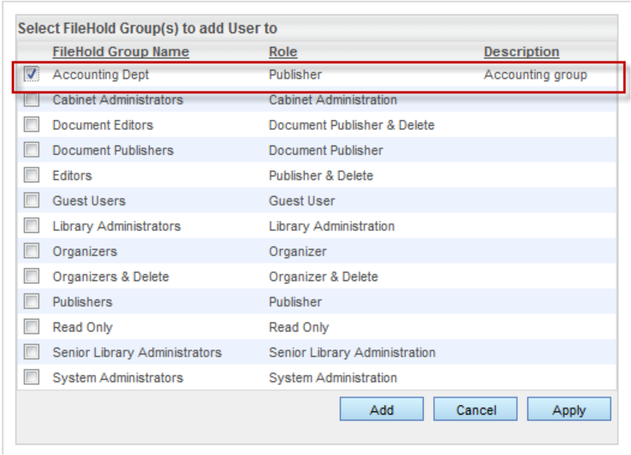
When users belong to more than one FileHold group they will inherit the access level of the highest group of which they are a member. For example if a user is assigned to the Marketing group (associated with a read-only role) and the Sales group (associated with the publisher role) they will have full 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.


User
Marketing Group – Read-only role
Sales Group – Publisher Role
Sales and Marketing Group membership applied to Cabinet
Effective permissions of User will be Publisher (highest possible level)
Marketing Group membership applied to Folder
Effective permissions of User will be Read-only
Sales Group membership applied to Schema
Effective permissions of User will be Publisher as long as the Cabinet and Folder levels are not restricted

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 Web Client, go to **Administration Panel > System Management > Permissions > 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.

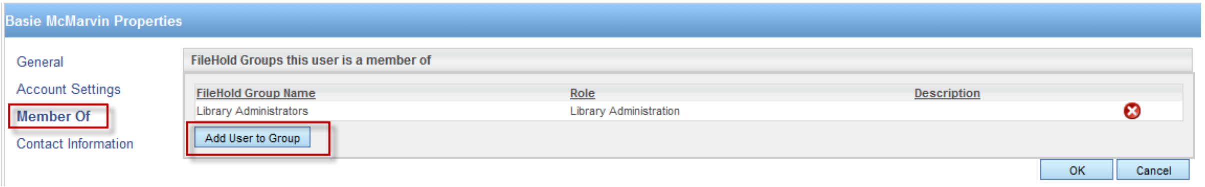


Select FileHold Group(s) to add User to

	FileHold Group Name	Role	Description
☑	Accounting Dept	Publisher	Accounting group
☐	Cabinet Administrators	Cabinet Administration	
☐	Document Editors	Document Publisher & Delete	
☐	Document Publishers	Document Publisher	
☐	Editors	Publisher & Delete	
☐	Guest Users	Guest User	
☐	Library Administrators	Library Administration	
☐	Organizers	Organizer	
☐	Organizers & Delete	Organizer & Delete	
☐	Publishers	Publisher	
☐	Read Only	Read Only	
☐	Senior Library Administrators	Senior Library Administration	
☐	System Administrators	System Administration	

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

1. In the Web Client, go to **Administration Panel > System Management > Permissions > 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**.



Basie McMarvin Properties

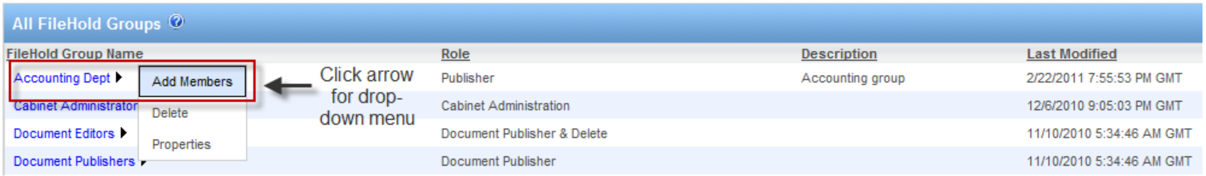
FileHold Groups this user is a member of

FileHold Group Name	Role	Description
Library Administrators	Library Administration	

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. Go to **Administration Panel > System Management > Permissions > Groups** and select **Add Members** from the drop-down menu on the group name.
   - In FDA, go to **Administration > User & Group Management > Groups** and right-click on a group name and select **Add Member**.



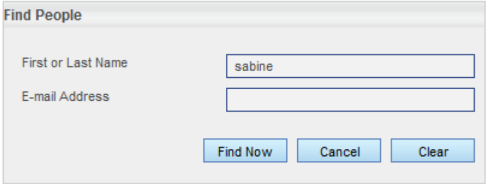
All FileHold Groups

FileHold Group Name	Role	Description	Last Modified
Accounting Dept	Publisher	Accounting group	2/22/2011 7:55:53 PM GMT
Cabinet Administrator	Cabinet Administration		12/6/2010 9:05:03 PM GMT
Document Editors	Document Publisher & Delete		11/10/2010 5:34:46 AM GMT
Document Publishers	Document Publisher		11/10/2010 5:34:46 AM GMT

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

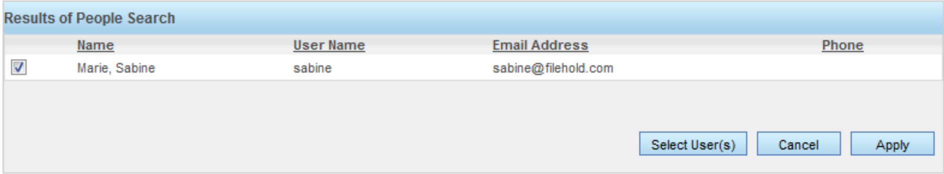
1. In the Web Client, go to **Administration Panel > System Management > Permissions > Groups** and select **Properties** from the drop-down menu on the group name.
   - In FDA, go to **Administration > User & Group Management > Groups** and click the **Group Name** in the list.
2. In the FileHold Group Members area, click **Add Members**.
3. In the Find People window, enter the first or last name of the user and/or the email address and click **Find Now**.
4. 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: sabine

E-mail Address:



Results of People Search

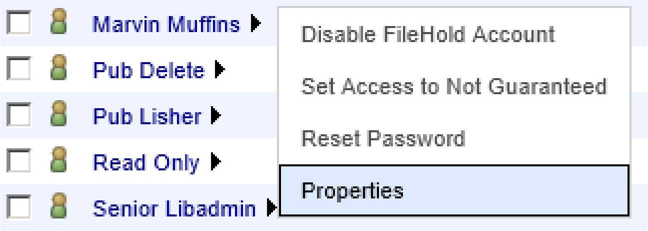
	Name	User Name	Email Address	Phone
☑	Marie, Sabine	sabine	sabine@filehold.com	

4.5. 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

1. In the Web Client, go to **Administration Panel > System Management > Permissions > Users** and click on a user name.
   - Alternatively, 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.
   - Alternatively, in FDA, log in with system administrator rights and go to **Administration > User & Group Management > Users**.



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

4.6. VIEWING GROUP PROPERTIES

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

TO VIEW GROUP PROPERTIES

1. In the Web Client, go to **Administration Panel > System Management > Permissions > Groups** and click on a group name.

- Alternatively, you can 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.
- Alternatively, in FDA, log in with system administrator rights and go to **Administration > User & Group Management > Groups**.

2. Update or view the group name, description, role, notes, group members and restrictions for the user and click **OK**.

4.7. 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. Go to **Administration Panel > System Management > Permissions > Users**.
2. Use any of the following filters:
   - Enabled users only
   - Local users only
   - First or last name starts with
   - Company starts with
   - Department starts with
   - Email address contains
   - Group
   - Last logged on from <date> to <date>
3. Click **Apply Filter**. The number of results and the report are shown below. The number of rows that are displayed in the report view can be adjusted to show 15, 30, or 60 rows at a time. Click on the column to sort in ascending or descending order.
4. To export the results, click **Export as CSV**.

In the List of Users, you can add, modify, disable, guarantee access, set a viewer license and many more functions. See the following sections for more information.

4.8. 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. It is recommended that you disable user accounts instead of deleting them.

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.

To delete a user account

1. Go to **Administration Panel > System Management > Permissions > Users** and select the check box for user account you want to delete. You can use the Filter feature to find a user.
2. Click **Delete**.
3. You will receive a warning message that you are about to delete a user and it will specifically warn that "*All previous associations with documents added by this user shall be lost and are not recoverable*".

   This message simply means that the user account and its associations cannot be recovered if you delete the account, and the Cabinets, Folders, and Documents created by this user will no longer have an owner, as the user has been permanently deleted.

   Deleting a user does not delete the Cabinets, Folders, and Documents - it removes the user's ownership of those items. If you wish to maintain these ownership associations, then simply disable the account.
4. Click **OK** to delete the user. The user account is removed from the list of FileHold users, and there is no way to recover this account.
5. Change ownership using the Change Document Owner and Change Cabinet/Folder Owner features in the library administration area to give the cabinets, folders, and documents created/owned by this user to a new owner. See the *Library Administration Guide* or the FileHold Knowledge Base for details.

4.9. 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 **Administration Panel > System Management > Permissions > Groups** and click the arrow next to the group name.
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.

4.10. 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.

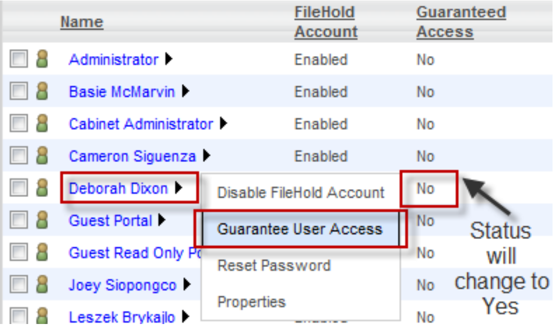
For example, a company with 40 total (named) users and 20 concurrent licenses means that all 40 people share the same pool of 20 concurrent connections. If two of the named users are given guaranteed access then they will each have a dedicated concurrent license ensuring they always be able to get into 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 **Administration Panel > System Management > Permissions > Users** and click the ▶ next to the user name.

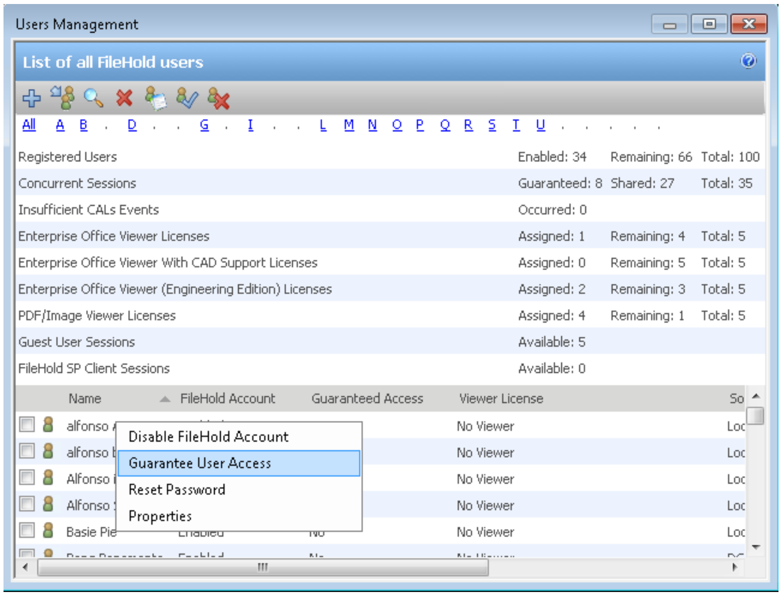
- In FDA, go to **Administration > User and Group Management > Users**.

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 ▶		No
□	Guest Portal ▶		No
□	Guest Read Only Po		No
□	Joey Siopongco ▶		No
□	Leszek Brykajlo ▶	Enabled	No

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



Users Management

List of all FileHold users

Registered Users	Enabled: 34	Remaining: 66	Total: 100
Concurrent Sessions	Guaranteed: 8	Shared: 27	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: 0		

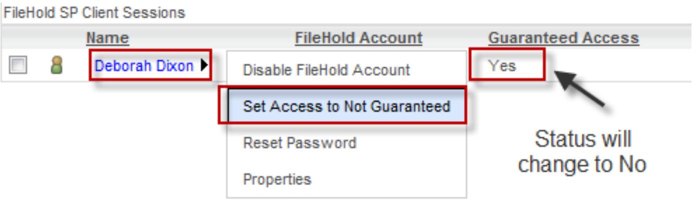
	Name	FileHold Account	Guaranteed Access	Viewer License	So
□	alfonso			No Viewer	Loc
□	alfonso			No Viewer	Loc
□	Alfonso			No Viewer	Loc
□	Alfonso			No Viewer	Loc
□	Basie Pie	Enabled	No	No Viewer	Loc

To Remove Guaranteed User Account Access

1. In the Web Client, go to **Administration Panel > System Management > Permissions > 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.



4.11. 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 **Administration Panel > System Management > Permissions > 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.

4.12. 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 is a Web Viewer or 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.

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:

- Brava Viewer
- Brava with CAD support
- Brava Engineering Edition

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 **Administration Panel > System Management > Permissions > 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
   - Enterprise Office Viewer, CAD
   - Enterprise Office Viewer, Engineering
4. Click **OK**.

4.13. 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. You will need to enable a user account if they have exceeded the number of login attempts set in FileHold.

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 **Administration Panel > System Management > Permissions > 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 **Administration Panel > System Management > Permissions > 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.

5. MICROSOFT SQL REPORT PERMISSIONS

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

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

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

- In the FileHold Library under Reports.
- As a custom web page integrated into a web application.

- Via the SQL Server Reporting Services Home Page. Once on the home page users can navigate to the FH Reports folder and select a report to view.

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

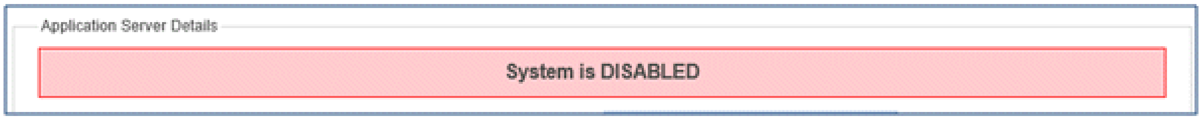
To set report security

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

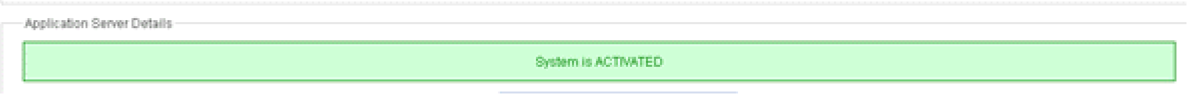
6. LICENSING

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 the Application Server Details area, a status is shown if the system is activated or deactivated.

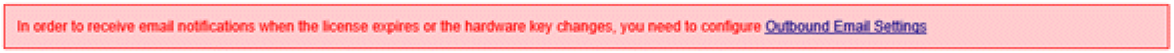


System is DISABLED



System is ACTIVATED

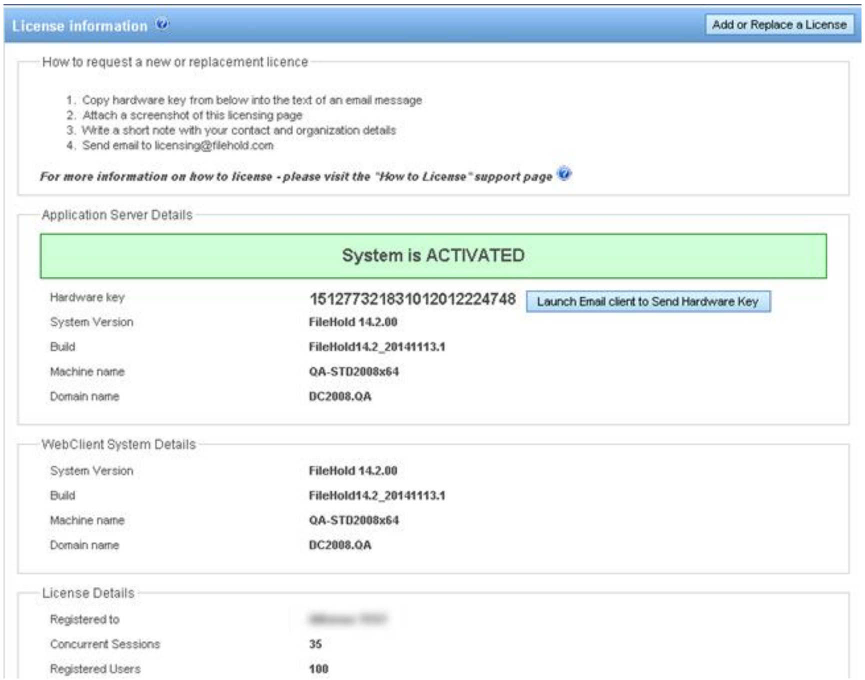
If the Outbound Email Settings are not configured, a message is displayed at the top of the licensing screen. Click the link to configure the outbound email settings.



In order to receive email notifications when the license expires or the hardware key changes, you need to configure Outbound Email Settings

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.



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 and organization details
4. Send email to licensing@filehold.com

For more information on how to license - please visit the "How to License" support page

Application Server Details

System is ACTIVATED

Hardware key	151277321831012012224748
System Version	FileHold 14.2.00
Build	FileHold14.2_20141113.1
Machine name	QA-STD2008x64
Domain name	DC2008.QA

WebClient System Details

System Version	FileHold 14.2.00
Build	FileHold14.2_20141113.1
Machine name	QA-STD2008x64
Domain name	DC2008.QA

License Details

Registered to	[redacted]
Concurrent Sessions	35
Registered Users	100

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 **Administration Panel > System Management > 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 Apply a License Key

1. In the Web Client, go to **Administration Panel > System Management > 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 or Replace a License**.
3. Click **Choose File** and select the new license file provided.
4. Once the license file is located, click **Upload and Show License Information**. The new license key information appears and a message will indicate the license is valid.
5. Click **Update System License** to complete the process.

6.1. 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.

7. ADMINISTRATION REPORTS

A number of reports are available for the system administrator to maintain and monitor the document management system.

7.1. USER ACTIVITY LOG

he User Activity log is a report that displays the user name, which client they logged into, and the time and date they logged in and out of the system. The User Activity log available filters include: user name (drop down list), full name, user logon name starts with, login date range, logout date range, and active sessions only (check box).

The following column information is displayed: full name, user login name including the internal ID number (the internal ID number is used to distinguish users with the same name), client (FDA, Web Client, Mobile, FH Instrumentation, Microsoft SharePoint, Custom), version and build number, connection pool (normal, guest, or SharePoint), client address, log in date and time, log out date and time.

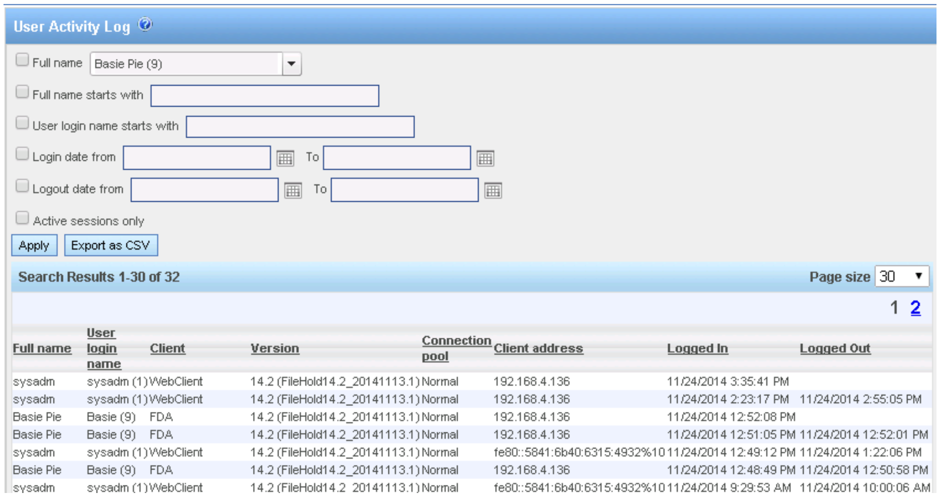
The User Activity log is accessible only by system administrators. This log is never deleted or overwritten.

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. In the Web Client, go to **Administration Panel > Administration Report > User Activity**.
2. Use any of the following filters:
   - Full Name
   - Full name starts with
   - User login name starts with
   - Login date from - to
   - Logout date from - to
   - Active sessions only – When enabled, displays only those users who are using a currently logged into the system.

3. Click **Apply Filter**. The number of results and the report are shown below. The number of rows that are displayed in the report view can be adjusted to show 15, 30, or 60 rows at a time. Click on the column to sort in ascending or descending order.
4. To export the results, click **Export as CSV**.



User Activity Log

□ Full name Basie Pie (9)
□ Full name starts with
□ User login name starts with
□ Login date from To
□ Logout date from To
□ Active sessions only

Search Results 1-30 of 32

Page size 30

1 2

Full name	User login name	Client	Version	Connection pool	Client address	Logged In	Logged Out
sysadm	sysadm (1)	WebClient	14.2 (FileHold14.2_20141113.1)	Normal	192.168.4.136	11/24/2014 3:35:41 PM	
sysadm	sysadm (1)	WebClient	14.2 (FileHold14.2_20141113.1)	Normal	192.168.4.136	11/24/2014 2:23:17 PM	11/24/2014 2:55:05 PM
Basie Pie	Basie (9)	FDA	14.2 (FileHold14.2_20141113.1)	Normal	192.168.4.136	11/24/2014 12:52:08 PM	
Basie Pie	Basie (9)	FDA	14.2 (FileHold14.2_20141113.1)	Normal	192.168.4.136	11/24/2014 12:51:05 PM	11/24/2014 12:52:01 PM
sysadm	sysadm (1)	WebClient	14.2 (FileHold14.2_20141113.1)	Normal	fe80::5841:6b40:6315:4932%10	11/24/2014 12:49:12 PM	11/24/2014 1:22:06 PM
Basie Pie	Basie (9)	FDA	14.2 (FileHold14.2_20141113.1)	Normal	192.168.4.136	11/24/2014 12:48:49 PM	11/24/2014 12:50:58 PM
sysadm	sysadm (1)	WebClient	14.2 (FileHold14.2_20141113.1)	Normal	fe80::5841:6b40:6315:4932%10	11/24/2014 9:29:53 AM	11/24/2014 10:00:06 AM

7.2. SYSTEM AUDIT LOG

The System Audit Log logs activities performed by a system administrator. 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. In the Web Client, go to **Administration Panel > Administration Reports > System Audit Log**.
2. Use any of the following filters:
   - Username
   - Description contains – Enter a full or partial description such as "deleted folder" or "added"
   - From <date> to <date>
3. Click **Apply Filter**. The number of results and the report are shown below. The number of rows that are displayed in the report view can be adjusted to show 15, 30, or 60 rows at a time. Click on the column to sort in ascending or descending order.
4. Click **Export to CSV** to export to a CSV file.

7.3. INSUFFICIENT CONCURRENT SESSIONS 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. This report is accessible by system administrators.

TO RUN THE INSUFFICIENT CONCURRENT SESSIONS LOG

1. In the Web Client, go to **Administration Panel > Administration Reports > Insufficient Sessions**.
2. Enter a username and a date range, if applicable, and click **Apply Filter**. The results of the report are shown below. The number of results and the report are shown below. The number of rows that are displayed in the report view can be adjusted to show 15, 30, or 60 rows at a time. Click on the column to sort in ascending or descending order.
3. To export the results, click **Export as CSV**.

7.4. EFFECTIVE PERMISSIONS REPORT

The Effective Permissions report allows system administrators to view the permissions of users in the system and modify permissions. The report can be filtered by user, the object type (library, archive or schema), library location, schema name, the origin of the role (group, library or inherent), and enabled and disabled users.

This log is never deleted or overwritten. The following information is displayed in the effective permissions report:

Symbol	Column Header	Description
Cabinet icon	-	Permissions at the cabinet level.
Folder icon	-	Permissions at the folder level.
Schema icon	-	Permissions at the schema level.
L	-	Library
A	-	Archive
S	-	Schema
	Full name	First and last name of the user
	User login name	The login name of the user including the unique ID number.
	Name	Name of the cabinet, folder, or schema. Click on the link to change the permissions at this level
	Location	The library location where the folder is located. This only contains a value when the object is a folder. The format of the location is the parent object's name followed by the parent object's ID. Multiple senior objects are separated by forward slash. Example, CabinetA (5) / DrawerB (1) / FolderGrpC (14).

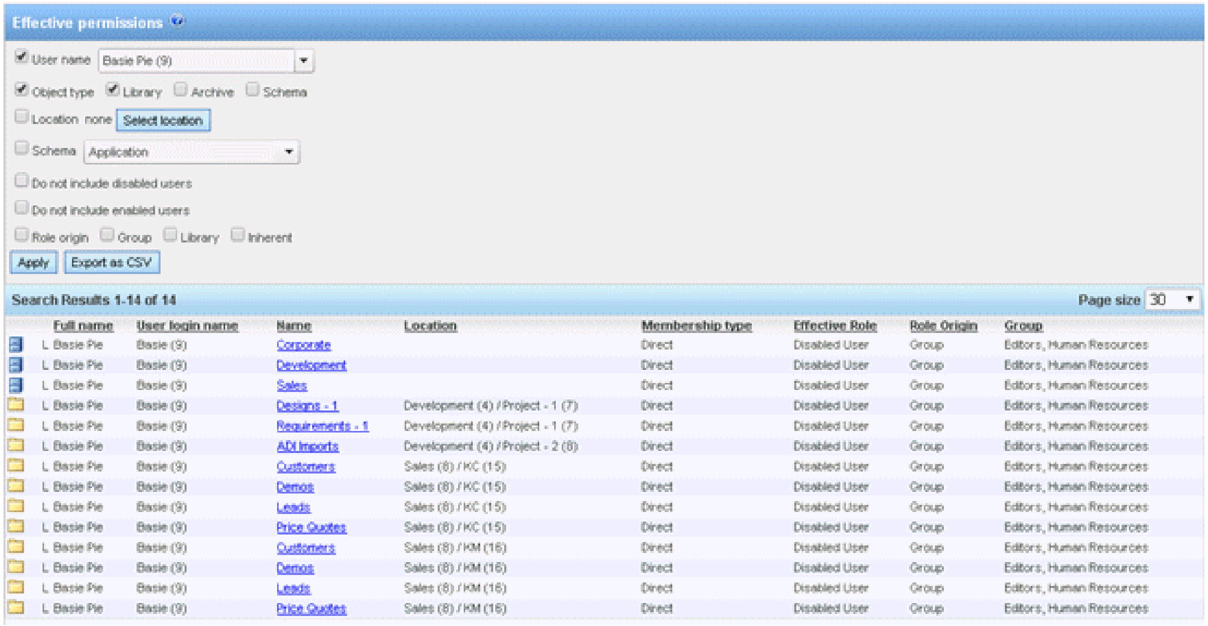
Symbol	Column Header	Description
	Membership type	Direct – The value is direct if the specific user, not group, is assigned directly to the object as a member or owner. Indirect – For all other cases the value will be indirect. This includes the situation for inherent permissions such as system administrators. If a user is directly assigned to an object and they are also indirectly assigned by a group, if both the highest implied role and highest assigned role match then the membership type is direct.
	Effective role	The resulting permission in that area: Member – Used with schemas. Owner – Owner of either a cabinet or folder. Disabled user – The user is disabled in the system. See Determining Effective Role for more information.
	Role origin	Library – The role is set at the cabinet or folder level. Group – The role is set at the group. Inherent – The role is inherent such as senior library or system administrator See Role Origin for more information.
	Group	Name of the group where the user has the highest level of permissions. If the role is Owner and the membership type is Direct there is no group. See Group Effective Role for more information.

TO VIEW THE EFFECTIVE PERMISSIONS REPORT

1. In the Web Client, go to **Administration Panel > Administration Report > Effective Permissions**.
2. Use any of the following filters:

- User Name – Select a user name from the list.
- Object type – Select Library, Archive (library archive), or Schema.
- Location – Click Select Location to select a specific area in the library.
- Schema – Select a schema name from the list
- Do not include disabled users – Select this option to leave any disabled users out of the report results. Only enabled users are shown.
- Do not include enabled users – Select this option to leave any enabled users out of the report results. Only disabled users are shown.
- Role origin – Select Group (role is from the group membership), Library (role is assigned at a folder or cabinet), or Inherent (role is inherent such as senior library or system administrator).

3. Click **Apply Filter**. The number of results and the report are shown below. The number of rows that are displayed in the report view can be adjusted to show 15, 30, or 60 rows at a time. Click on the column to sort in ascending or descending order.
4. To modify permissions at any level, click on the **Name** link. The properties for that level opens.
5. To export the results, click **Export as CSV**.



☑ User name: Basie Pie (9)

☑ Object type ☑ Library □ Archive □ Schema

□ Location none

□ Schema: Application

□ Do not include disabled users

□ Do not include enabled users

□ Role origin □ Group □ Library □ Inherent

Search Results 1-14 of 14 — Page size 30

	Full name	User login name	Name	Location	Membership type	Effective Role	Role Origin	Group
	L Basie Pie	Basie (9)	Corporate		Direct	Disabled User	Group	Editors, Human Resources
	L Basie Pie	Basie (9)	Development		Direct	Disabled User	Group	Editors, Human Resources
	L Basie Pie	Basie (9)	Sales		Direct	Disabled User	Group	Editors, Human Resources
	L Basie Pie	Basie (9)	Designs - 1	Development (4) / Project - 1 (7)	Direct	Disabled User	Group	Editors, Human Resources
	L Basie Pie	Basie (9)	Requirements - 1	Development (4) / Project - 1 (7)	Direct	Disabled User	Group	Editors, Human Resources
	L Basie Pie	Basie (9)	ADI Imports	Development (4) / Project - 2 (8)	Direct	Disabled User	Group	Editors, Human Resources
	L Basie Pie	Basie (9)	Customers	Sales (8) / KC (15)	Direct	Disabled User	Group	Editors, Human Resources
	L Basie Pie	Basie (9)	Demos	Sales (8) / KC (15)	Direct	Disabled User	Group	Editors, Human Resources
	L Basie Pie	Basie (9)	Leads	Sales (8) / KC (15)	Direct	Disabled User	Group	Editors, Human Resources
	L Basie Pie	Basie (9)	Price Quotes	Sales (8) / KC (15)	Direct	Disabled User	Group	Editors, Human Resources
	L Basie Pie	Basie (9)	Customers	Sales (8) / KM (16)	Direct	Disabled User	Group	Editors, Human Resources
	L Basie Pie	Basie (9)	Demos	Sales (8) / KM (16)	Direct	Disabled User	Group	Editors, Human Resources
	L Basie Pie	Basie (9)	Leads	Sales (8) / KM (16)	Direct	Disabled User	Group	Editors, Human Resources
	L Basie Pie	Basie (9)	Price Quotes	Sales (8) / KM (16)	Direct	Disabled User	Group	Editors, Human Resources

7.4.1. Determining Effective Role

For library or archive objects the effective role is a combination of the groups they belong to and their library role assignments. The owner library role assignment is the effective role regardless of any other roles the user may have. When a user is directly assigned their effective role is the highest role they are assigned across all groups they are members of. When a user is assigned as part of one or more groups their effective role is the highest of their assigned groups taking into account advanced security reductions in role.

In the following table Library and Archive are synonymous.

Object	Role Assignment(s)	Effective Role
Schema	Any, user not disabled	Member
Schema	Organizer or lower and the user is disabled.	Disabled User
Library	Library admin or lower and the user is disabled.	Disabled User
Library	Any, user not disabled, assigned as owner	Owner
Library	Any, user not disabled, directly assigned, not modified	*highest implied role*
Library	Any, user not disabled, directly assigned, modified	*modified role*
Library	Any, user not disabled, indirectly assigned	*highest assigned role*

7.4.2. Determining the Highest Implied Role

The highest implied role is used when a user is assigned directly to an option. As there is no group assignment the user's group membership must be checked. The user's effective role will be the highest role for all their group assignments.

For example, if the user is assigned to a group with the Organizer role and a second group with the Document Publisher role their highest role would be Organizer. For any object they are assigned to their effective role will be Organizer.

There is a special implied role when a cabinet administrator owns the cabinet, but not a folder in the cabinet, nor is a member of a folder in the cabinet. This case should be treated as though the cabinet administrator was directly assigned as a member of the folder.

7.4.3. Determining a Modified Role

Modified roles are configured with the advanced security setting on a cabinet or folder. Modified roles are absolute. Regardless of the role normally assigned to the user or group the modified role can be any lower role. For example, this means that a group with a library administration role could be assigned to a cabinet as read only for that cabinet. System administrators and senior library administrators cannot have their roles modified.

7.4.4. Determining the Highest Assigned Role

The highest assigned role is used when a user is indirectly assigned to an object by membership in a group. Their effective role will the highest role of all groups they are members of that are assigned to the object. If this role of any group has been modified this must be taken into account when determining the highest role.

For example, assume a user is assigned as a member of GroupA (Organizer), GroupB (Document Publisher), and GroupC (Document Publisher). GroupA and GroupC have been assigned to Folder1. GroupA has a modified role to Publisher. The user's highest assigned role for Folder1 would be Publisher.

7.4.5. Role Origin

The following table describes the role origin. In the table Library and Archive are synonymous.

Object	User or Group Role	Assignment	Role Origin
Schema	System administrator	None	Inherent
Schema	Senior library administrator	None	Inherent
Schema	Library administrator	None	Inherent
Schema	Cabinet administrator	None	Inherent
Schema	All other roles	Member	Group
Library	System administrator	None	Inherent
Library	Senior library administrator	None	Inherent
Library	System administrator	Owner	Library
Library	Senior library administrator	Owner	Library

Object	User or Group Role	Assignment	Role Origin
Library	Library administrator	Owner	Library
Library	Cabinet administrator	Owner	Library
Library	Organizer	Owner	Library
Library	Publisher	Owner	Library
Library	All assignable roles[1], not modified	Member	Group
Library	All assignable roles, modified	Member	Library

[1] All assignable roles include Library administrators and lower roles.

7.4.6. Group Effective Role

List of groups matching effective role taken from list of groups used to compute highest role. If the role is Owner and the membership type is Direct there is no group.

Example 1, user is a member of GroupA (Document Publisher), GroupB (Organizer), and GroupC (Document Publisher). User is directly a member of Folder1. The effective role is Organizer and the group is GroupB.

Example 2, same user as example 1. GroupB is a member of Folder2 with reduced role to Document Publisher. The effective role is Document Publisher and the group is GroupB.

Example 3, same user as example 1. GroupA and GroupC are members of Folder3. Effective role is Document Publisher and the groups are GroupA and GroupC.

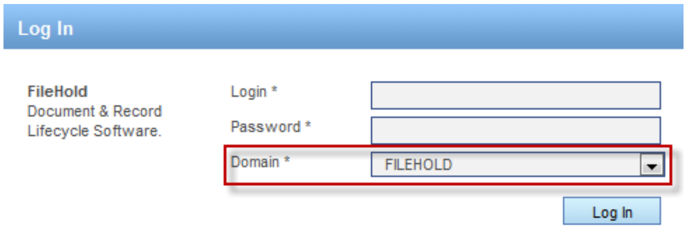
Example 4, user is a member of GroupD (Cabinet administrator). GroupD is owner of Cabinet1. Effective role for user is Cabinet administrator and the group is GroupD.

8. SYSTEM CONFIGURATION: GENERAL SETTINGS

In the general 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.

8.1. SETTING THE DEFAULT DOMAIN

Active Directory integration is an optional component of FileHold, and allows you to add Active Directory domain users to FileHold. When a domain user (user account that 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.



Log In

FileHold
Document & Record
Lifecycle Software.

Login *

Password *

Domain * FILEHOLD

To set the default domain

1. Go to **Administration Panel > System Configuration > 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**.

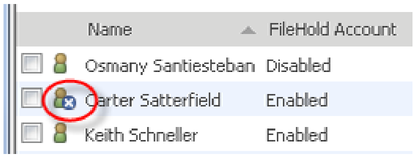
8.2. REMOVING LICENSES FROM DISABLED USERS IN THE DOMAIN

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. In the Web Client, go to **Administration Panel > System Configuration > 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.

   When a user has been disabled in the domain, the user icon will appear as follows in the Users List:



Name	FileHold Account
Osmany Santiesteban	Disabled
Carter Satterfield	Enabled
Keith Schneller	Enabled

8.3. 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. Setting the outbound email settings allows user to receive alerts and reminders on folders and documents via email. Alert settings for users can be set in File > Preferences & Settings > Alert Preferences from the FileHold Desktop Application.

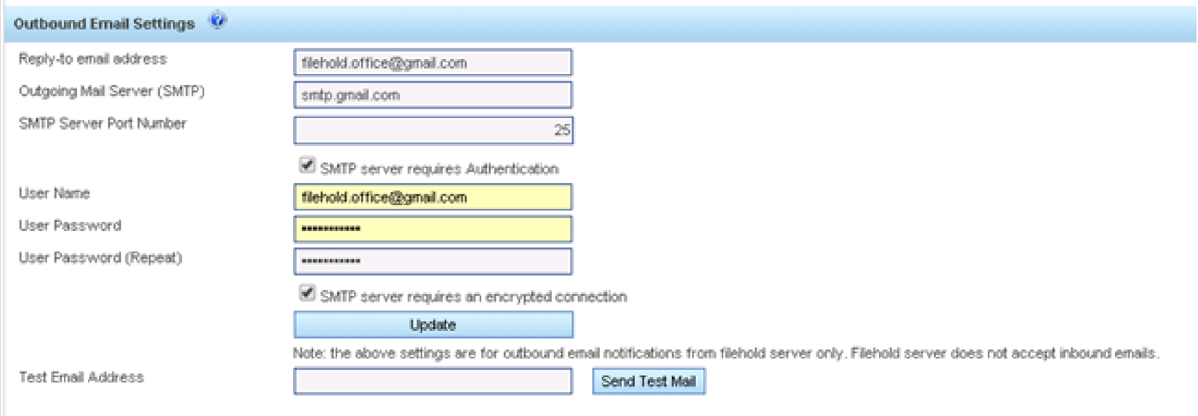
You may need to create an email account on your email server in order for FileHold to use this feature.

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 **Administration Panel > System Configuration > 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.



Outbound Email Settings

Reply-to email address	filehold.office@gmail.com
Outgoing Mail Server (SMTP)	smtp.gmail.com
SMTP Server Port Number	25
	☑ SMTP server requires Authentication
User Name	filehold.office@gmail.com
User Password	•••••••••••••
User Password (Repeat)	•••••••••••••
	☑ SMTP server requires an encrypted connection
	Update
	Note: the above settings are for outbound email notifications from filehold server only. Filehold server does not accept inbound emails.
Test Email Address	Send Test Mail

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.

8.4. 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 **Administration Panel > System Configuration > 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**.

8.5. 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, go to **Administration Panel > System Configuration > General**.
2. n the Document Shortcuts area , do one of the following:

- To enable document shortcuts, select the check box.
- To disable document shortcuts, clear the check box.

8.6. ENABLING 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**.

8.7. 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. In the Web Client, go to **Administration Panel > System Configuration > General**.
2. In the Event Schedule Settings area, select the following check boxes, if applicable:
   - Enable Convert to Record Events —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**.

8.8. 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.

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. In the Web Client, go to **Administration Panel > System Configuration > 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.

8.9. 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.

8.10. 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.

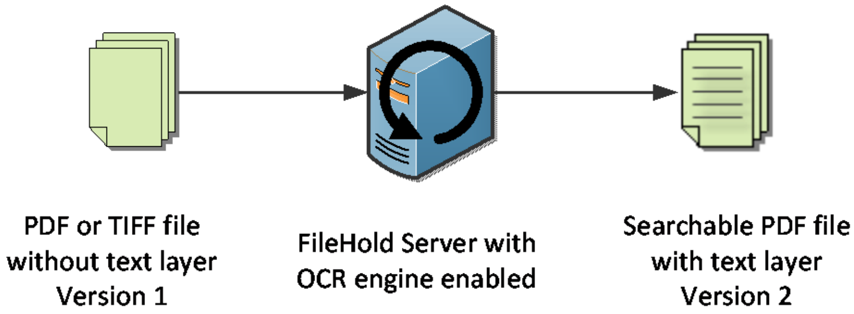
Server side OCR can be a time consuming mechanism; therefore, documents are added to a queue to be processed. All new documents, new versions, manually added or through an automatic import mechanism (such as watched folders or managed imports), are automatically added to the queue. Existing repository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

9. SYSTEM CONFIGURATION: SECURITY

In the System configuration > Security area, you can set timeout value, logon attempt value, set the password policy for local users, and enable self-registration.

9.1. LOGON 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.

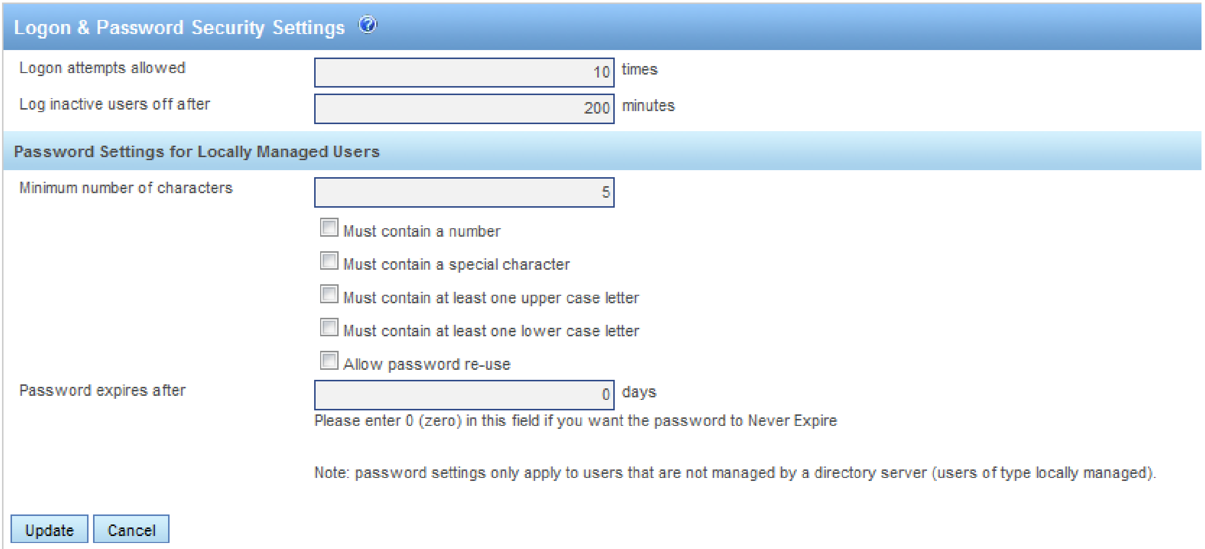
The password settings **only** apply to FileHold locally managed users and not domain users synchronized with Active Directory. Domain user policies are defined by the Active Directory security policy defined by your organizations IT group.

TO SET THE LOGON AND PASSWORD SECURITY SETTINGS

1. Go to **Administration Panel > System Configuration> Security> Logon**.

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. You will need to enable their account in order to gain access to the system.
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.

   TIP: There is an additional timeout for web client users to conserve memory. By default, after 15 minutes, the web client state will be purged from the server. The user will receive a message that they were timed out, but they can return to their session by clicking on the supplied link. They will not be required to login unless they have exceeded the inactivity time. The default value of the timeout can be changed on the server in the web client web.config file. The value to edit is ViewStateCacheLifetime, which is found in the <appSettings> section. As the view state cache requires memory on the server, increasing the value may increase the server memory usage.
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).

7. Click **Update**.

9.2. 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:

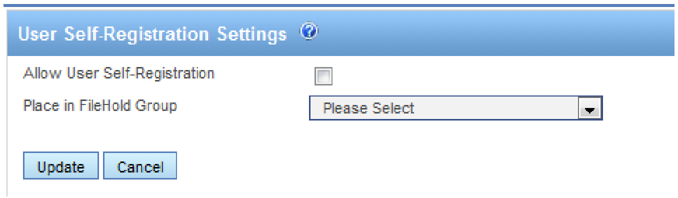
- The system is being deployed for the general public and user registration needs to be self-serve.
- The system is being used by an organization that does not have or plan to use Active Directory to manage the users. This provides access while limiting administrator burden to create user accounts.
- 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. In the Web Client, go to **Administration Panel > System Management > Permissions > Groups**.
2. Create a new group for the self-registered users. See Creating FileHold Groups for more information.
3. Go to **Administration Panel > System Configuration> Security > Self-Registration**.



User Self-Registration Settings

Allow User Self-Registration ☐

Place in FileHold Group: Please Select

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).

10. DOCUMENT VIEWER CONFIGURATION

You can configure the features of the viewer that is available to users when they are using the FileHold Desktop Application (FDA). Viewers have many user features and many benefits that increase productivity and save companies money. Viewers are purchased on a per user basis and assigned to registered users by the IT administrator.

There are 2 viewer types available:

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

   For a complete list of file formats that are supported, see the Knowledge Base.

TO CONFIGURE THE VIEWER SETTINGS

1. In the Web Client, go to **Administration Panel > System Configuration > Document Viewers (FDA)**.
2. Select a viewer type and select one or more of the following options. The type and level of viewer determines which settings are available. Not all settings are available in all viewer types.
   - Allow Users To Compare Documents
   - Allow Users To Publish Documents As Adobe PDF Files
   - Allow Users To Publish Documents As TIFF Files
   - Allow Users To Publish Documents As CSF Files
   - Allow Users To Save View In JPEG Format
   - Allow Users To Print / Print Regions Of Documents
   - Allow Users To Create ISO Banners / Watermarks For Printing
   - Allow Users To Copy Text and Markups In A Document To The Clipboard
   - Allow Users To Copy Regions Of Image Files To The Clipboard
   - Allow Users To View / Create / Edit Markups
   - Allow Users To Publish Documents As Dwf Files
   - Allow Users To Show Or Hide Layers
   - Enable Measurement Tools For Users
   - CAD File Path References For Viewing Of CAD files
   - Enable Document Redaction (The redaction module is an optional feature. Contact sales@filehold.com for more information)
3. To select all the options, click **Check All**.
4. To remove the selections, click **Uncheck All**.
5. Click **Save**.

11. DOCUMENT 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.

IMPORTANT #1: Do not use File/folder compression on the FileHoldData directory, DocumentRepository folder structure, FullTextSearch folder structure, or the FHURMBackups folder structure.

IMPORTANT #2: 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.

VERY IMPORTANT: End users should never have access to the document repository locations for any reason - this is a location that only domain / data backup / Server administrators should have access to, along with the FileHold service account that runs the entire FileHold system. It is the responsibility of each FileHold customer to secure the DocumentRepository path, along with the FileHoldData path so that end users are not able to directly modify documents. The Desktop Client and Web Client are to be used at all times. Failure to protect the document storage or other areas of the FileHoldData directory, including Full text search and FHURMBackup folder(s) may void FileHold warranty and result in consulting charges to attempt to repair damage. The FileHold data directory that typically contains DocumentRepository, FullTextSearch and FHURMBackup folders and file contents must be backed up nightly, along with the four (4) or five (5) SQL Databases and four (4) or five (5) SQL Log files that comprise the FileHold system. Please refer to the FileHold backup and recovery guide located here for more information on backups.

TO ACCESS THE REPOSITORY LOCATIONS

1. In the Web Client, go to **Administration Panel > System Configuration > Document 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.

Field Name	Description
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.

TO CHANGE THE THRESHOLD OF THE REPOSITORY

1. Go to **Administration Panel > System Configuration > Document 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**.

For example: For a 20% reserve in a repository that has the capacity of 39.90 GB, you can set the threshold to 8172 MB (39.90 GB x 20% x 1024 MB/GB).

TIP: The less data a disk has on it, the faster it will operate. This is because on a well defragmented drive, data is written as close to the outer edge of the disk as possible, as this is where the disk spins the fastest and yields the best performance. Disk seek time is normally considerably longer than read or write activities. As noted above, data is initially written to the outside edge of a disk. As demand for disk storage increases and free space reduces, data is written closer to the center of the disk. Disk seek time is increased in locating the data as the head moves away from the edge, and when found, it takes longer to read, hindering disk I/O performance. This means that monitoring disk space utilization is important not just for capacity reasons but for performance also. As a rule of thumb, work towards a goal of keeping disk free space between 20% to 25% of total disk space. If free disk space drops below this threshold, then disk I/O performance will be negatively impacted. (Source: MSDN (link is external))

12. 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 General settings page.

12.1. 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 **Administration Panel > 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

Option	Values	Default Value
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.

12.2. 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 **Administration Panel > 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

Option	Values	Default Value
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
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.

12.3. 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 **Administration Panel > 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
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.

12.4. 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 **Administration Panel > 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
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

Option	Description	Values	Default Value
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.

12.5. 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 **Administration Panel > 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

Option	Values	Default Value
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
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

Option	Values	Default Value
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
Orientation of the thumbnail view - determines the location of the thumbnail position when using the PDF/Image viewer	Top Bottom Left Right	Bottom

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.

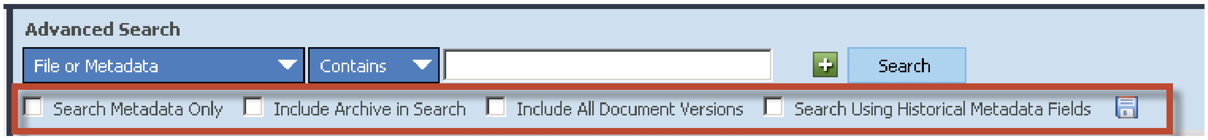
4. To reset the value for all users, click the **Reset** button next to the option name. At the prompt message, click **OK**. The settings will take effect the next time the user logs into FileHold.

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.

12.6. 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.


Advanced Search
File or Metadata
Contains
Search
☐ Search Metadata Only
☐ Include Archive in Search
☐ Include All Document Versions
☐ Search Using Historical Metadata Fields

To set the global Advanced Search options

1. In the Web Client, go to **Administration Panel > 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

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