FileHold

Document & Record Lifecycle Software

System Administration Guide

version 16.3

For further information about this manual or other FileHold Systems products, contact us at 3010 Boundary Road Office #2H, Burnaby, British Columbia, Canada, V5M 4A1, via email sales@filehold.com, our website http://www.filehold.com, or call 604-734-5653.

Proprietary Notice

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

TABLE OF CONTENTS

1. OVERVIEW

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 client options
- Enable viewer features
- Set Microsoft® SQL Report permissions
- View the document repository locations
- View the dashboard
- View the full text search settings

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 are accessing the document management system, group these users into logical groups, and provide a descriptive name for the groups. A descriptive group name makes more sense to you or to other administrator's 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 is 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 organization's 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 need to evaluate the users of the system and group them into logical groups, such as Accounting, Marketing, Sales, and so on. You 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
- License information

You 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.

TIP: If multi-factor authentication has been configured for the system, you need to authenticate your login through Duo. See Multi-factor Authentication for details.

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 **Administration > Full Administration menu** at the top of the screen. Once logged in, the different areas of the system administration and Library Administration features 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 > **Web administration panel**.

To log out from the Web Client

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

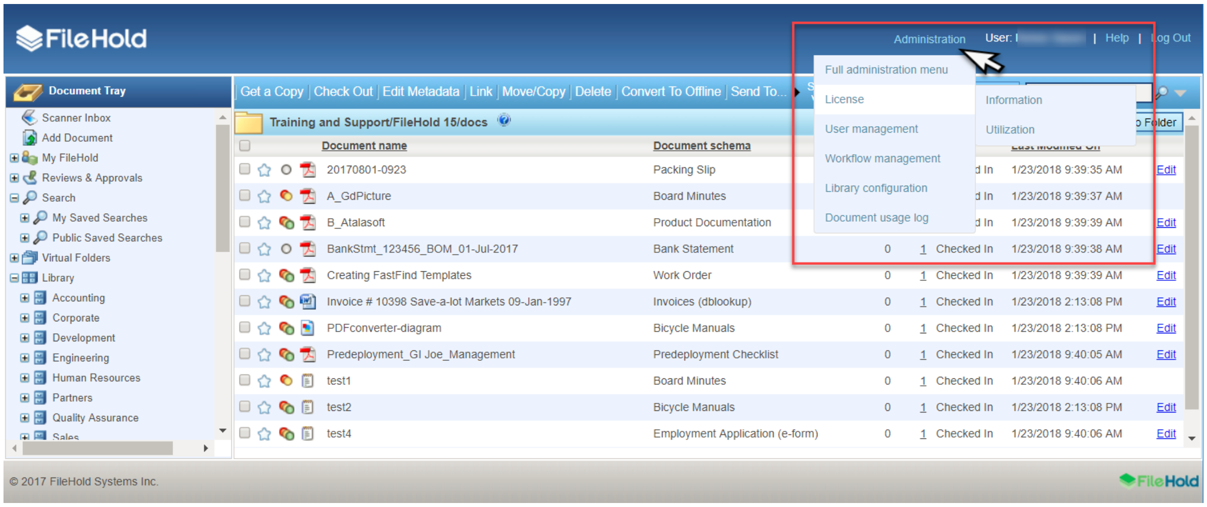
To log out from the FDA

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

3. WEB CLIENT ADMINISTRATION MENU

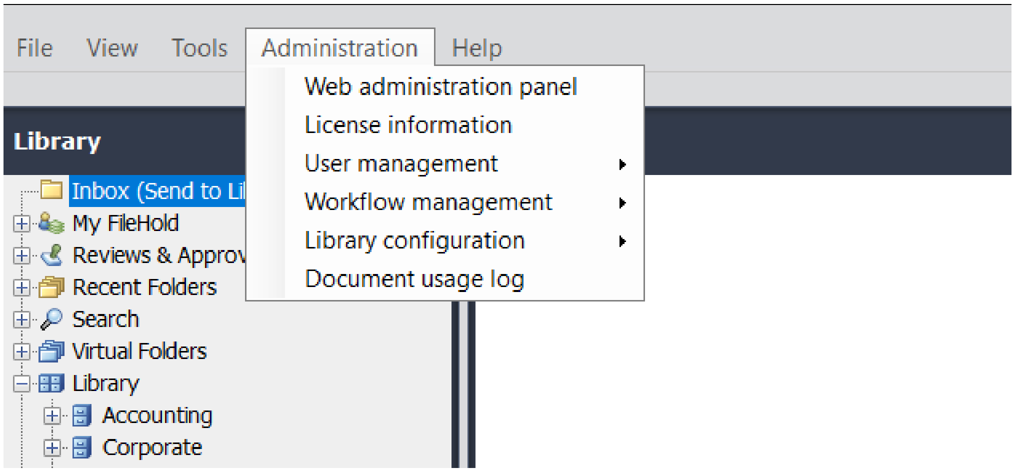
The administrative functionality in FileHold is only available to those users with sufficient administrator rights.

Some frequently accessed system administration and library administration functionality can be found under the Administration menu for both the Web Client and FileHold Desktop Application (FDA). This provides quick easy access to specific administrative functionality without the need to leave or lose the information on the current library screen.



Document name	Document schema					
20170801-0923	Packing Slip			d In	1/23/2018 9:39:35 AM	Edit
A_GdPicture	Board Minutes			d In	1/23/2018 9:39:37 AM	
B_Atalasoft	Product Documentation			d In	1/23/2018 9:39:39 AM	Edit
BankStmt_123456_BOM_01-Jul-2017	Bank Statement	0	1	Checked In	1/23/2018 9:39:38 AM	Edit
Creating FastFind Templates	Work Order	0	1	Checked In	1/23/2018 9:39:39 AM	Edit
Invoice # 10398 Save-a-lot Markets 09-Jan-1997	Invoices (dblookup)	0	1	Checked In	1/23/2018 2:13:08 PM	Edit
PDFconverter-diagram	Bicycle Manuals	0	1	Checked In	1/23/2018 2:13:08 PM	Edit
Predeployment_GI Joe_Management	Predeployment Checklist	0	1	Checked In	1/23/2018 9:40:05 AM	Edit
test1	Board Minutes	0	1	Checked In	1/23/2018 9:40:06 AM	
test2	Bicycle Manuals	0	1	Checked In	1/23/2018 2:13:08 PM	Edit
test4	Employment Application (e-form)	0	1	Checked In	1/23/2018 9:40:06 AM	Edit

Web Client Administration menu



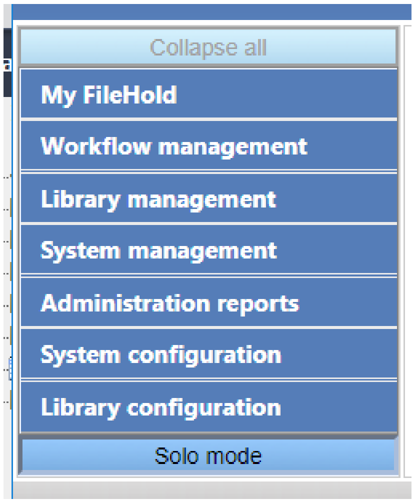
FileHold Desktop Application Administration menu

The full administration menu can be accessed:

- In the Web Client, click **Administration** and select **Full administration menu**
- In the FDA, from the Administration menu, select **Web Administration Panel**.

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

In the Administration panel, a setting called **Solo Mode** can be enabled so only one section of the Administration panel expands 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:

- System management > User Management > Users
- System management > User Management > Groups
- System management > License > Information
- System management > License > Utilization
- Administration reports > User activity
- Administration reports > System audit log
- Administration reports > Insufficient sessions
- Administration reports > Effective permissions
- Administration reports > Search performance log
- Administration reports > Courier usage log
- System configuration > Settings > General
- System configuration > Settings > Search
- System configuration > Settings > Document viewers
- System configuration > Settings > Custom reports
- System configuration > Settings > Export scripts
- System configuration > Security > Logon
- System configuration > Security > Self registration
- System configuration > Document repository locations
- System configuration > Client options > Alert preferences

- System configuration > Client options > Workflow preferences
- System configuration > Client options > FastFind preferences
- System configuration > Client options > Misc preferences
- System configuration > Client options > FDA preferences
- System configuration > Client options > Advanced search options
- Library configuration > Settings > Workflow. See the *Workflow and Courier Guide* for more information.

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 documents.

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
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

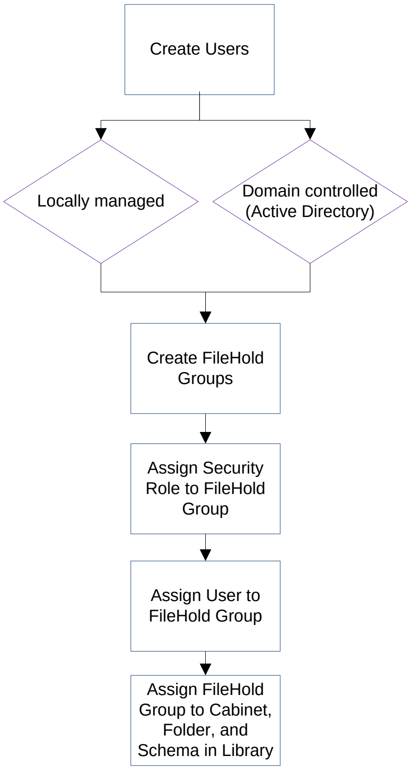
WARNING: System administrators should be very careful about which users/groups receive delete permissions. Remember that it is easier to mark or flag files for deletion than it is to recover and restore them from the IT Enterprise backup system.

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 has 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. REGISTERTED USER ACCOUNTS

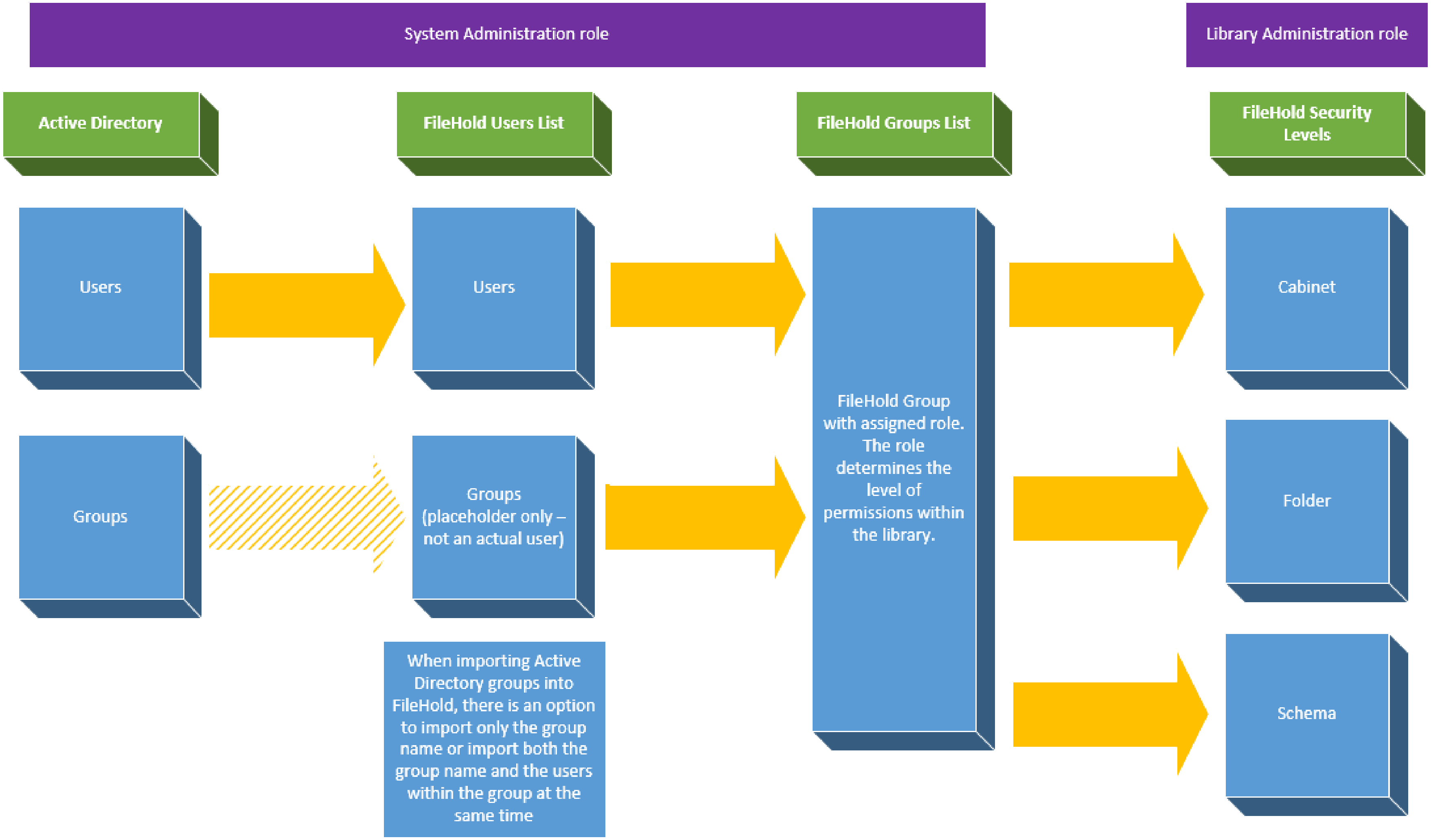
Each user accessing FileHold requires a registered user account. FileHold has multiple ways of ensuring user account authentication and authorization of resources:

- 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.
- Multi-factor authentication with Duo

Granular roles-based security allows the system administrator to quickly control the exact level of access a group of users 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 schema. Security can be configured at multiple levels so documents can even be stored in the same folder yet carry differing permissions of access.

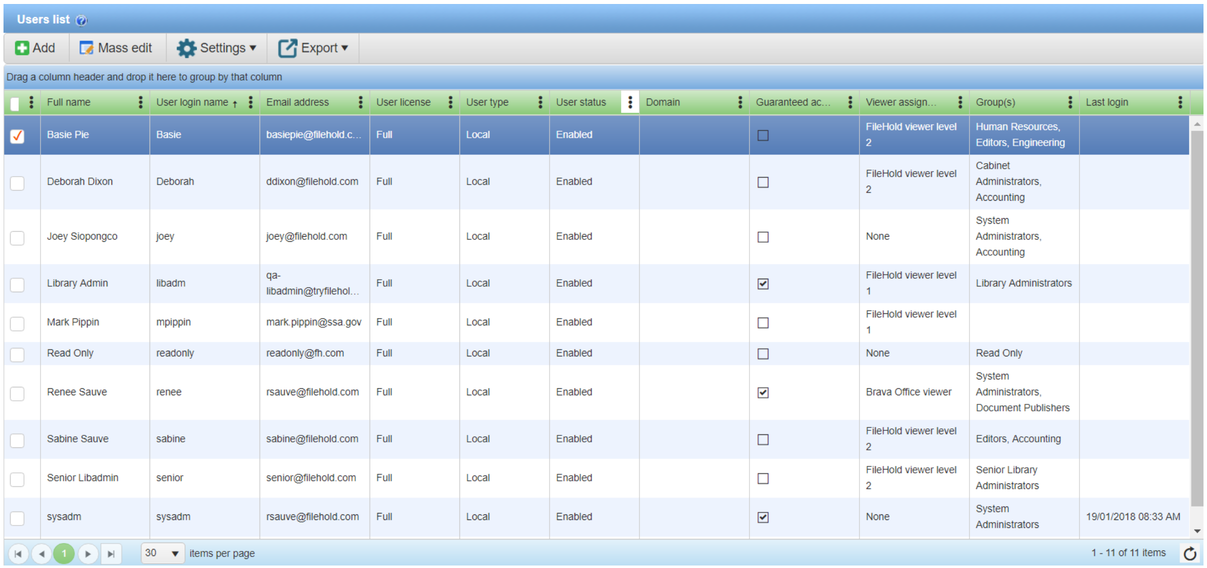
There are two types of user accounts: Locally Managed Users and Active Directory Synchronized Users. Both types of accounts can co-exist on the same FileHold Server.

- 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. 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. When importing Active Directory groups into FileHold, you have the option to bring just the group name or all the users within the group. Benefits of using Active Directory are: single sign-on, synchronization of FileHold with the domain, and the use of Active Directory groups with FileHold Groups. See the following diagram for a high-level overview of the process.


System Administration role
Library Administration role
Active Directory
FileHold Users List
FileHold Groups List
FileHold Security Levels
Users
Users
Groups
Groups (placeholder only – not an actual user)
FileHold Group with assigned role. The role determines the level of permissions within the library.
Cabinet
Folder
Schema
When importing Active Directory groups into FileHold, there is an option to import only the group name or import both the group name and the users within the group at the same time

4.2.1. Users list

The list of users is accessible in the Administration Panel in the Web Client under **System Management > User Management > Users**. The Users list page is where you create and manage all of your users of FileHold. Anyone accessing FileHold requires a user account.


Users list

Add | Mass edit | Settings ▾ | Export ▾

Drag a column header and drop it here to group by that column

□	Full name	User login name ↑	Email address	User license	User type	User status	Domain	Guaranteed ac...	Viewer assign...	Group(s)	Last login
☑	Basie Pie	Basie	basiepie@filehold.c...	Full	Local	Enabled		□	FileHold viewer level 2	Human Resources, Editors, Engineering	
□	Deborah Dixon	Deborah	ddixon@filehold.com	Full	Local	Enabled		□	FileHold viewer level 2	Cabinet Administrators, Accounting	
□	Joey Siopongco	joey	joey@filehold.com	Full	Local	Enabled		□	None	System Administrators, Accounting	
□	Library Admin	libadm	qa-libadmin@tryfilehol...	Full	Local	Enabled		☑	FileHold viewer level 1	Library Administrators	
□	Mark Pippin	mpippin	mark.pippin@ssa.gov	Full	Local	Enabled		□	FileHold viewer level 1		
□	Read Only	readonly	readonly@fh.com	Full	Local	Enabled		□	None	Read Only	
□	Renee Sauve	renee	rsauve@filehold.com	Full	Local	Enabled		☑	Brava Office viewer	System Administrators, Document Publishers	
□	Sabine Sauve	sabine	sabine@filehold.com	Full	Local	Enabled		□	FileHold viewer level 2	Editors, Accounting	
□	Senior Libadmin	senior	senior@filehold.com	Full	Local	Enabled		□	FileHold viewer level 2	Senior Library Administrators	
□	sysadm	sysadm	rsauve@filehold.com	Full	Local	Enabled		☑	None	System Administrators	19/01/2018 08:33 AM

The default columns displayed are:

Column Header	Description
Full name	First and last name of the user.
User login name	The login name of the user.
Email address	The email address of the user. This is the email account that the FileHold notification emails are sent to.
User status	Enabled or disabled.
User license	Full, Limited Registered user, or Portal alias user. • A Full user license is a user that has been assigned to a group with a role of read-only or higher. Full users consume the full concurrent sessions. • A Limited Registered user is a user that has been assigned to a group with a role of Limited. A single limited registered user account can be used by a single user or shared amongst many people. Limited registered users consume the limited concurrent sessions. • A Portal alias user is a user that has been assigned to a group with the role of Limited and is used in conjunction with the Anonymous portal. Portal alias users consume the limited concurrent sessions. For more information on limited registered or portal alias users and the anonymous portal, see the Knowledge Base.
User type	• Local user • Domain user • Domain group – This is just a placeholder for a domain group and does not use up a user license.

Column Header	Description
Domain	The domain that the user belongs to if a domain user or group. If a local user, the domain is blank.
Guaranteed access	A concurrent session is dedicated to a user.
Viewer assignment	A FileHold viewer level 1, FileHold viewer level 2, FileHold viewer level 3, Brava Office viewer, Brava Office viewer CAD, Brava Office viewer Engineering, or None. *Starting in 2017, Brava viewer licenses are no longer available for new purchases. This information is retained for existing users only.* For more information on how to use the viewers, see the Knowledge Base.
Web scanning	WebCap scanning license is assigned.
Group(s)	The name of the group(s) the user is assigned to.
Inherited groups	Displays the name of any FileHold groups that have a domain group assigned to it and the user is a member of.
Last login	The last time the user logged in.

Other columns that can be displayed are: last modified date, street, PO Box, city, state/province, zip/postal code, country/region, work, mobile, home, page, instant messenger, IP phone, fax, title, company name, department, office, division, web page, and notes.

Edits to the user properties can be changed for some of the displayed columns directly in the Users list. For example, you can change the user's status, viewer level, guaranteed access, and web scanning license.

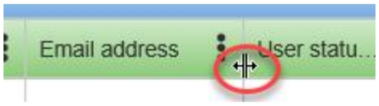
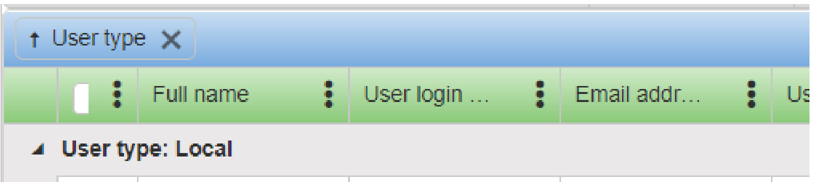
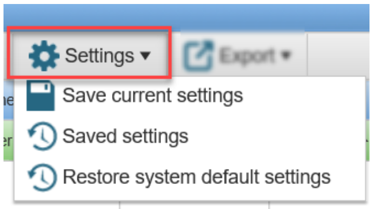
TO EDIT DIRECTLY IN THE USERS LIST

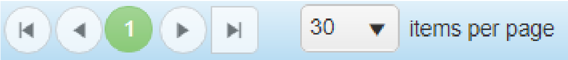
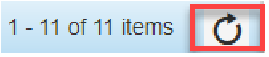
1. Click in the cell for the user property that you want to change.
2. Change the property.
3. If the property cannot be changed in the Users list view, simple double-click on the row and you can edit the full user properties. See Creating Locally Managed Users for more information.

4.2.2. How to manipulate the Users List view

The users list can be modified to add or remove columns, resize or change the order of the columns, sort ascending or descending, filter the results, and save these different views. The displayed information can be exported out of the system in order to do further analysis on user accounts.

Function	Description
Sort ascending/descending	Click on the column header to sort ascending or descending. Alternatively, click ⋮ in the column header and select **Sort Ascending** or **Sort Descending**. An up or down arrow shows in the column header indicating the sort order.

Function	Description
Add or remove columns	Click ⋮ in the column header and select **Columns**. Select the check boxes for the columns to be displayed. Clear the check boxes to remove the header.
Resize columns	Hover the cursor between the column headers to resize a column. 
Filter	Click ⋮ in the column header and select Filter. Select the filter options and click **Filter**. The filter options available depend on what type of column is selected. A white filter icon ⋮ is shown in the header if the column is being filtered. To clear the filter, go to **Filter** and click **Clear**.
Multi-select users for mass edit	Use **Shift** or **Ctrl** keys on your keyboard.
Change column position	Drag and drop columns to the desired position.
Group by a column	Drag and drop a column header to top blue bar that says "Drag a column header and drop it here to group by that column". To remove the grouping, click the **X** next to the header name in the blue bar.  User type Full name User login … Email addr… Us User type: Local
Save view settings	If the view is modified, the view can be saved for reuse. Click **Settings > Save**. Enter a view name and click **OK**. To use a saved view, go to **Settings > Saved Settings > *<view name>*.** To delete a saved view, go to **Settings > Saved Settings > *<view name* > Delete**. To restore to the default view, go to **Settings > Restore system default settings**.  Settings Export Save current settings Saved settings Restore system default settings

Function	Description
Scroll through pages	In the bottom left corner, use the scroll settings to: - Go to first page - Go to previous page - Go to next page - Go to last page Adjust the number of items per page: 15, 30, 60 
Refresh screen	Click **Refresh** in the bottom right corner. 

4.2.3. Creating Locally Managed Users

A locally managed user is a user account that is created and managed, including passwords, 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 > User Management > Users.**
   - Alternatively, in FDA, log in with system administrator rights and go to **Administration > User & Group Management > Users**.
2. Click **Add** ➕ Add.
3. Select **Locally Managed User** and click **Next**.
4. In the User license page, the Authentication method: Local is displayed.
5. Select the User license type: Full, Limited, or Portal alias.
   - A Full user license is a user that has been assigned to a group with a role of read-only or higher. Full users consume full concurrent sessions.
   - A Limited registered user is a user that has been assigned to a group with a role of Limited. A single limited registered user account can be used by a single user or shared amongst many people. Limited registered users consume limited concurrent sessions.
   - A Portal alias user is a user that has been assigned to a group with the role of Limited and is used in conjunction with the Anonymous portal. Portal alias users consume limited concurrent sessions. For more information on portal alias users and the anonymous portal, see the Knowledge Base.
6. In the General page, fill in the following information and click **OK**:
   - First Name

- Last Name
- User Logon Name
- Email
- Default Language
- Time Zone – Select the time zone for the user. See Miscellaneous Preferences for more information.
- Short date format – Set the short date format for the user. See Miscellaneous Preferences for more information.
- Long date format – Set the long date format for the user. See Miscellaneous Preferences for more information.
- Short time format – Set the short time format for the user. See Miscellaneous Preferences for more information.
- Long time format – Set the long time format for the user. See Miscellaneous Preferences for more information.
- Source — Locally managed user account (cannot be edited)
- Initials – See Displaying Middle Initial with User's Full Name for more information.

7. In the Account Settings page, enter the following information under the General account settings area:

- 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.
- 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.
- Send activation email — Select this check box in order to send the new user an email containing a link to activate their user account. Enter an additional information for the user in the text box. If this option is enabled, the "User must change password at next logon option" is disabled. This option is not available after a user account has been created. For additional configuration for the subject line and contact email address on the notification email, see Logon Security.
- Exclude user from multi-factor authentication — If multi-factor authentication (MFA) has been enabled for the system, the user can be excluded from having to use it to log into FileHold. By default, the check box is disabled. See Logon Security for more information.

TIP: There are cases where a headless technical user is required, such as using the API, so there is no person to complete an MFA challenge. Technical users should take care to configure such clients in a secure, safe manner.

8. In the License Options Assignment area, select the viewer license for the user. By default, the user is assigned a FileHold viewer level 1 license. For detailed information about the viewers and their functionality, see the FileHold Knowledge Base.

- None
- FileHold viewer level 1
- FileHold viewer level 2
- FileHold viewer level 3

9. Select the **Web scanning license assignment** check box if the user is to be assigned a WebCap scanning license. For more information about WebCap, see the Knowledge Base.
10. In the Account expiration area, select an account expiration option. An account expiration date is good to use when you have contractors or temporary workers. The global password expiry is set in the System Configuration > Security > Logon page.

- Follow global policy to <never expire> *(or)* <expire in *x* days>.
- Follow global policy to expire in *x* days or, if sooner, end date of <date>.

11. In the Member Of section, add the user to a group. See Adding Users to Groups for more information.
12. In the Contact Information page, enter the user's contact information such as addresses, phone numbers, and company information. This information is optional but may be necessary for things such as two-factor authentication or workflow.
13. Enter the password for the user twice and click **OK**.
14. Click **OK**. The user is added to the list of registered users.

4.2.4. Synchronizing Microsoft Active Directory Users and Groups (Domain)

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

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

When adding domain groups, the group names can be viewed in the Users List; however, they are not using up a registered user license account. Domain groups are simply placeholders that allow you to assign them to FileHold security groups.

Domain groups can be assigned to FileHold security groups that can in turn be given access (membership) to specific content located throughout the library. Synchronization of a domain group allows 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.

When adding domain users, domain users have the option to be added with a "full user", "limited", or "portal alias" license type. When adding domain groups, proxy users can be added as "full user" or "limited" license types. If a user belongs to two domain groups and the proxy users for each group have a different license, a configuration setting determines the license type. See Changing the User License Type for Domain Proxy Users for more information. Domain group proxies can never have a portal alias license type.

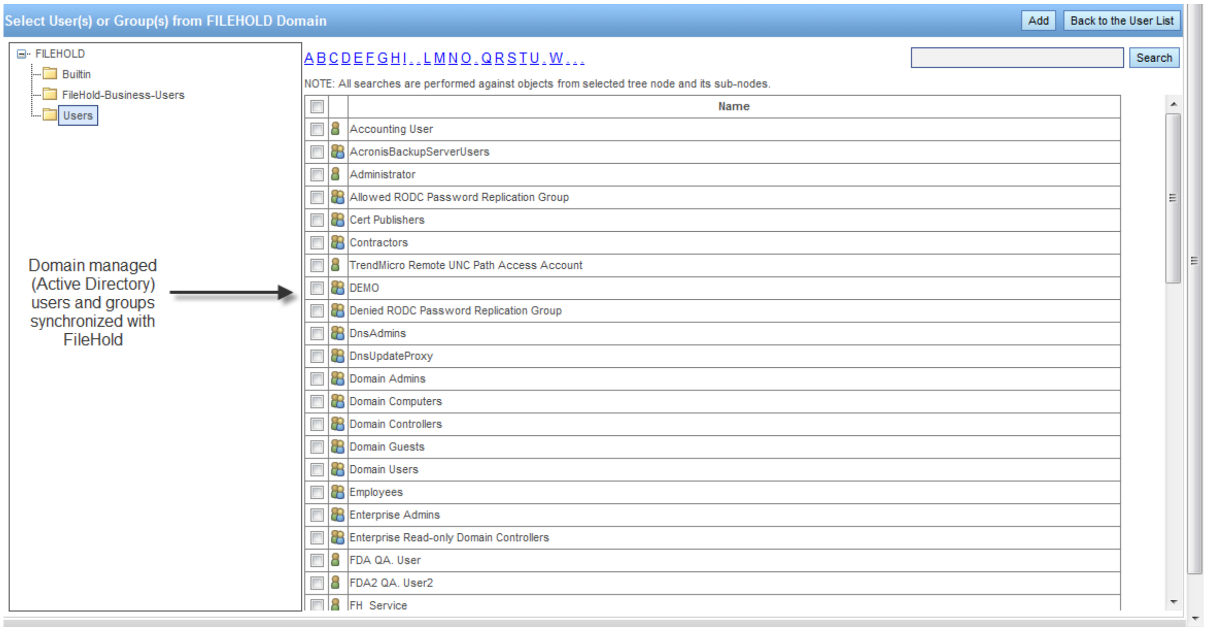
NOTE: It is important to keep in mind that some Active Directory deployments can be complex as they employ custom schemas and objects that may not be industry standard and can require additional effort to synchronize.

If you did not purchase the Active Directory option, you need to create locally managed users. You are not able to synchronize FileHold with Active Directory. To purchase the Active Directory synchronization module, 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 > User Management > Users.**
   - Alternatively, in FDA, log in with system administrator rights and go to **Administration > User & Group Management > Users**.
2. Click **Add** ➕ Add.
3. Select the domain name from the list.
4. To search for a domain user or group in the list, enter the name in the search field and click **Search**.
5. Select the check boxes for the users or groups you want to add and click **Add**.


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

6. Assign the user license type:
   - A Full user license is a user that has been assigned to a group with a role of read-only or higher. Full users consume the full concurrent sessions.
   - A Limited user is a user that has been assigned to a group with a role of Limited. A single limited registered user account can be used by a single user or shared amongst many people. Limited registered users consume the limited concurrent sessions.
   - A Portal alias user is a user that has been assigned to a group with the role of Limited and is used in conjunction with the Anonymous portal. Portal alias users consume the limited concurrent sessions.
7. If adding domain groups, select one of the following:
   - 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 is synchronized with the domain.

8. If adding domain groups, assign the user license type:
   - Full user
   - Limited
9. Click **OK**.
10. A confirmation message appears stating how many domain groups and users were added to FileHold. Click **OK.**
11. Continue to add more users and groups to FileHold.
12. To return to the user list, click **Back to the User List**.
13. To set viewer, guaranteed access, multi-factor authentication exclusions, and scanning (WebCap) licenses, select **Properties** next to the user's name and go to **Account Settings**. See Creating Locally Managed users for more information on these settings.

4.2.5. Changing the User License Type for Domain Proxy Users

Domain proxy users for domain groups allow automatic assignment of FileHold groups to users. However, this has the potential to cause a conflict if a limited user is assigned to a non-limited group. If a limited user is assigned to a not limited role or a full user is only assigned to limited role group(s) via a domain proxy user, a new web.config setting "DomainProxyUser.AutomaticUserTypeChange" in *C:\Program Files\FileHold Systems\Application Server\UserRoleManager* can determine the outcome:

- Elevate – Automatically convert the limited user to full user type and assign group if license is available. Leave user type as is if no license available.
- Lower – Automatically convert the full user to limited user type and assign group if license is available. Leave user type as is if no license available.
- Both – Elevate + Lower.
- None Do not change the user type. This is the default value.

The System audit log captures if user type was changed or if it failed due to no license or due to configuration.

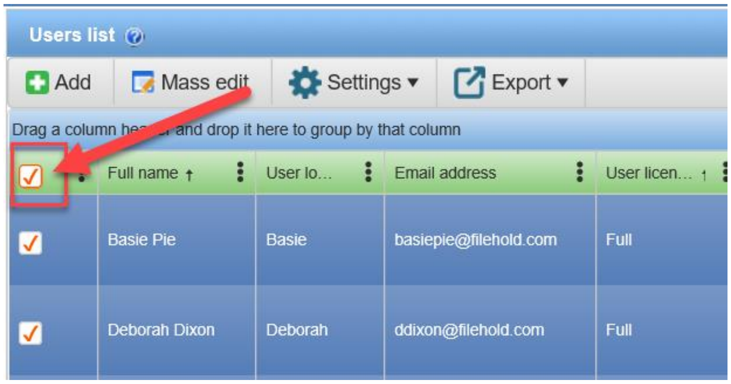
If the assignment failed or if a limited user is assigned to a full group, a notification email can be sent to system administrators according to the setting in a new web.config setting "DomainProxyUser.SendChangeWarning" in *C:\Program Files\FileHold Systems\Application Server\UserRoleManager*. When the setting is true, a notification email is sent. For example:

- *"Limited user is assigned to full group(s). No full licenses are available so they cannot be converted to full. They will not be able to log in."*
- *"Full user is only assigned to limited group(s). No limited licenses are available so they cannot be converted to limited."*
- *"Limited user is assigned to a full group. Configuration prevents them from being converted to a full user. They will not be able to log in."*

4.2.6. Mass Editing Users

The Mass Edit screen allows you to mass update a user status, delete local users, reset passwords, change user license, change viewer license, update web scanning license, and add or remove users to groups.

In order to make mass updates, users must first be selected on the Users page. Use the check boxes next to the user name or use the **Shift** or **Ctrl** keys on your keyboard to select multiple users or select the top-level check box in the check box column to select all users.



	Full name	User lo...	Email address	User licen...
✓	Basie Pie	Basie	basiepie@filehold.com	Full
✓	Deborah Dixon	Deborah	ddixon@filehold.com	Full

After you have mass edited the users, a summary page is shown summarizing the changes that were made. If sufficient licenses are available, the license count is highlighted in green. If the number is not sufficient, it is highlighted in red.

To mass edit users

1. Go to **Administration > User Management > Users**.
2. In the Users list screen, use the check boxes **Shift** and/or **Ctrl** keys to select multiple users. To select all users, select the top-level check box.

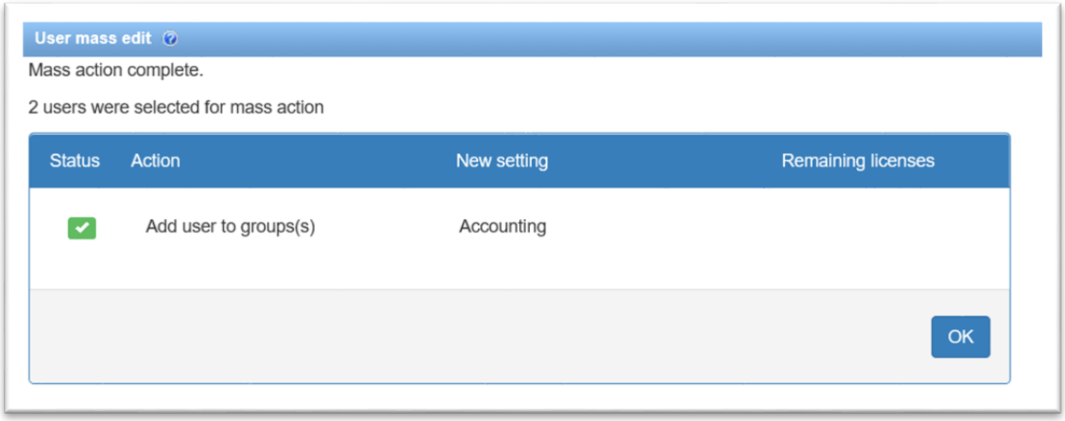
   TIP: Use the filters in the column headers to get a list of the users that require updating, then select the top-level check box to select all users.
3. Click **Mass Edit**. If sufficient licenses are available, the license count is highlighted in green. If the number is not sufficient, it is highlighted in red. You can still perform the action if there are not sufficient licenses. The following functions are available from the User mass edit screen:

Function	Description
Update user status	Enabled or Disabled When an employee joins or leaves an organization, they 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 need to enable a user account if they have exceeded the number of login attempts set in FileHold.

Function	Description
Delete user	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 needs 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.
Automatic password reset	Sends an email to selected users containing a link to reset their password. See Resetting User Passwords for more information.
Update user license	Changes the type of user license assigned to the user account. See User Roles and Accessing the Library for more information. Full – For users requiring a role of read-only or higher. Full users consume the full concurrent sessions. Limited registered – For users requiring a role of limited. Limited registered users can only be assigned to groups with the limited role. A single limited registered user account can be used by a single user or shared amongst many people. Limited registered users consume limited concurrent sessions. Portal alias – The single user account that is required to be set up to use with the Anonymous Portal. The portal alias user can only be assigned to a group with the limited role. The portal alias user consumes limited concurrent sessions. A separate portal alias account can be created for each anonymous portal. See the Knowledge Base for more information on the Anonymous Portal.

Function	Description
Update viewer license assignment	Set a viewer license for the currently selected users: • FileHold viewer level 1 • FileHold viewer level 2 • FileHold viewer level 3 • Brava Office viewer • Brava Office viewer CAD • Brava Office viewer Engineering • None *Starting in 2017, Brava viewer licenses are no longer available for new purchases. This information is retained for existing users only.* For more information on how to use the viewers, see the Knowledge Base.
Update web scanning license assignment	Select the two checkboxes to give a WebCap web scanning license for currently selected users. To clear the web scanning license, select the first check box only.
Add user to group(s)	Add currently selected users to a group. Select the group from the list.
Remove users from group(s)	Remove the currently selected users from a group. Select the group name from the list.

4. Click **Submit**.
5. A summary screen appears with a list of the actions that were completed. It may also show the number of remaining licenses, depending on the action taken or messages relating to the number of users effected by the change.


User mass edit

Mass action complete.

2 users were selected for mass action

Status	Action	New setting	Remaining licenses
✓	Add user to groups(s)	Accounting	

6. Click **OK** to return to the Users list.

4.2.7. Exporting the Users list

The Users list can be exported out to a PDF, Excel, or CSV file.

Use the filters in the column headers to filter the list, sort ascending or descending, reposition columns, or group information as all users on all pages are exported. See How to manipulate the Users List view for me information.

TO EXPORT THE USERS LIST

1. Use the filters in the column headers, move column position, sort order, and grouping to manipulate the users list. All users in the list are exported in the displayed view.
2. Click **Export** and select one of the options: PDF, Excel, or CSV.
3. Depending on your browser, you are prompted to open or save the file.

4.2.8. Displaying Middle Initial with User's Full Name

In order to see the full name and middle initial of users in the logs, users page, group members, and metadata pane, a web config file needs to be modified and a tool run in FHIT. This feature is useful when you have users with same names.

TO DISPLAY A USER'S MIDDLE INITIAL

1. Go to C:\Program Files\FileHold Systems\Application Server\UserRoleManager and open the web.config file.
2. Under <appSettings>, locate the following key and change the value from 0 (off) to 1 (on).

```
<add key="UseMiddleInitialInFullName" value="0" />
```

3. Save the web.config file.
4. Open the FH Instrumentation Tool (FHIT) and go to **Actions > Users Management** and select **Update full names**.
5. Click **Start**.
6. Enter the system administrator username and password and click **Next**.
7. Click **Update**. The status should change to "Completed successfully".
8. Click **Finish**. The user's initial now appears in the logs, users page, group members, and metadata pane.

4.2.9. 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 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 ADD OR REMOVE GUARANTEED ACCESS FOR A USER ACCOUNT

1. In the Web Client, go to **Administration > System Management > User Management > Users**.
   - In FDA, go to **Administration > User and Group Management > Users**.
2. Do one of the following:
   - Select or clear the check box in the Guaranteed Access column.
   - Right-click on a user name and select Properties. In the Account Settings page, select or clear the **User has guaranteed system access** check box.

4.2.10. Resetting User Passwords

This is only for locally managed users. You cannot reset a password for a domain user in FileHold.

You can reset a user password for:

- Individual users if they have lost or forgotten it. You can reset the password for them manually or send an email containing a link to reset their password.
- Many users using the Mass Edit button. This option sends a notification email to the selected users which contains a link that allows them to change their password. This option can be used in such situations such as after an upgrade or migration and you need to reset all local users' passwords. You can use the filter options to get the list of users whose passwords need to be reset. The time out settings for the notification email can be configured as well as a partial subject name and contact email. See Logon Security for more information. The users can click on the link provided to reset their password in the FileHold Web Client.

TO RESET A LOCAL USER PASSWORD FOR AN INDIVIDUAL

1. Go to **Administration Panel > System Management > User Management > Users** and right-click next to the user name.
   - In FDA, go to **Administration > User & Group Management > Users** and right-click on the user name.
2. Do one of the following:
   - Select **Reset Password** to manually enter a password for the user. 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.
   - Select **Automatic password reset** to send the user an email that contains a link to reset their password. The link to reset the password is time-sensitive and expires after a certain period of time. See Logon and Password Security for more information.

TO RESET A PASSWORD FOR MANY USERS

1. Go to **Administration > Full administration menu > System Management > User Management > Users** and select the check boxes for those users whose passwords needs to be changed. Use the Shift and/or Ctrl keys to multiple users. Alternatively, to reset the password for all users, click the top-level check box. You can use the filter to search for the set of users.
2. Click **Mass Edit**.

3. In the User mass edit screen, select the **Automatic password reset** checkbox and click **Submit**.
4. A summary screen appears confirming the mass update. Click **OK**.
5. An email with a link to reset their password is sent to the selected users. Once the link is clicked, they are taken to the web client to reset their password. The link must be clicked within the specified time limit or it expires. If the email timeout expires, they need to be resent the email to reset their password.

4.2.11. 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 > User Management > Users.**
   - Alternatively, in FDA, log in with system administrator rights and go to **Administration > User & Group Management > Users**.
2. Right-click on the user name and select **Properties**. Alternatively, double-click on the user name.
3. Update or view the User License, General, Account Settings, Member Of, or Contact Information for the user and click **OK**.

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*.

Groups can be restricted from performing certain functions such as emailing and initiating a Courier process. Groups with document publisher or lower roles assigned to them can have the ability to print, view or download documents disabled.

To create a FileHold group

1. In the Web Client, go to **Administration > User Management > Groups**.
   - Alternatively, in FDA, log in with system administrator rights and go to **Administration > User Management > 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.

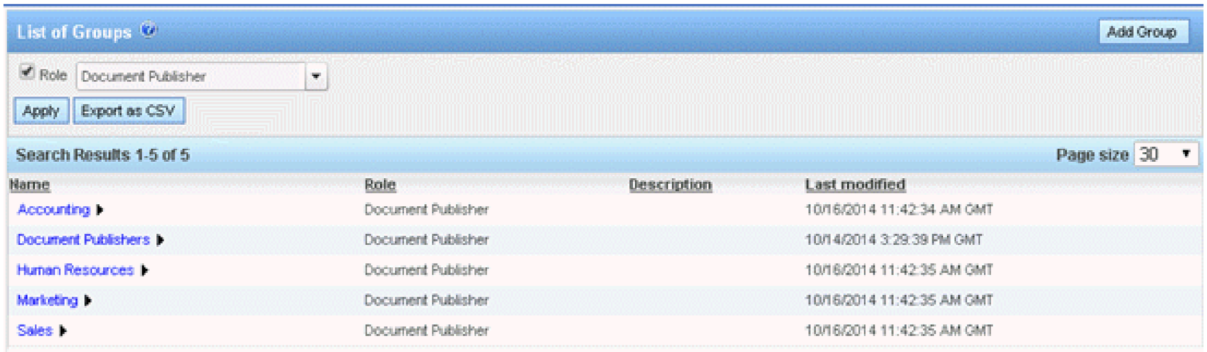
3. Enter the following information:

Field	Description
Group Name	Enter a name for the group.
Description	Enter a description for the group, if needed.
Role	Select a role from the list. See User Roles and Accessing the Library for descriptions.
Notes	Enter any additional information about the group, if needed.
FileHold Group Members	If you have a lot of members in the group, select **Display all members on one page** check box to display all the members on a single page otherwise, page numbers with members are displayed. Click **Add Members** to add users to the group. See Adding Users to Groups for more information.
Restrictions	Select the **Disable ad hoc searches** check box to prevent users from performing any type of ad-hoc search in FileHold. The only kind of searches that a user can perform are public saved searches. An administrator needs to configure these for groups that have ad-hoc searches disabled. Select the **Disable emailing documents** check box if users are not able to email documents from FileHold. Select the **Disable sending to Courier** check box to prevent users from initiating a Courier process on documents. This option is enabled by default when a group is created. This option is not available for limited and read-only groups. For document publisher and lower role groups, select the **Disable download (open, local copy)** and/or **Disable printing functions** in order to prevent them from getting a copy or printing documents. If the limited or read only user has been assigned a viewer license, the download and print functionality is also disabled in the viewer. For document publisher and lower role groups, select the **Disable viewing** to prevent users to view documents in the FileHold viewer.

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.



Document Publisher

Search Results 1-5 of 5

Page size 30

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.

All roles provide document emailing capability. Roles higher than Document Publisher have the Courier functionality. These functions can be disabled on a role by role basis by a System Administrator in the FileHold Groups area. Limited and read-only group roles can have the viewing and printing abilities restricted. See Creating FileHold Groups for more information.

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

Role Name	Description
Limited	A user assigned to a group with a “limited” role has restricted access to the system. Users can only get a copy or view documents in the library. Groups assigned to a “limited” role are used for when multiple people can share the same username and password to log into FileHold to see the same documents in the library. For example, documents such as newsletters, forms, or corporate policies may need to be accessible to all company employees but they do not require a full registered user license and full functionality. There are two user account types that can be assigned to a limited role: • Limited Registered user accounts can log into FileHold using a single username and password. • Portal Alias user account types are used in conjunction with the Anonymous portal and require no login. Using limited registered or anonymous portal user account types are a cost-effective way for many people to view documents in the repository but with very limited functionality. User accounts assigned a role of “limited” consume “Limited concurrent sessions”. Limited concurrent sessions are the number of users that can log into FileHold at the same time using a limited registered or portal alias account. For example, 30 people may have the same login credentials but only 20 can use FileHold at the same time because there are only 20 limited concurrent sessions. If multiple people log into FileHold with the same user name, the log files record the same user name regardless of the actual person that logged into the system. Groups assigned the limited role restrict users from downloading, viewing, emailing, or printing documents in the group properties.
Read Only	A Read-Only user role may only download or open and read documents from FileHold. They cannot edit, delete, or create documents. They can email documents if given this functionality by system administrators. Read-only users may be restricted from downloading, viewing, emailing, or printing documents. Read-only users can participate in workflows but cannot initiate workflows.
Document Publisher	Document Publisher user role can read, get a copy, add, check-in/check-out, edit documents, and metadata. They can move documents that are owned by them. They cannot delete any documents including those which they have added to the system. Document publishers can initiate workflows, participate in workflows, and initiate Courier transmissions. Document publishers may be restricted from downloading, viewing, emailing, or printing documents.

Role Name	Description
Document Publisher + Delete	Document Publisher Plus Delete user role can do everything a Document Publisher can do and delete their own documents. They must be the owner of the document in order to delete it. To see the owner of a document, you can look at the version properties in the metadata pane.
Publisher	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 is owned by them and they cannot change the ownership.
Publisher + Delete	Publisher plus Delete user role can do everything that a Publisher can do plus delete documents, folders and folders group owned (created) by them.
Organizer	The Organizer role is for users who are responsible for organizing documents that are scanned or imported into the system or who are assigned to organize documents added by other users. For example, organizers would move the documents generated by scanner operators to their correct folder in the library. Only trusted personnel should be given this role. Organizer role user can: • Move all documents (which they have an access to) in other places in the library including documents which they do not own. In other words, they can move documents that are owned by other users. • Move, copy or clone all folders and folder groups regardless of their ownership. In case of cloning, they 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 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 cannot 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 are 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.

4.4. ADDING USERS TO GROUPS

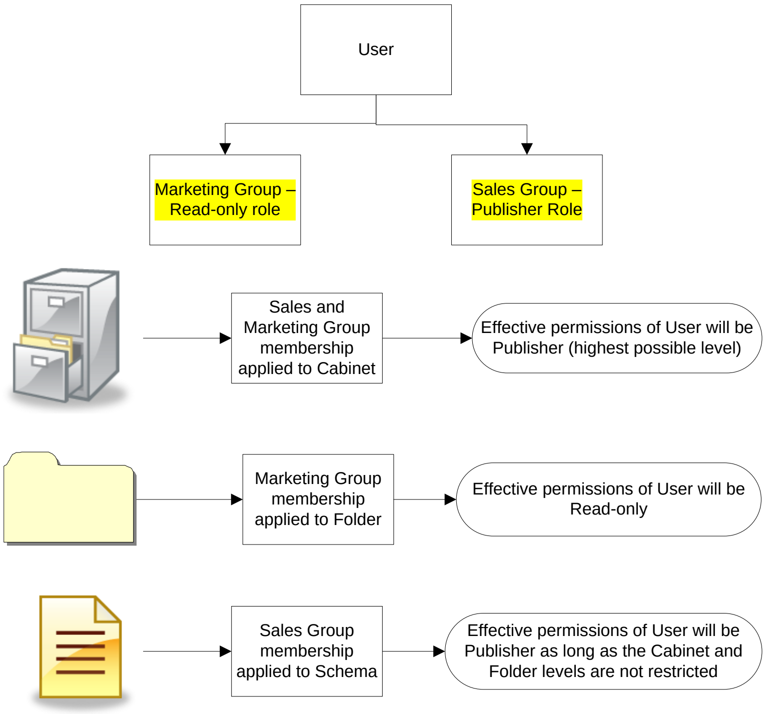
Once the users are in the system, you can add them to FileHold groups. Users can be assigned to an unlimited number of groups and groups can contain one or more users.

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 users from the User list and clicking Mass Edit.
- Selecting the user properties in the Users list.
- 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.
- Adding users to a group en masse

When users belong to more than one FileHold group they inherits 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 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 has only read-only rights. If only the Sales group is assigned to folder, then the user has 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

Effective permissions for a user in a particular area of the library or schema can be viewed in the Effective permissions report.

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

1. Go to **Administration > User Management > Users.**
2. Double-click on a user name.
3. In the User Properties, click **Member Of**.
4. In the FileHold Groups this user is a member of list, click **Add User to Group**.
5. 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 > User Management > Groups** and select **Add Members** from the drop-down menu on the group name.
2. In the Find People window, enter the first or last name of the user and/or the email address and click **Find Now**.
3. In the Results of People Search area, select the check box next to the user name(s) and click **Select User(s)**. The user is added to the group.

TO ADD USERS TO GROUP USING THE GROUP PROPERTIES

1. Go to **Administration > User Management > Groups** and select **Properties** from the drop-down menu on the group name.
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.

TO ADD USERS TO A GROUP EN MASSE

See Mass Editing Users for more information.

4.5. VIEWING GROUP PROPERTIES

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

TO VIEW GROUP PROPERTIES

1. Go to **Administration > User Management > 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.
2. Update or view the group name, description, role, notes, group members and restrictions for the user and click **OK**.

4.6. DELETING GROUPS

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

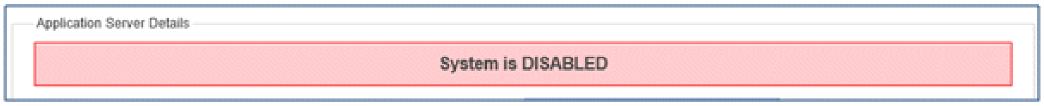
TO DELETE A GROUP

1. Go to **Administration > User Management > 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. A warning message is displayed about deleting the group. Click **OK** to delete the group.

5. LICENSING

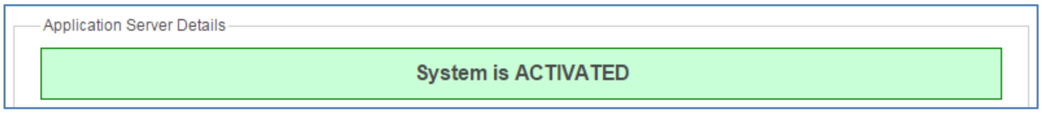
The License information page displays a summary of all the enabled features, number of registered user licenses, number of concurrent sessions, number of viewers, the software version, hardware key, and other information pertaining to the license. The date the license was issued and the license time limit is also shown.

In the Application Server Details area, a status is shown if the system is activated, deactivated, or disabled. If the system is deactivated, you have 7 days from the deactivation date to request a new license. See License Expiration Grace Period for more information.



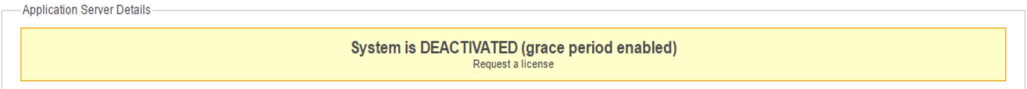
Application Server Details

System is DISABLED



Application Server Details

System is ACTIVATED

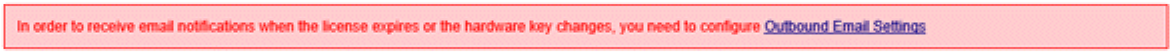


Application Server Details

System is DEACTIVATED (grace period enabled)

Request a license

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

The following table describes the server details of the licensing page.

Field	Description
Application Server Details	
System Version	The version of application server that is installed.
Build	The current build number of FileHold. See FileHold Software Versions for more information.
Machine name	Name of the server that FileHold is installed on.
Domain name	Name of the domain(s) that is synchronized with FileHold. This is displayed only if this feature has been installed and configured.
Unique ID	A unique identifier given for each installation of FileHold.
Web Client System Details	
System Version	The version of web server that is installed.
Build	The current build number of FileHold. See FileHold Software Versions for more information.
Machine name	Name of the server that FileHold is installed on.

Field	Description
Domain name	Name of the domain that is synchronized with FileHold. This is displayed only if this feature has been installed and configured.
License Details	
Registered to	The name of the company that the license is registered to.
License issued	The date the license was installed.
License time limit	The date and time the license expires. If the FileHold license has been fully paid, then the time limit is "unlimited".
Description	A description of the license.
Full concurrent sessions	The number of concurrent sessions available to users assigned a Full registered user account type. Concurrent access licenses determine how many users with read-only permissions and higher can log into FileHold at the same time (concurrently).
Full registered users	A Full user license is a user that has been assigned to a group with a role of read-only or higher. Full users consume the full concurrent sessions.
Portal alias users	A portal alias user is a user assigned to a group with a role of "limited" and is used in conjunction with the Anonymous portal. Portal alias users consume limited concurrent sessions.
Limited registered users	A limited registered user is a user assigned to a group with the role of "limited". Limited registered users consume the limited concurrent sessions.
Limited concurrent sessions	The number of limited session packs. This is the number of users assigned to the "limited" role that can be logged into FileHold at the same time (concurrently). Packs are sold in with a minimum of 10 sessions.
Capture concurrent sessions	The number of SmartSoft Capture licenses purchased for scanning.
Available Courier use units	The number of Courier license units available for Courier.
SharePoint client concurrent sessions	Enabled or disabled – SharePoint integration is enabled or disabled in the system.
Workflow module	Enabled or disabled – The workflow module is enabled or disabled in the system.
Active Directory module	Enabled or disabled – The active directory module is enabled or disabled in the system.
Redaction module	Enabled or disabled – The redaction feature is enabled or disabled in the Brava viewer. *Starting in 2017, Brava viewer licenses are no longer available for new purchases. This information is retained for existing users only.*

Field	Description
FastFind module	Enabled or disabled – The FastFind feature is enabled or disabled in the system.
Print-to-FileHold	Enabled or disabled – The Print-to-FileHold feature is enabled or disabled in the system.
Enhanced Repository	Enabled or disabled – The enhanced document repository feature is enabled or disabled in the system.
Custom Providers & Queries	Enabled or disabled – When enabled, allows for lookups into file types other than databases.
OCR Module	Enabled or disabled – The server-side OCR feature is enabled or disabled in the system.
Image/PDF compression	Enabled or disabled – PDF and TIFF documents can be compressed to a smaller file size if this option is enabled. Files processed by server-side OCR engine can also be compressed, if the OCR Module is enabled in the license.
Automatic Document Importation	Enabled or disabled – The ADI feature is enabled or disabled in the system.
Digital Signature	Enabled or disabled – If this option is not enabled, then Adobe Sign is not available for use. The message "*The external signature feature is a license option. Contact sales@filehold.com to enable this feature*" appears if configuration is attempted.
Allow server plugins	Typically disabled.
Allow FDA plug-ins	Typically disabled.
Allow rebranding of the Web Client	When enabled, the Web Client can be rebranded.
Allow rebranding of the FDA	When enabled, the FDA can be rebranded.
Document Viewer Licenses	
Number of FileHold viewer level 1 licenses	Number of viewer licenses for viewing of PDF and image file formats in both the FDA and Web Client.
Number of FileHold viewer level 2 licenses	Number of viewer licenses for viewing extended file formats, annotations, watermarks, comments, and document assembly.
Number of FileHold viewer level 3 licenses	Number of viewer licenses for using redaction plus all of the level 2 features.
Number of Brava Office Viewer named licenses (includes PDF/Image Viewer)	Number of viewer licenses for viewing of a number of file extension types. *Starting in 2017, Brava viewer licenses are no longer available for new purchases. This information is retained for existing users only.*

Field	Description
Number of Brava Office Viewer with CAD Support named licenses (includes PDF/Image Viewer)	Number of viewer licenses for viewing of a number of file extension types including AutoCAD formats. *Starting in 2017, Brava viewer licenses are no longer available for new purchases. This information is retained for existing users only.*
Number of Brava Office Viewer (Engineering Edition) named licenses (includes PDF/Image Viewer)	Number of viewer licenses for viewing of a number of file extension types including several engineering file formats. *Starting in 2017, Brava viewer licenses are no longer available for new purchases. This information is retained for existing users only.*
Web scanning licenses	
Number of licenses	The number of licenses for scanning documents through the Web Client. See the Knowledge Base for more information on Web Cap scanning.

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.

FileHold software is activated by licensing the software. There are three steps to licensing FileHold.

1. Request a new license file from FileHold licensing. Use the **Request a License** button.
2. Receive a new license file by email from FileHold.
3. Apply the new license file to your FileHold server.

To request a new license key

1. In the Web Client, go to **Administration > 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 **Request a License**.
3. Fill out the following information in the Request a License form:
   - Select the reason for the license request in the “Please provide the reason you are requesting a new license file” list.
   - Enter any details for the license request in the “Please provide the reason details”.
   - Enter the name of your organization. This is a required field.
   - Enter the email address of the user who receives the license. This defaults to the currently logged in user’s address. This is a required field.
   - Enter the contact name. This defaults to the currently logged in user’s name. This is a required field.
4. Select one of the following request methods:

- Send the request directly to FileHold —Sends the email directly to licensing@filehold.com. This is the preferred method if you have an internet connection available on the FileHold server.
- Open email client to send request — Opens an email using the default email client with the license details and addressed to licensing@filehold.com.
- Copy the request to the clipboard — The text for the body of the email displays below. Copy and paste the contents into an email and send to licensing@filehold.com.

5. Click **Cancel** to return to the License information page. The licensing team emails a new license to the contact in the request. The license file must be saved locally in order to install the license.

TO INSTALL A LICENSE KEY

1. In the Web Client, go to **Administration > 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 **Install a License**. The license file is emailed to the contact email on the request form. Ensure the license file is saved locally so that it can be installed.
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 indicate the licensed is valid "*This is a valid license file. Click the Update system license button to replace the current license or click Cancel for no license changes.*"
5. Click **Update System License** to complete the process.
6. After a new license has been updated, you are asked to reset the password for the Outbound Email Settings and the external database passwords for any metadata fields that are the type drop down database or schema lookups if configured. The message "*IMPORTANT: After you update the system license you should verify your connection with the outgoing mail server and external database connections configured in dropdown menus or schema lookups. It may be necessary to reenter the password(s) for those connections"* appears at the top of the screen.

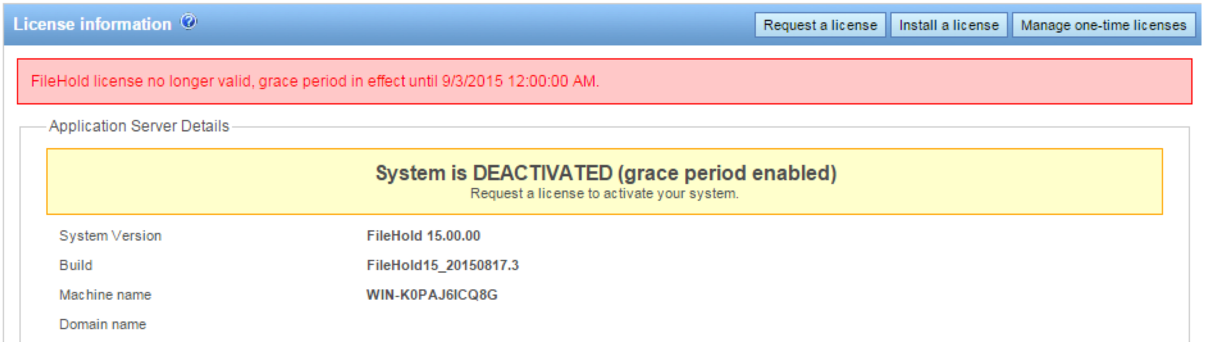
TIP: You *do not* need to reboot or restart the web server after a new license is added.

5.1. LICENSE EXPIRATION GRACE PERIOD

When a license expires or the hardware key is changed and does not match the current license file, an email entitled "*Attention Required: Your FileHold license has expired*" is sent automatically to the email addresses of the system administrators of FileHold. The content of the email includes the date when the 7-day grace period ends. When the grace period is effect, the notification is sent out on a daily basis through the FH email notifications (daily summary) scheduled task.

The system continues to work normally until the grace period expires. If you receive the license expiration notification email, use the Request a license procedure to get a new license key.

The License information page also displays messages stating that the system is deactivated, the grace period is enabled, and the date and time in which the grace period expires. If you do not get a new license prior to the grace period expiring, then the system is deactivated.



FileHold license no longer valid, grace period in effect until 9/3/2015 12:00:00 AM.

System is DEACTIVATED (grace period enabled)
Request a license to activate your system.

System Version	FileHold 15.00.00
Build	FileHold15_20150817.3
Machine name	WIN-K0PAJ6ICQ8G
Domain name	

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 for licensing options.

5.2. COURIER LICENSES FOR COURIER

There are circumstances where a user needs exclusive rights to view or approve a single or small set of documents in FileHold. In these cases, it may be impractical and excessively costly to assign these users a FileHold registered user license. Instead, a FileHold feature called Courier, can be used to route documents for review and/or approval to people outside of the FileHold system.

A license type called Courier Licenses is needed when documents are sent out through Courier. Customers can purchase these Courier licenses in “packs”. These license packs contain the number of units purchased. Units are consumed when documents are sent out through a Courier transmission. The number of units consumed in a view or approve action depends on the action taken on a document. For example, viewing document consumes one unit and approving a document requires two units. Packs can be priced differently according to volume. Contact sales@filehold.com for Courier license pricing.

One-time usage is given to a specific user for a specific operation. Some examples of Courier license use are:

- Five documents are transmitted to a construction sub-contractor (external user); 4 for viewing and 1 for approval. A total of 6 Courier units is consumed for these license grants.
- One contract is transmitted to an outside property company and must be countersigned by the VP of operations (internal user). A total of 2 Courier units is consumed.
- A corporate attestation document must be accepted by all 600 company employees. 50 employees are regular FileHold users. 1100 Courier units is consumed.

Courier licenses observe the following rules:

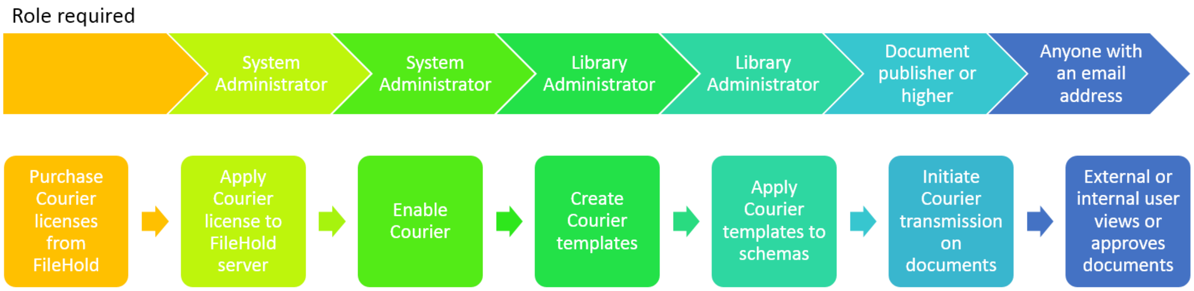
- The license is perpetual as long as the main FileHold license is active and until explicitly cancelled or fully consumed.
- The license units are reserved for completing the viewing or approving action when a document is transmitted through Courier.
- The license for a “view” is fully consumed when the document is downloaded. A document can be viewed again even if the action is completed.
- The license units for approval are fully consumed when the document is approved or not approved.
- If changes are requested to the documents (approval postponed) units are not consumed.

- If a document is not approved, the actions for any other recipients are cancelled and units are returned if the action has not already completed.
- If the transmission expires before the user completed the activity, no usage units are consumed.
- Courier licenses have no inherent expiry, but the Courier template by impose an expiry. For example, if a user is asked to approve a document the Courier license is fully consumed after the approval is complete. If the user is given a document to view, the document remains viewable on the same license unless the right to view is explicitly removed in the workflow template. See the *Library Administration Guide* for more information on Courier templates.

NOTE: If a document is routed to a registered FileHold user, no Courier licenses are consumed. The Courier license is perpetual as long as the registered user is enabled. If a user is disabled their grants are suspended, but not cancelled. If the user is re-enabled the suspension is lifted.

Once the Courier license pack has been obtained, the license file needs to be installed in order to route documents. Courier licenses are managed from the Licensing page. Multiple packs can be installed in the system at one time. A license pack can be installed exactly once on exactly one FileHold server as identified by its unique id.

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

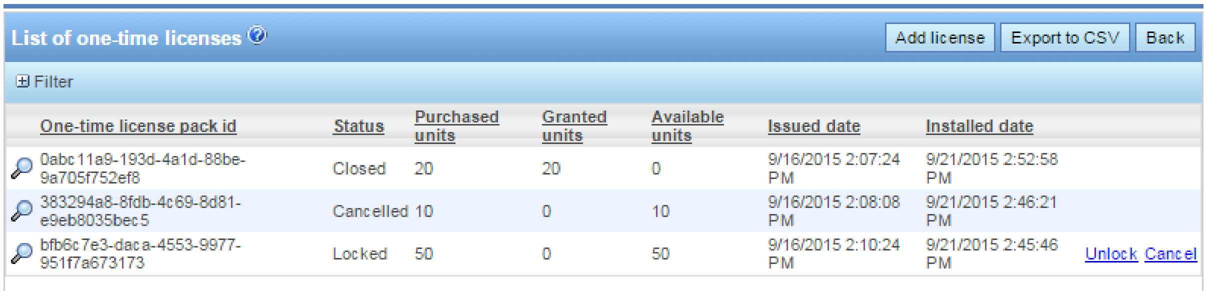

Role required
System Administrator
System Administrator
Library Administrator
Library Administrator
Document publisher or higher
Anyone with an email address
Purchase Courier licenses from FileHold
Apply Courier license to FileHold server
Enable Courier
Create Courier templates
Apply Courier templates to schemas
Initiate Courier transmission on documents
External or internal user views or approves documents

To add Courier license packs

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 **Manage Courier licenses**.
3. In the List of Courier licenses screen, click **Add license**.
4. In the Upload a Courier license file screen, click **Choose file** to select the otlic license file that was sent to you from licensing@filehold.com.
5. Click **Upload and validate**. The message “The uploaded Courier license file is valid” Is displayed.

NOTE: If the Courier license was already uploaded, a message “The uploaded Courier license file has already been added” is displayed. The the license file is not valid, a message “The uploaded Courier license file is not valid” is displayed.

6. Click **Add license**. The license is added to the list of Courier licenses.



	One-time license pack id	Status	Purchased units	Granted units	Available units	Issued date	Installed date	
🔍	0abc11a9-193d-4a1d-88be-9a705f752ef8	Closed	20	20	0	9/16/2015 2:07:24 PM	9/21/2015 2:52:58 PM	
🔍	383294a8-8fdb-4c69-8d81-e9eb8035bec5	Cancelled	10	0	10	9/16/2015 2:08:08 PM	9/21/2015 2:46:21 PM	
🔍	bfb6c7e3-daca-4553-9977-951f7a673173	Locked	50	0	50	9/16/2015 2:10:24 PM	9/21/2015 2:45:46 PM	Unlock Cancel

The following table describes the List of Courier licenses screen:

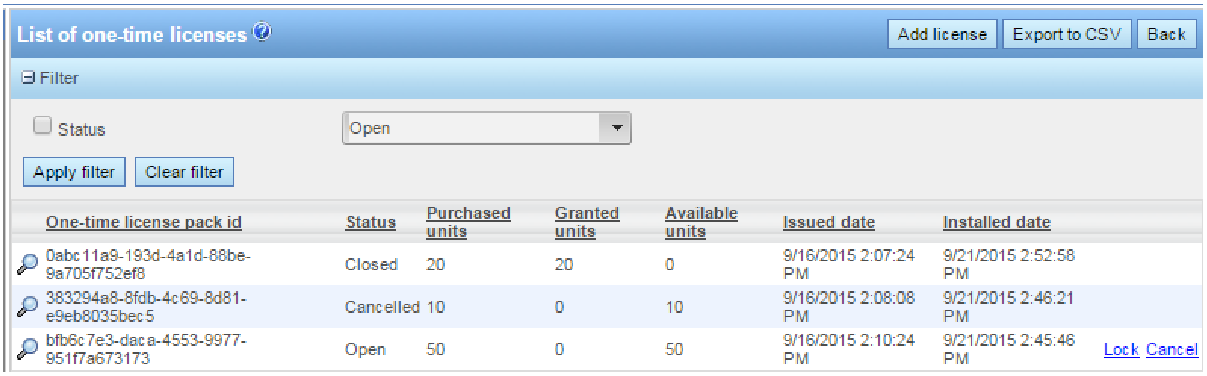
Column	Description
Courier license pack id	The ID code for the license. This is a unique code for each pack.
Status	Open – the license pack is available for consumption. Closed – the license pack has been fully consumed. Locked – the license pack is locked and units cannot be consumed. Cancelled – the license pack was cancelled and cannot be consumed or reinstated. Use this option with caution.
Purchased units	The total number of units in the pack.
Granted units	The number of units consumed in the pack.
Available units	The number of remaining units in the pack.
Issued date	The date the license was issued.
Installed date	The date the license was uploaded to FileHold.

To view Courier license pack log details

1. In the Web Client, go to **Administration Panel > System Management > License Information** and click **Manage Courier licenses**.

2. In the List of Courier licenses, click the **View** icon 🔍 to view the log details of a license pack.

- Optionally, expand the Filter area (+) and select a status of the Courier license pack to narrow down the list.



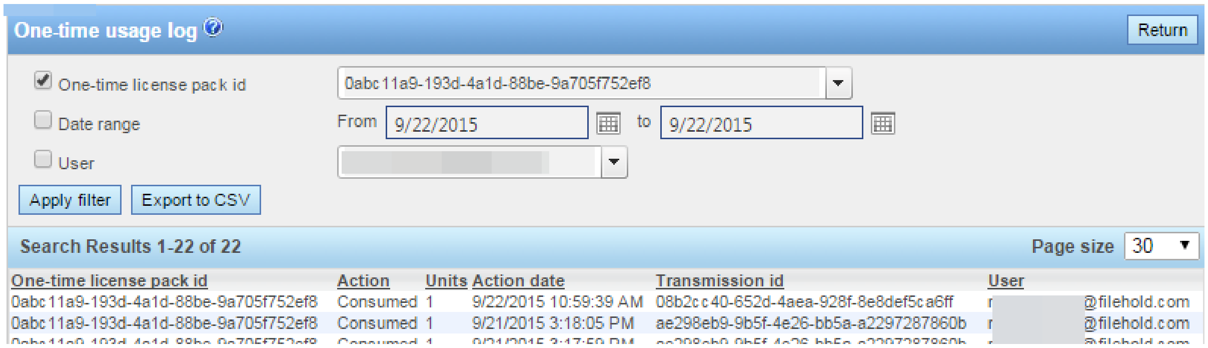
□ Status — Open

	One-time license pack id	Status	Purchased units	Granted units	Available units	Issued date	Installed date	
🔍	0abc11a9-193d-4a1d-88be-9a705f752ef8	Closed	20	20	0	9/16/2015 2:07:24 PM	9/21/2015 2:52:58 PM	
🔍	383294a8-8fdb-4c69-8d81-e9eb8035bec5	Cancelled	10	0	10	9/16/2015 2:08:08 PM	9/21/2015 2:46:21 PM	
🔍	bfb6c7e3-daca-4553-9977-951f7a673173	Open	50	0	50	9/16/2015 2:10:24 PM	9/21/2015 2:45:46 PM	Lock Cancel

3. The details for the usage of the Courier license pack are shown. Use any of the following filters:

- Courier license pack id. This can be changed to another license pack ID.
- Date range from <date> to <date>
- User. This is the email address of the recipient of the Courier transmission.

4. 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 using the Page size drop down. Click on the column to sort in ascending or descending order.
5. Click **Export to CSV** to export the results to a CSV file.



☑ One-time license pack id: 0abc11a9-193d-4a1d-88be-9a705f752ef8

☐ Date range: From 9/22/2015 to 9/22/2015

☐ User: [redacted]

Search Results 1-22 of 22

Page size 30

One-time license pack id	Action	Units	Action date	Transmission id	User
0abc11a9-193d-4a1d-88be-9a705f752ef8	Consumed	1	9/22/2015 10:59:39 AM	08b2cc40-652d-4aea-928f-8e8def5ca6ff	r[redacted]@filehold.com
0abc11a9-193d-4a1d-88be-9a705f752ef8	Consumed	1	9/21/2015 3:18:05 PM	ae298eb9-9b5f-4e26-bb5a-a2297287860b	r[redacted]@filehold.com
0abc11a9-193d-4a1d-88be-9a705f752ef8	Consumed	1	9/21/2015 3:17:59 PM	ae298eb9-9b5f-4e26-bb5a-a2297287860b	r[redacted]@filehold.com

The following table describes the List of Courier licenses screen:

Column	Description
Courier license pack id	The ID code for the license. This is a unique code for each pack.
Action	Reserved – the action has been assigned but not yet completed. The unit is held in reserve for the action. Consumed – the action has been completed and the unit was used. Returned – the unit has been returned because a document was marked as not approved by another user before another action could be completed.
Units	The total number of units in the pack.
Action date	The date the action was completed.
Transmission id	The unique transmission identifier for the Courier action. Click on the transmission ID to go to the Courier transmission detail screen. See the *Library Administration Guide* for more information on the Courier transmission log.
User	The email address of the person that the action was assigned to.

TO LOCK/UNLOCK COURIER LICENSE PACKS

Locking a Courier license pack prohibits the consumption of the units. The pack can be unlocked when consumption needs to be resumed.

1. In the Web Client, go to **Administration Panel > System Management > License Information** and click **Manage Courier licenses**.
2. From the List of Courier licenses, click **Lock** for the license pack ID that is to be locked from consumption.
3. To free up the license pack, click **Unlock**. The pack units can now be consumed.

TO CANCEL ONE TIME LICENSE PACKS

You can only cancel a Courier license pack if it has not yet been consumed. A cancelled license can never be used again.

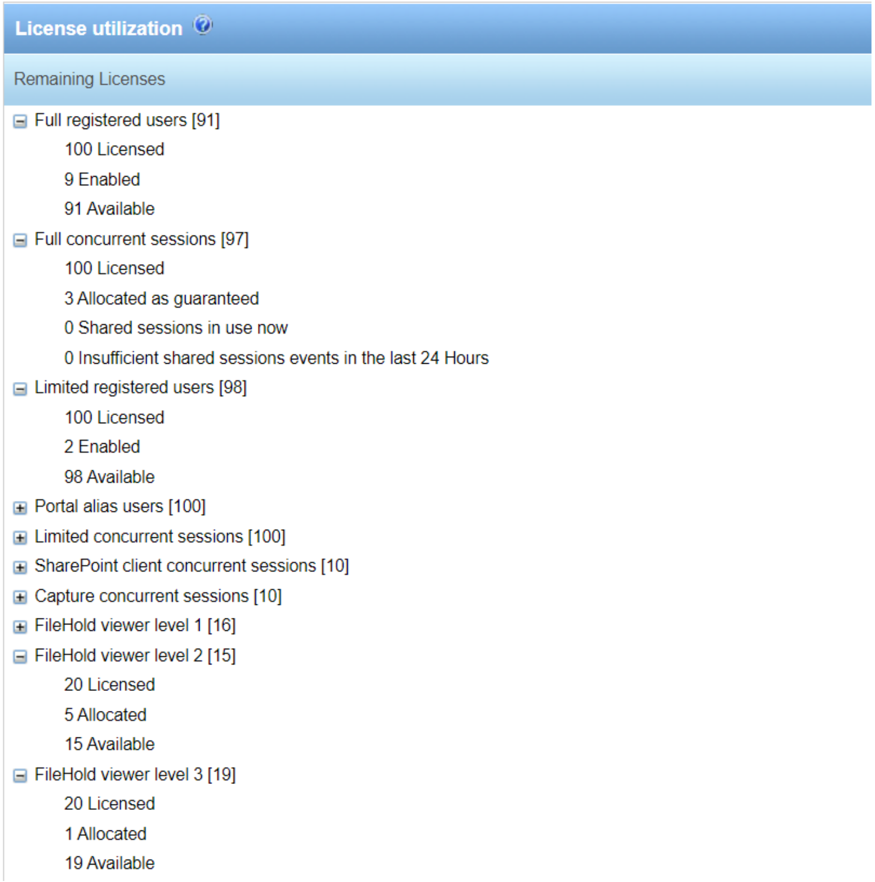
1. In the list of Courier licenses, click **Cancel** for the license pack you want to cancel / not use.
2. A message is displayed “Warning: You are about to permanently cancel a Courier license. Are you sure you want to continue?”
3. Enter a system administrator password to confirm the cancellation and click **OK**. The status of the license is changed to “Cancelled”.

EXPORT LIST OF COURIER LICENSES TO CSV

1. In the Web Client, go to **Administration Panel > System Management > License Information** and click **Manage Courier licenses**.
2. From the List of Courier license or in the Courier usage log, click **Export to CSV** to export the results to a CSV file. The csv file is downloaded.

5.3. LICENSE UTILIZATION

The License utilization page contains a summary of the purchased licenses. The total number of licenses, the number in use/enabled, and the number available are shown for full registered users, full concurrent sessions, viewers, Capture licenses, WebCap scanning licenses, SharePoint sessions, limited sessions, and more.



License utilization

Remaining Licenses

⊟ Full registered users [91]
100 Licensed
9 Enabled
91 Available

⊟ Full concurrent sessions [97]
100 Licensed
3 Allocated as guaranteed
0 Shared sessions in use now
0 Insufficient shared sessions events in the last 24 Hours

⊟ Limited registered users [98]
100 Licensed
2 Enabled
98 Available

⊞ Portal alias users [100]

⊞ Limited concurrent sessions [100]

⊞ SharePoint client concurrent sessions [10]

⊞ Capture concurrent sessions [10]

⊞ FileHold viewer level 1 [16]

⊟ FileHold viewer level 2 [15]
20 Licensed
5 Allocated
15 Available

⊟ FileHold viewer level 3 [19]
20 Licensed
1 Allocated
19 Available

To view the license utilization

1. In the Web Client, go to the **Full administration menu > System Management > License > Utilization**.
2. The following table describes the information in the Remaining Licenses area. The various licensing options can be expanded or collapsed by clicking on the + or -, respectively. The number of licenses remaining is shown in brackets.

Item	Description
Full registered users	A Full user license is a user that has been assigned to a group with a role of read-only or higher. Full users consume the full concurrent sessions.
Full concurrent sessions	The number of concurrent sessions available to users assigned a Full registered user account type. Concurrent access licenses determine how many users with read-only permissions and higher can log into FileHold at the same time (concurrently).
Limited registered users	A limited registered user is a user assigned to a group with the role of “limited”. Limited registered users consume the limited concurrent sessions.
Portal alias users	A portal alias user is a user assigned to a group with a role of “limited” and is used in conjunction with the Anonymous portal. Portal alias users consume limited concurrent sessions.

Item	Description
Limited concurrent sessions	The number of limited session packs. This is the number of users assigned to the “limited” role that can be logged into FileHold at the same time (concurrently). Limited sessions are sold with a minimum of 10.
Capture concurrent sessions	Indicates the total number of copies of SmartSoft Capture that was purchased. A license for a single copy of Capture allows for use by any number of users. There is no restriction to the number of workstations Capture can be installed on, but the concurrent use of Capture cannot exceed the total number of single copies purchased by the customer. For example, if the customer purchases 5 copies of Capture and installs the software on 20 workstations, 5 users can simultaneously run the software. If a 6th person attempts to run Capture, they receive a message that a license is not available.
FileHold viewer level 1	The number of level 1 viewers that are licensed, allocated and available to be assigned to a user account. FileHold viewers can be used in both the FileHold Desktop Application and the Web Client. Level 1 viewer includes the PDF/Image viewer in the FileHold Desktop Application.
FileHold viewer level 2	The number of level 2 viewers that are licensed, allocated, and available to be assigned to a user account. FileHold viewers can be used in both the FileHold Desktop Application and the Web Client. Level 2 viewer includes the PDF/Image viewer in the FileHold Desktop Application.
FileHold viewer level 3	The number of level 3 viewers that are licensed, allocated, and available to be assigned to a user account. FileHold viewers can be used in both the FileHold Desktop Application and the Web Client. Level 3 viewer includes the PDF/Image viewer in the FileHold Desktop Application.
Brava Office viewer	The number of Brava viewers that are licensed, allocated, and available to be assigned to a user account. See the Knowledge Base for more information on the functionality and features of the Brava viewers. *Starting in 2017, Brava viewer licenses are no longer available for new purchases. This information is retained for existing users only.*

Item	Description
Brava Office viewer, CAD	The number of Brava CAD viewers that are licensed, allocated, and available to be assigned to a user account. See the Knowledge Base for more information on the functionality and features of the Brava viewers. *Starting in 2017, Brava viewer licenses are no longer available for new purchases. This information is retained for existing users only.*
Brava Office viewer, Engineering	The number of Brava Engineering viewers that are licensed, allocated, and available to be assigned to a user account. See the Knowledge Base for more information on the functionality and features of the Brava viewers. *Starting in 2017, Brava viewer licenses are no longer available for new purchases. This information is retained for existing users only.*
Web scanning licenses	The number of WebCap licenses that are licenses, allocated, and available. See the Knowledge Base for more information on the functionality and features of WebCap.

6. ADMINISTRATION REPORTS

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

6.1. USER ACTIVITY LOG

The 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).

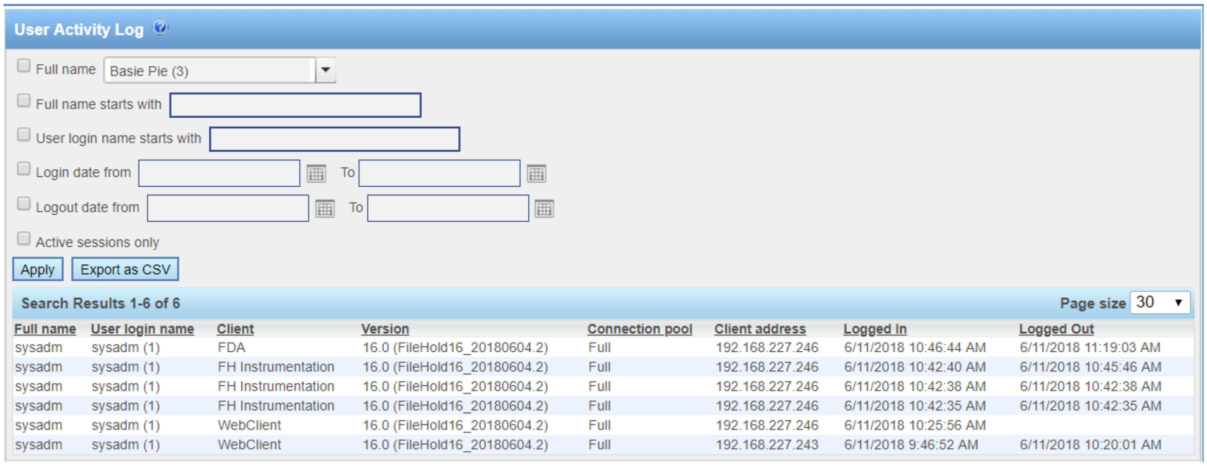
The following column information is displayed: full name, user login name including the internal ID number (the internal ID number is used to distinguish users with the same name), client (FDA, Web Client, Mobile, FH Instrumentation, Microsoft SharePoint, Custom), version and build number, connection pool (full, limited, 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 > Full Administration Menu > Administration Reports > 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**.



□ Full name: Basie Pie (3)

□ Full name starts with:

□ User login name starts with:

□ Login date from: To:

□ Logout date from: To:

□ Active sessions only

Search Results 1-6 of 6 — Page size: 30

Full name	User login name	Client	Version	Connection pool	Client address	Logged In	Logged Out
sysadm	sysadm (1)	FDA	16.0 (FileHold16_20180604.2)	Full	192.168.227.246	6/11/2018 10:46:44 AM	6/11/2018 11:19:03 AM
sysadm	sysadm (1)	FH Instrumentation	16.0 (FileHold16_20180604.2)	Full	192.168.227.246	6/11/2018 10:42:40 AM	6/11/2018 10:45:46 AM
sysadm	sysadm (1)	FH Instrumentation	16.0 (FileHold16_20180604.2)	Full	192.168.227.246	6/11/2018 10:42:38 AM	6/11/2018 10:42:38 AM
sysadm	sysadm (1)	FH Instrumentation	16.0 (FileHold16_20180604.2)	Full	192.168.227.246	6/11/2018 10:42:35 AM	6/11/2018 10:42:35 AM
sysadm	sysadm (1)	WebClient	16.0 (FileHold16_20180604.2)	Full	192.168.227.246	6/11/2018 10:25:56 AM	
sysadm	sysadm (1)	WebClient	16.0 (FileHold16_20180604.2)	Full	192.168.227.243	6/11/2018 9:46:52 AM	6/11/2018 10:20:01 AM

6.2. 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
- Modifying user accounts and FileHold groups
- Adding and deleting FileHold groups
- Enable and disabling licenses
- Resetting passwords
- Adding and removing users to and from FileHold groups
- Additional repositories are added or existing repositories are modified
- License is updated. The unique license ID is included in the details.
- Courier licenses - When new license packs have been added, closed, locked, unlocked or cancelled.
- If the permission setting “Enable optional passwords in workflow templates” is enabled or disabled.
- External ad-hoc Courier users are added to transmissions at initiation time
- Change in general system settings
- Change in email settings
- Change security settings
- Change search settings
- Initialized FTS index
- If the user type was changed from full to limited or vice versa, if it failed due to no license, or due to configuration when there is a synchronization of domain proxy users.

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 > Full Administration Menu > 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.

6.3. INSUFFICIENT CONCURRENT SESSIONS LOG

Concurrent access licenses determine how many users can log into the document management system at the same time (concurrently). This number varies depending upon how many concurrent user licenses your organization has purchased. There are different types of concurrent sessions:

- Full – Concurrent sessions used by registered users with a read-only role or higher.
- Limited – Limited concurrent sessions used by users with a limited role. Limited concurrent sessions allow large numbers of users to access the document repository using a generic username and password.
- Capture – The number of SmartSoft Capture sessions. SmartSoft Capture is a scanning application that works with FileHold. See the Knowledge Base for more information on Capture.

To see how many concurrent sessions you have, review the License Utilization page or the License Information page. You can see who is logged in and using a concurrent session from the User Activity Log.

To determine if there are enough concurrent user licenses for the software, run the Insufficient Sessions report 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.

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 run the Insufficient concurrent sessions log

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

6.4. 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).
	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 is 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.

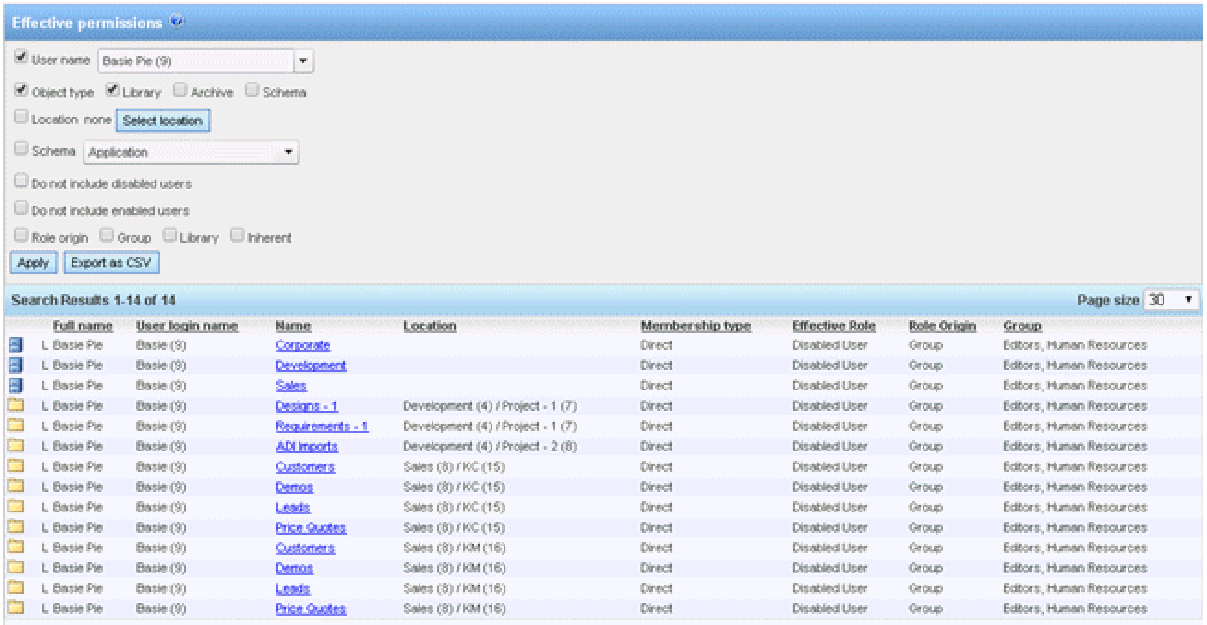
Symbol	Column Header	Description
	Effective role	The resulting permission in that area: Member – Used with schemas. Owner – Owner of either a cabinet or folder. Disabled user – The user is disabled in the system. *<Role name>* – The effective role of the user. If marked with an asterisk (*), this indicates that the user's permissions are reduced at that level of the library or they are not the owner. For example, a user is assigned to a group with a library administration role and cabinet administration role but only the group with the cabinet administration role has access to that level of the library. 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 > Full Administration Menu > Administration Reports > 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**.



Effective permissions

☑ 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

6.4.1. 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*

6.4.2. 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 is 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 is 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.

If marked with an asterisk (*), this indicates that the user’s permissions are reduced at that level of the library or they are not the owner. For example, a user is assigned to a group with a library administration role and cabinet administration role but only the group with the cabinet administration role has access to that level of the library.

6.4.3. 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.

6.4.4. 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 is 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.

6.4.5. 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

Object	User or Group Role	Assignment	Role Origin
Library	System administrator	Owner	Library
Library	Senior library administrator	Owner	Library
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.

6.4.6. 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.

6.5. SEARCH PERFORMANCE LOG

The search performance log is a way to record the searches that are being run in the system. Since FileHold does not restrict how users conduct their searches, this log can help the FileHold support team and customers pinpoint any search issues.

In order to see the search performance log results, it must first be enabled in **System configuration > Search settings**. See Search Engine Settings for more information.

The search performance log includes a record of all search types performed in the document management software. This includes not only searches (full text, advanced, saved searches) in FileHold but also when the folder list, virtual folder, document tray, linked documents, my favorites, checked out documents, document alerts, document reminders, recently accessed, recently added, and workflow documents list is accessed since these are essentially different types of searches as well.

The log can be filtered for a particular user, the view type, and action dates. The search results display the full name and user name, the status, the view type, the search type, various time measurements, and the date and time the search was performed. The search results can be exported to a CSV file and used for further analysis.

The following information is displayed in the search results:

Column Name	Description
Full name	Full name of the user
User login name	Username of the user
Status	Success — executed search was successful Error — executed search was not successful. An error occurred during the search. Timeout — the search took too long to execute and timed out
View type	Folder list Search results Virtual folder Linked document list Document tray My favorites Checked out documents Document alerts Document reminders Recently accessed Recently added Workflow documents
Search type	Saved search — regular saved search Quick search — quick search AdHoc — empty saved search, adhoc advanced search, or full text search
FTS term	The search term used in the full text search. This is truncated if too long. The full term is available in the search details page.
ID	Relative to the view type: Folders and virtual folders — folder ID number Workflow documents — workflow GUID Linked documents — parent document ID Search results — saved search ID All other views — no ID (empty)
Total ms	The total time of execution of the GetDocumentsBySnapshot method (without the network time)
FTS ms	The time of execution of the full text search. If FTS is used. This includes the network time between LM and FTS services (which are on the same host so it is negligible).

Column Name	Description
FTS size	The total number of results from the full text search. The full text search is the first stage in a search query so this number may be large, depending on the search query performed.
SQL create ms	The time of execution of the SQL query which performs the search and creates the snapshot. This includes the network time between the application server and database server.
SQL size	The number of results in the SQL database. The SQL search is the second stage in a search query. This number takes into account the number of records in SQL found plus the permissions of the user. If no SQL query was performed (only a full text search), then the SQL size is the same as the FTS size minus permissions of the user. For all other views, the SQL size is the number of documents displayed. For example, if there are 190 documents in a folder view, then the SQL size is 190. The SQL size number is the total number of results seen by the user in the view.
SQL read ms	The time of execution of the SQL query which returns the first page of search results
Date/time	The date and time that the search was performed

TO RUN THE SEARCH PERFORMANCE LOG

1. In the Administration Panel, go to **Administration Reports > Search performance log**.
2. Select any or none of the following filters:

- User name — Select the name of the user from the list.
- View type — Select one of the view types from the list. Options include: folder list, search results, virtual folder, document tray, linked documents, my favorites, checked out documents, document alerts, document reminders, recently accessed, recently added, and workflow documents.
- Action date — Enter the From and To date from the date pickers.

3. 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 header to sort in ascending or descending order.
4. To view the details of a search, click **Details** (magnifying glass icon) 🔍 next to the search record. The following table describes the details that are displayed for each view type. For more information on search details, see the API documentation.

View Type	Condition	Operator	Operand
Folder list	Library location	Equal	<name of folder>
	Only last version	Equal	True
Search results	File or metadata	Contains	<value entered for search>
	Only last version	Equal	True or False
	ReturnLastForBinaryVersion	Equal	True or False
	Include archive in search	Equals	True or False
	Saved search	Equal	<name of saved search>
	<metadata field name>	<operator selected for search>	<value of metadata>
Virtual folder	Virtual folder	Equal	<name of virtual folder>
Linked document list	IsLinkedWithDocument	Equal	<FileHold ID of the linked document>
Document tray	Tray	Equal	True
My favorites	IsStarredByUser	Equal	True
	Only last version	Equal	True
Checked out documents	Is checked out by user	Equal	<first and last name of user>
	Only last version	Equal	True
Document alerts	WithAlert	Equal	True
	Only last version	Equal	False
	ReturnLastForBinaryVersion	Equal	False
	IncludeDeleted	Equal	True
Document reminders	With reminder	Equal	True
	Only last version	Equal	True
	ReturnLastForBinaryVersion	Equal	False
Recently accessed	Document log action	InList	Downloaded, Viewed, Emailed
	LogActionPerformer	Equal	GUID of user Empty GUID indicates current user.
	Document Log Date	Greater or equal	<date>
	Only last version	Equal	False
	ReturnLastForBinaryVersion	Equal	True

View Type	Condition	Operator	Operand
Recently added	Document log action	InList	Add document, Checked in, Created by copy
	LogActionPerformer	Equal	GUID of user Empty GUID indicates current user.
	Document Log Date	Greater or equal	<date>
	Only last version	Equal	False
	ReturnLastForBinaryVersion	Equal	True
Workflow documents	Workflow instance	Equal	<name of workflow>
	Only last version	Equal	false

5. Click **Return to log report** to return to the list.
6. To permanently remove all displayed entries from the search log, click **Remove filtered log entries**. This function is primarily used to allow for the control of privacy of searches as needed.
7. To export the results, click **Export as CSV**.

6.6. COURIER USAGE LOG

A FileHold feature called Courier, can be used to route documents for review and/or approval to people outside of the FileHold system. A license type called Courier Licenses is needed when documents are sent out through Courier. Customers can purchase these Courier licenses in “packs”. These Courier license packs contain the number of units purchased. Units are consumed when documents are sent out through a Courier process. The number of units consumed varies for a view or approve action. For example, viewing a document consumes one unit and approving a document consumes two units.

The Courier usage log can be used to view the use and consumption of units in a Courier license pack. This log can also be viewed from the list of Courier licenses in the licensing area.

To view Courier license pack log details

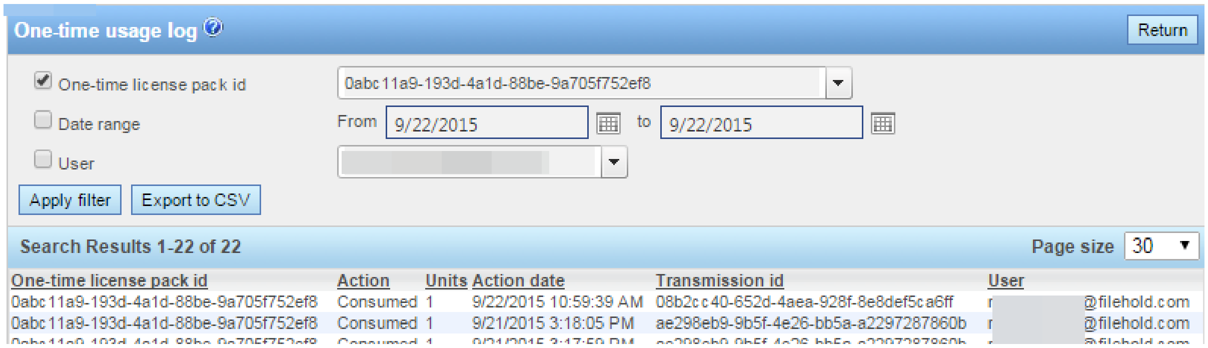
1. In the Web Client, go to **Administration > Full Administration Menu > Administration Reports > Courier usage log.**
2. Use any of the following filters:

- Courier license pack id. This is the license pack ID number. Each Courier license pack has a unique ID.
- Date range from <date> to <date>
- User. This is the email address of the recipient of the Courier transmission.

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 using the Page size drop down. Click on the column to sort in ascending or descending order.

4. Click **Export to CSV** to export the results to a CSV file.



One-time usage log

☑ One-time license pack id: 0abc11a9-193d-4a1d-88be-9a705f752ef8

□ Date range: From 9/22/2015 to 9/22/2015

□ User: [redacted]

Search Results 1-22 of 22

Page size 30

One-time license pack id	Action	Units	Action date	Transmission id	User
0abc11a9-193d-4a1d-88be-9a705f752ef8	Consumed	1	9/22/2015 10:59:39 AM	08b2cc40-652d-4aea-928f-8e8def5ca6ff	r[redacted]@filehold.com
0abc11a9-193d-4a1d-88be-9a705f752ef8	Consumed	1	9/21/2015 3:18:05 PM	ae298eb9-9b5f-4e26-bb5a-a2297287860b	r[redacted]@filehold.com

The following table describes the List of Courier licenses screen:

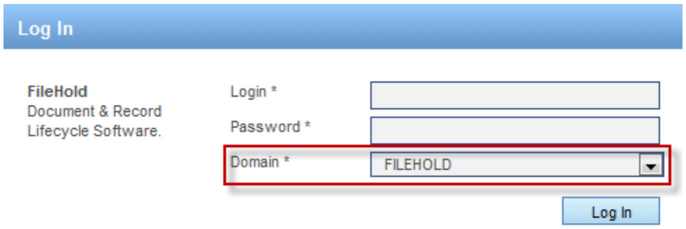
Column	Description
Courier license pack id	The ID code for the license. This is a unique code for each pack.
Action	Reserved – the action has been assigned but not yet completed. The unit is held in reserve for the action. Consumed – the action has been completed and the unit was used. Returned – the unit has been returned because a document was marked as not approved by another user before another action could be completed.
Units	The total number of units in the pack.
Action date	The date the action was completed.
Transmission id	The unique transmission identifier for the Courier action.
User	The email address of the person that the action was assigned to.

7. SYSTEM CONFIGURATION: GENERAL SETTINGS

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

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

7.2. 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 > Settings > General**.

8. 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.

7.3. 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 Alert Preferences. See the *End User Guide* for more information on Alert Preferences.

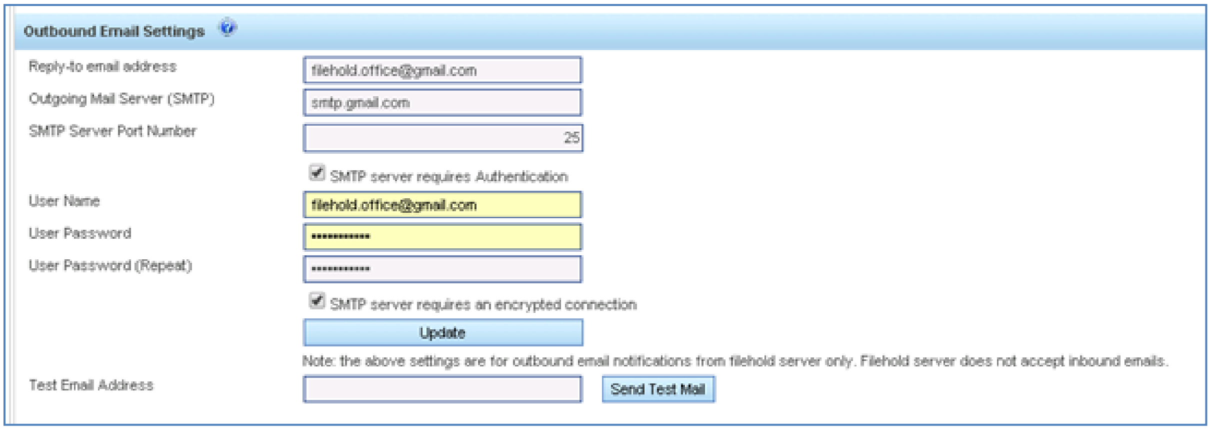
You may need to create an email account on your email server in order for FileHold to use this feature.

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.

NOTE: When sending an email using the built-in web email client, it can use the logged in users email address or the email address configured in the outbound email settings as the “From” address. A key, “Email.FromGlobalUser” can be configured in the Library Manager web config file. For new installs, the value defaults to true. For upgrades prior to 16.2, the default value is false. Setting this key to true emails using the outbound email address as the “From” address. This helps maintain proper email server configurations.

TO SET THE OUTBOUND EMAIL SETTINGS

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

Note: the above settings are for outbound email notifications from filehold server only. Filehold server does not accept inbound emails.

Test Email Address

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.

7.4. ENABLING COURIER

Courier is a feature which allows documents to be viewed or approved by people outside of the FileHold document management system.

To allow your users to utilize Courier, go to **Administration Panel > System Configuration > Settings > General** and click the **Enable Courier** check box. Once enabled, users are able to initiate a Courier process on documents provided the feature has not been disabled at the group level.

See Courier Licenses (Courier) and the *Workflow and Courier Guide* for more information on Courier.

7.5. ENABLING THE DASHBOARD

See System Administration Dashboard for more information.

7.6. 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 > Full Administration Menu > System Configuration > Settings > General > Document/Version Control Fields** area.
2. Select the **Enable Document Control Fields** check box, if applicable.
3. Select the **Enable Version Control Fields** check box, if applicable.
4. Click **Update**.

7.7. 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. In the Administration Panel, go to **Global Settings > 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 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.
   - Allow document version create date to be overridden – Allows the document version create date to be modified when importing document versions via Indirect Metadata > Import Jobs.
3. Click **Update**.

7.8. 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 can no longer be edited (checked out and in) 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 > Settings > General**.
2. In the Event Schedule Settings area, select the following check boxes, if applicable:
   - Enable Convert to Record Events —Allow documents to be automatically converted to a record after a specified period of time.
   - Enable Archive Events —Allow documents to be automatically sent to the archive after a specified period of time.
   - Enable Delete Events — Allow documents to be automatically “soft” deleted after a specified period of time.
   - Enable User Defined Events — Allow email and/or document alerts to be sent to specific administrative groups or document owners to notify them of an important document date or event.
3. Click **Update**.

7.9. INSUFFICIENT CAL NOTIFICATION SETTINGS

Concurrent access licenses (CALs) determine how many users can log into the document management system at the same time. This includes full concurrent sessions, limited sessions, and SmartSoft Capture sessions. 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 Utilization 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 > Settings > General > Insufficient CAL Notification Settings**.
2. In the Notification Interval field, select **Daily** or **Weekly**.
3. In the Recipients field, select **None**, **System Administrators Only**, or **Library and System Administrators**. “None” indicates that no emails are sent.

7.10. CLIENT OPTIONS BYPASS MODE FOR ADMINISTRATORS

The Client Options 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

1. In the Web Client, go to **Administration Panel > System Configuration > Settings > General**.
2. In the Centralized Options Management are, select the **Exclude Administrators** check box. When enabled, Library Administrators and higher roles can set their own preferences regardless of what options are enforced in the global settings.

When enabled, Administrators can set their own preferences regardless of what options are enforced in the global settings. See Client Options for more information.

7.11. ENABLING 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 is an optional feature that is controlled in the FileHold license called "OCR Module". To purchase the server-side OCR feature, contact sales@filehold.com.

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 take a higher priority in the queue via a setting. They are 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.

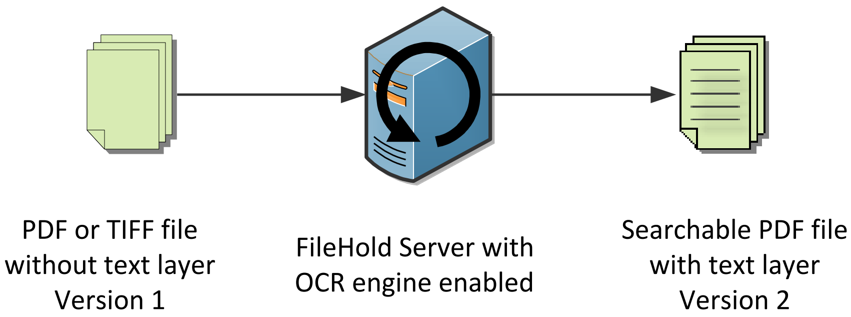
The criteria for adding a document to OCR processing queue are:

- The document must be an "Electronic Document" format. Electronic records and offline documents are not 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.

Compression is available for PDF and TIFF files that have gone through the server-side OCR process. This is controlled by the license setting "Image/PDF compression". The original version of the document can be removed by enabling the setting "OcrRemoveOriginalDocuments" in the web config file in Library Manager. If this option is enabled, the pre-OCR/pre-compressed version is soft deleted and a new version is checked in.

The Document usage log records which files that have undergone both OCR and compression or files that have only been OCR'd.



TO ENABLE SERVER-SIDE OCR

1. Go to **Administration Panel > System Configuration > Settings > 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 > Settings > 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 are processed. They are added to the queue with a low priority and do not affect the position of existing documents in the queue.

7.11.1. Configuration of Server-Side OCR

There are several configuration options for server side OCR that can be configured on the FileHold server by an administrator. See Server side OCR engine configuration in the Knowledge Base for more information.

8. SYSTEM CONFIGURATION: SEARCH SETTINGS

Use the Search Engine settings to configure how you want the search feature to return data. The Search settings page has been split into basic and advanced settings. It is recommended that the advanced search settings be left at the default values as changing the search engine settings can dramatically affect system search performance. If you make any changes, please note the previous settings and document your changes. Please read carefully all examples within this area. We recommend populating and using the system for a period of time before making major adjustments.

NOTE: Instead of enabling fuzzy, phonic, stemming, or synonym searching globally, you can perform these types of searches "on the fly" in a regular search. See Search Request Types for more information.

To configure search engine settings

1. Go to **Administration Panel > System Configuration > Settings > Search**. The basic settings are shown.
2. In the Error Email Addresses area, select the groups of users that receive a daily email with a summary of search engine warnings and errors: System Administrators, Library Administrators, Administrators (both library and system administrators), or No alerts.
3. In the Type of Errors to Send area, select the type of events that administrators want to be notified about:

- Index Errors Only — documents that are not capable of being indexed, search criteria errors, and index access errors.
- Un-indexed Files Only — files that are encrypted, digitally secured or damaged and cannot be indexed by the full text search engine.
- Both Un-indexed and Index Errors
- None

4. Select one of the following options for **Enable raw full text engine queries for role**. A raw query is a search that does not pre-process the query before sending it to the dtSearch engine. It is up to the user to provide the necessary dtSearch query syntax and avoid any FileHold specific search index content. If the user provides other FTS search criteria, the raw option is included in parenthesis and joined with an AND. See the *End Users Guide* for more information on raw queries.

- System administrators – This is the default.
- Senior library administrators and higher
- Library administrators and higher
- Cabinet administrators and higher
- All users

5. In order to log the searches conducted by users, select the **Is logging enabled** check box. Since FileHold does not restrict how users conduct their searches, this log can help the FileHold support team and customers pinpoint any search issues. See Search Performance Log for more information on logging searches.
6. In the “Maximum number of search results” area, enter the number of files to return from a search. This is the maximum number of search results that are displayed in the search view. The default number is 5,000.
7. In the “Maximum number of intermediate search results” area, enter the number of to be assessed for relevance when a full text search is combined with a database search. The default number is 10,000. For example, if the maximum number of search results to return is set to 5,000 and the maximum number of intermediate search results is set to 10,000, the search proceeds until 10,000 files are found and the best matching of the 5,000 are shown in the search results. We recommend that you set this number to 500,000 if you have a very large collection of documents.
8. In the Search Timeout area, enter the time, in seconds, to terminate a search. This limits users' ability to overload the server with unnecessarily complex searches. The default is 60 seconds.
9. Click **Advanced** to view the advanced search settings.
10. In the Search Result Metadata Weighting area, select the weighting of how strongly you want the metadata to influence the search results on a scale of 1 to 10. A selection of 1

puts more weighting on the content in the documents and a selection of 10 puts more weighting on the metadata. The suggested setting is 3 if you have strong metadata capture set in your schemas.

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

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

14. In the Synonym Searching area, select the check boxes to search for synonyms or related words.
15. In the Hyphen Searching area, you can set how hyphen characters are indexed and searched. Select from the following options:

- Hyphen as ignore — Does not index the hyphen. For example, “first-class” is indexed as “firstclass”.
- Hyphen as a hyphen — Indexes the hyphen. For example, “first-class” is indexed as “first-class”.
- Hyphen as a space — Separates the hyphenated words into two words. For example, “first-class” is indexed as “first” and “class”.
- Hyphen all — Indexes a hyphen as all three of the above options.

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

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

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

17. In the Initialize Index area, click **Initialize Index** to start full-text search indexing.

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

18. Click **Update** to update the search engine settings.
19. Click **Basic** to return to the basic search settings.
20. Click **Restore Default** to revert the settings to their default values.

8.1.1. Rebuilding the Full Text Search Index

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

WARNING: Certain changes in FileHold configuration can cause a re-indexing of documents, such as editing or deleting a drop down or drill down metadata field value or deleting a metadata field from a schema. If the user performs one of these actions, a message "*You are about to make a change that will cause x documents to be re-indexed. While these documents are being re-indexed, users may notice decreased performance in the system.*" This message appears when at least 1000 documents are affected by the re-indexation. This setting can be controlled by the setting "ReindexWarningThreshold" in the web config file in *C:\Program Files\FileHold Systems\Application Server\LibraryManager*.

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

TO REBUILD THE RE-INDEX YOUR LIBRARY

1. Go to **Administration Panel > System Configuration > Settings > Search**.
2. Click the **Advanced** button.
3. In the Initialize Index area, click **Initialize Index** to start full-text search indexing.

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

9. SYSTEM CONFIGURATION: DOCUMENT VIEWERS

You can configure the features of the viewer that are available to users when they are viewing certain file extensions. Viewers have user features and benefits that increase productivity and save companies money. The FileHold viewer level 1 comes standard with a registered user account. When creating a registered user, they are automatically be assigned a level 1 viewer license. This can be changed to a level 2 or 3 viewer, if purchased. For more information on the viewers and their functionality, see the *End User Guide*.

There are certain viewer types available:

1. FileHold viewer level 1 – Supports viewing PDF, docx, and image files in the FDA and Web Client.
2. FileHold viewer level 2 – Supports viewing several file formats in the FDA and Web Client. Includes annotations, comments, and document assembly features.
3. FileHold viewer level 3 – Supports viewing several file formats in the FDA and Web Client. Includes annotations, comments, document assembly, and redaction features.
4. PDF/Image viewer – Starting in FileHold 16.2, the PDF/Image viewer is considered end of life and all users should transition to the FileHold viewer. The PDF/Image viewer is disabled by default but can still be enabled for use. This viewer supports viewing only PDF and image files and is for use in the FileHold Desktop application. Users get the use of both the PDF/Image viewer (FDA only) and the FileHold viewer when assigned a FileHold viewer license.
5. Brava viewer –The legacy Brava viewers can be disabled for use. The Brava viewers are no longer available for purchase and are considered end of life. All users should transition to the FileHold viewers. If you had previously purchased Brava viewers, the following were the three levels of Brava viewers available: Enterprise Office Viewer, Enterprise Office Viewer with CAD support, Enterprise Office Viewer Engineering Edition. For more information on the Brava viewer functionality, see the Knowledge Base.

TO CONFIGURE THE VIEWER SETTINGS

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

Option	FileHold viewer L1	FileHold viewer L2	FileHold viewer L3	PDF/Im-age viewer	Brava Office	Brava CAD	Brava Engin-eering
Allow users to create annotations		X	X				
Allow users to print/print regions of documents	X	X	X				

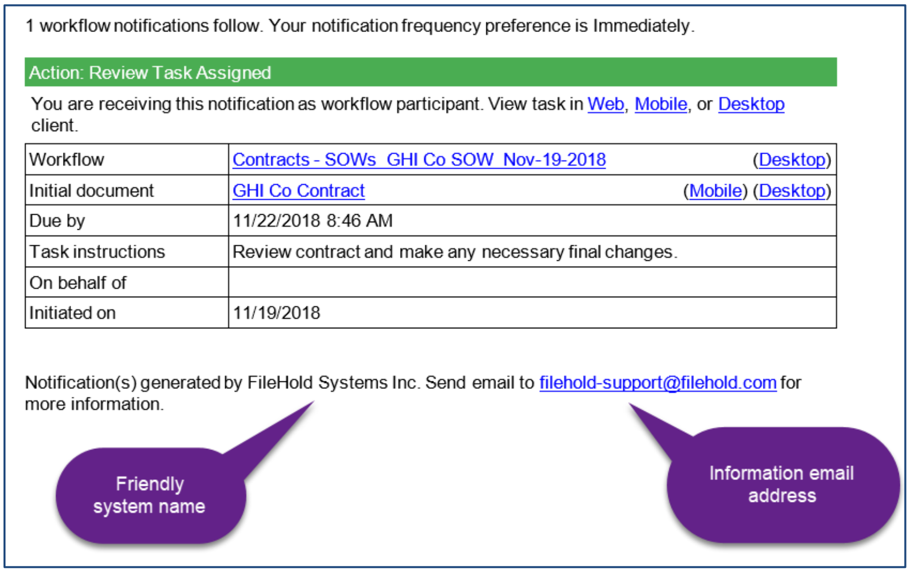
Option	FileHold viewer L1	FileHold viewer L2	FileHold viewer L3	PDF/Image viewer	Brava Office	Brava CAD	Brava Engineering
Allow users to publish documents as PDF files	X	X	X				
Allow users to copy pages to clipboard	X	X	X				
Allow users to manipulate pages	X	X	X				
Allow Users To Publish Documents As Adobe PDF Files				X	X		X
Allow Users To Publish Documents As TIFF Files				X	X		X
Allow Users To Save View In JPEG Format				X	X	X	X
Allow Users To Print / Print Regions Of Documents				X	X	X	X
Allow Users To Publish Documents As CSF Files					X	X	X
Allow Users To Compare Documents					X	X	X
Allow Users To Create ISO Banners / Watermarks For Printing					X	X	X
Allow Users To Copy Text and Markups In A Document To The Clipboard					X	X	X
Allow Users To Copy Regions Of Image Files To The Clipboard					X	X	X
Allow Users To View / Create / Edit Markups					X	X	X

Option	FileHold viewer L1	FileHold viewer L2	FileHold viewer L3	PDF/Image viewer	Brava Office	Brava CAD	Brava Engineering
Allow Users To Publish Documents As Dwf Files						X	X
Allow Users To Show Or Hide Layers						X	X
Enable Measurement Tools For Users						X	X
CAD File Path References For Viewing Of CAD files						X	X
Enable Document Redaction					X	X	X

3. To select all the options, click **Check All**.
4. To remove the selections, click **Uncheck All**.
5. To disable the use of the Brava viewers, select the **Disable the Brava viewer technology** check box. The message at the top of the screen changes to green and states "*The Brava viewer technology is disabled*."
6. Click **Save**.

10. SYSTEM CONFIGURATION: NOTIFICATIONS

The system notification settings allow an administrator to define the information displayed in the footer of the workflow notification emails.



1 workflow notifications follow. Your notification frequency preference is Immediately.

Action: Review Task Assigned

You are receiving this notification as workflow participant. View task in Web, Mobile, or Desktop client.

Workflow	Contracts - SOWs GHI Co SOW Nov-19-2018 (Desktop)
Initial document	GHI Co Contract (Mobile) (Desktop)
Due by	11/22/2018 8:46 AM
Task instructions	Review contract and make any necessary final changes.
On behalf of	
Initiated on	11/19/2018

Notification(s) generated by FileHold Systems Inc. Send email to filehold-support@filehold.com for more information.

Friendly system name

Information email address

To set system notification settings

1. Go to **Administration Panel > System Configuration > Settings > Notifications**.
2. In the Workflow notifications area, enter the following information:

- Friendly system name
- Information email address

3. Click **Save**.

11. SYSTEM CONFIGURATION: CUSTOM REPORTS

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 only provides documentation on how to integrate them. 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

4. Go to **Administration Panel > System Configuration > Settings > Custom Reports**.
5. In the Reporting Services Authorization window, click **Security**.
6. 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.
7. Click **Save**.

12. SYSTEM CONFIGURATION: EXPORT SCRIPTS

FileHold data can be exported to other systems upon a document action or workflow activity completion. For example, student transcripts can be sent to a storage vault or invoices can be sent to an accounting system to help automate invoice processing.

Export scripts are a custom integration solution. FileHold Professional Services can be contracted to prepare the export script. The export script contains a dll and the parameters for export. It is possible that the same script dll could have more than one configuration effectively creating more than one export script.

See the FileHold Knowledge Base for more information on export scripts.

13. 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.

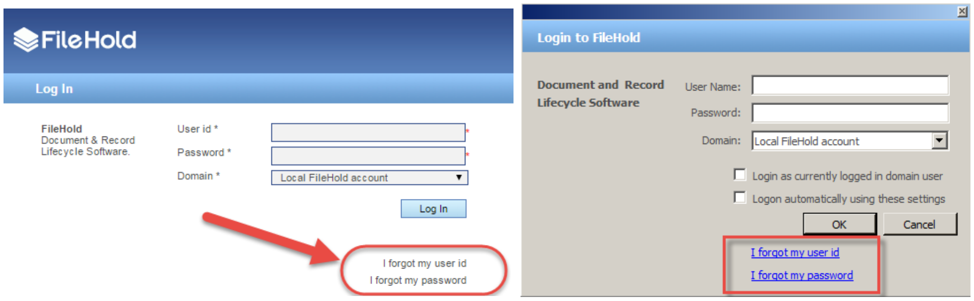
13.1. LOGON SECURITY

The logon settings allow the system administrator to manage the number of logon attempts allowed and the time-out settings for user sessions. If you need additional security when accessing the FileHold application, the multi-factor authentication feature can also be configured.

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 needs to enable the account in the Users area and if the user is a local user, reset their password.

The password security 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.

If local users (not domain users) forget their username or password, you can configure the Web Client login page or FDA login window to include links to recover their user ID and/or reset their passwords. If a user requests a password, a two-step verification process via a mobile phone can also be enabled with the use of a special plug-in. This sends a verification text message to the user’s mobile phone. If you want to use the mobile phone verification feature, contact sales@filehold.com.



SmartSoft Capture is the scanning application provided with every sale of FileHold. A license for a single copy of Capture allows for use by any number of users. A timeout value can also be set for Capture licenses. The inactivity timer can be set to automatically log off users and free the Capture license for another user which is especially good to set when multiple users are sharing a single license of Capture.

To set the logon and password security settings

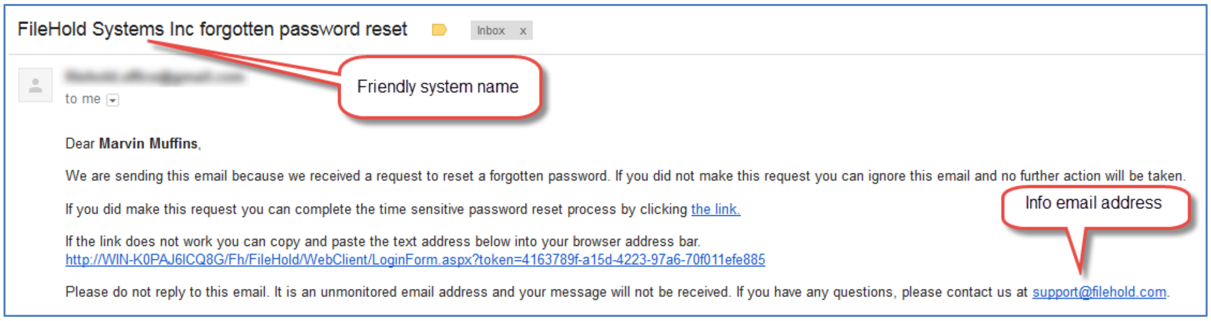
1. Go to **Administration Panel > System Configuration> Security> Logon**.
2. Enter the number of logon attempts allowed. The default number is 10. The user is locked out of the system after the number of login attempts has been exceeded. The system administrator receives an email stating that the user account has been disabled due to the exceeded number of login attempts. You 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. The time limit can be set to 0 to 9999 minutes with the default of 30 minutes.

   TIP: There is an additional timeout for web client users to conserve memory. By default, after 15 minutes, the web client state is purged from the server. The user receives a message that they were timed out, but they can return to their session by clicking on the supplied link. They are not 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 Expire Capture licenses after field, enter the amount of time, in minutes, that the system automatically logs an inactive user out of SmartSoft Capture. This is the amount of time that Capture is idle and not in use. This frees up a concurrent Capture license for another user. The time limit can be set to 0 to 9999 minutes with the default of 30 minutes.
5. To set up Multi-factor authentication, click **Configure**. Multi-factor authentication confirms the identity of users on devices before they connect to FileHold. See Multi-factor authentication for more information on how to configure this feature.
6. 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 only. The default is 5 characters.
7. 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

8. 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.
9. In the Password reset options area, in the **Administrator password reset verification email expires after** field, enter the amount of time, in hours, that the verification email is valid for when setting a password from the Users list page. See Resetting User Passwords for more information. If the user does not use the link in the verification email within this time period, then the link expires. The minimum amount of time is 1 hour, the maximum time is 999 hours.
10. Select the **Allow users to request a forgotten user ID with only an email address** check box to allow users to request their user ID by clicking on the “I forgot my user ID” link on the login screen. If this option is not enabled, the “I forgot my user ID” link is not available for use.

11. Select the **Allow users to reset a forgotten password** check box to allow users to set a new password by clicking on the "I forgot my password" link on the login screen. If this option is not enabled, the "I forgot my password" link is not available for use.
12. In the **User password reset verification email expires after** field, enter the amount of time in minutes that the verification email expires after it is sent to the user requesting the password. If the user does not use the link in the verification email within this time period, then the link expires and the user needs to request the password again. The minimum time is 5 minutes, the maximum is 9999 minutes.
13. In the **Friendly system name** field, enter the partial subject line for the email that gets sent to the users when resetting a password. For example, the email subject is "*<Friendly system name> forgotten password reset"* where <Friendly system name> could be "FileHold".



FileHold Systems Inc forgotten password reset

[redacted]
to me

Dear **Marvin Muffins**,

We are sending this email because we received a request to reset a forgotten password. If you did not make this request you can ignore this email and no further action will be taken.

If you did make this request you can complete the time sensitive password reset process by clicking the link.

If the link does not work you can copy and paste the text address below into your browser address bar.
http://WIN-K0PAJ6ICQ8G/Fh/FileHold/WebClient/LoginForm.aspx?token=4163789f-a15d-4223-97a6-70f011efe885

Please do not reply to this email. It is an unmonitored email address and your message will not be received. If you have any questions, please contact us at support@filehold.com.

14. In the **Info email address** field, enter the contact email address for the person providing assistance if the user is experiencing issues with resetting a password. This email address is provided on the email sent to the user requesting a forgotten password. For example, "*Please do not reply to this email. It is an unmonitored email address and your message will not be received. If you have any questions, please contact us at <contactname@yourdomainname.com>*." where <*contactname@yourdomainname.com*> is the info email address.
15. Select the **Force users to verify their identity with their mobile phone** check box to enable a two-step verification process in order for users to reset their password. To enable, a plug in for this feature must be installed and configured. Contact sales@filehold.com for information on enabling this feature. Users must also have a mobile phone number entered in their user account details or the two-step verification process does not work.
16. Select the **Force user to provide a mobile phone number when creating an account** check box to force mobile phone numbers to be entered in the Contact Information area when creating or modifying a local user account. This mobile phone number is required when using the two-step verification process. Any users without a mobile phone number are not able to reset their password.
17. Click **Update** to save any changes.

13.2. MULTI-FACTOR AUTHENTICATION CONFIGURATION

If you need additional security when accessing the FileHold application, the multi-factor authentication feature strengthens access security by requiring two methods to verify a user's identity. FileHold supports multi-factor authentication (MFA) with the Duo (www.duo.com) "Trusted Users" service.

Duo MFA is used when configured in FileHold. Each standard FileHold client supports MFA including: FileHold Desktop Application (FDA), web client, mobile web client, and Courier client.

The MFA feature has three basic operations:

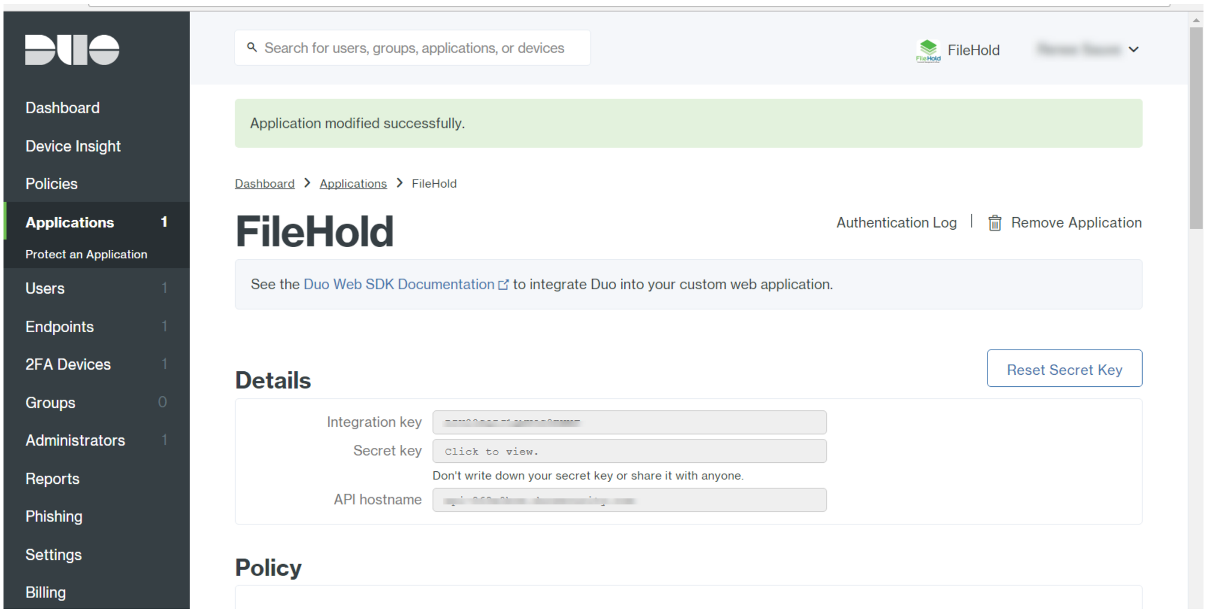
1. User logs on to FileHold.
2. FileHold application server contacts Duo to obtain an authentication. The user logging in selects the option to be authenticated: “push”, call, or text. If the user does not have a Duo account, they need to register and/or download the app.
3. Duo sends authentication to FileHold. The user is logged into FileHold if Duo successfully delivers the authentication.

An administrator needs to set up the Duo account at www.duo.com prior to configuring MFA in FileHold. This is the responsibility of the customer, not FileHold. Visit the Duo website for documentation.

Each user requiring authentication also need to set up their own accounts with Duo. See the *End User Guide* for more information. MFA can be disabled for a particular user account. See Creating Locally Managed Users for more information.

To configure DUO MFA

1. In the Administration panel, go to **System configuration > Security > Logon** and click **Configure** in the “Multi-factor authentication is disabled area”.
2. Select the **Provider** tab. The Duo account needs to be configured at www.duo.com in order for these settings to be entered. When setting up the account at Duo, select or search for the **Web SDK** application.
3. Once the Duo account has been set up, the details needed for FileHold are provided on your account page. Review the Duo documentation for more information.



Application modified successfully.

FileHold

See the Duo Web SDK Documentation to integrate Duo into your custom web application.

Details

Integration key [redacted]

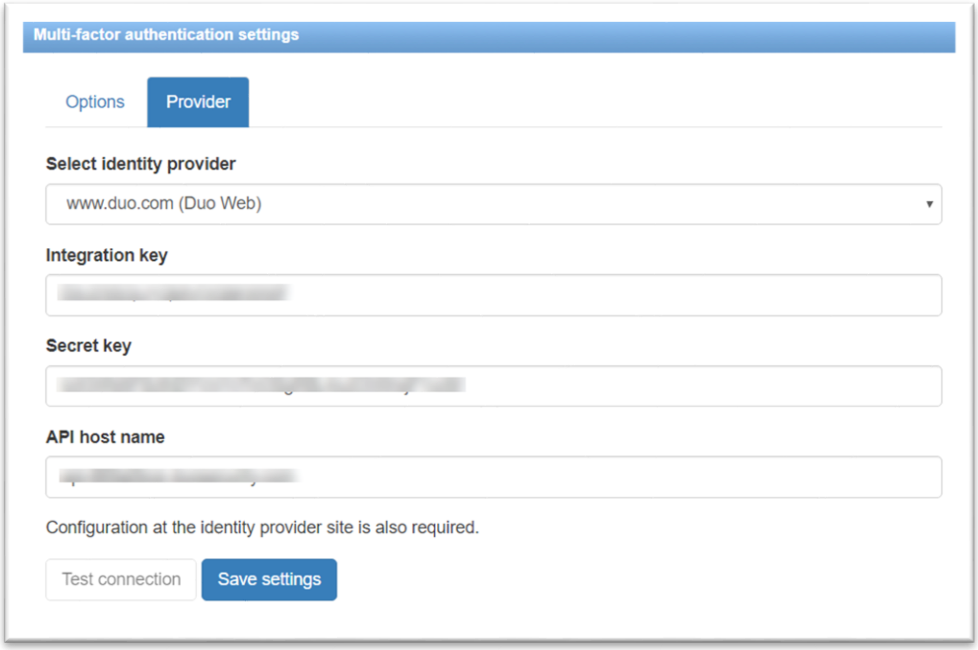
Secret key Click to view.

Don't write down your secret key or share it with anyone.

API hostname [redacted]

Policy

4. Copy and paste the Integration key, Secret key and API host name in the corresponding fields on the Provider tab in FileHold and click **Save Settings**.



Multi-factor authentication settings

Select identity provider: www.duo.com (Duo Web)

Integration key: [redacted]

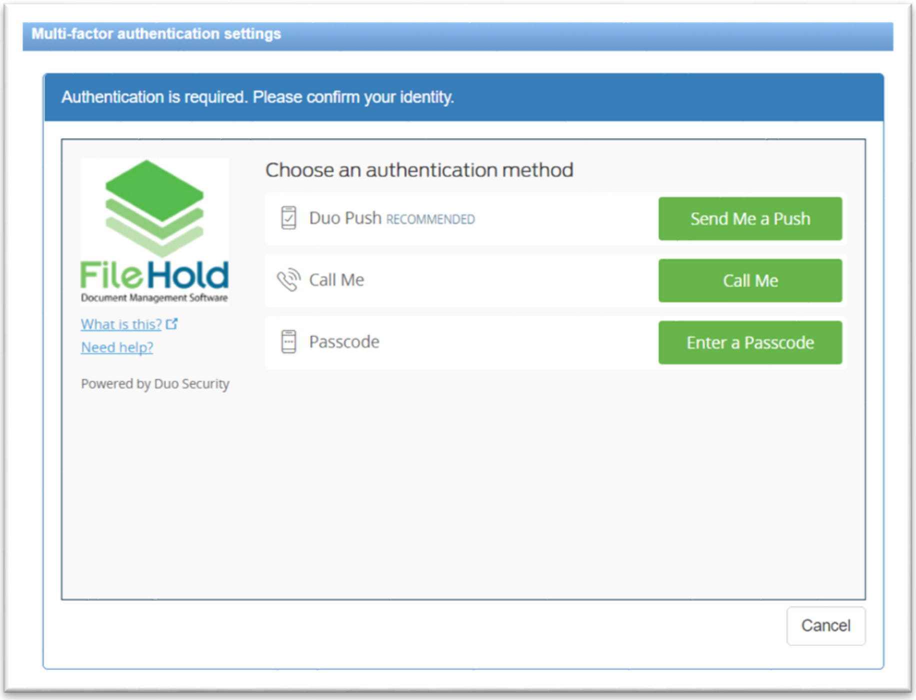
Secret key: [redacted]

API host name: [redacted]

Configuration at the identity provider site is also required.

5. Click **Test Connection**.
6. A message "*Authentication is required. Please confirm your identity*." appears. Select one of the authentication methods. If you can't authenticate or aren't sure what to do, click **Need help?** on the left side of the Duo prompt.

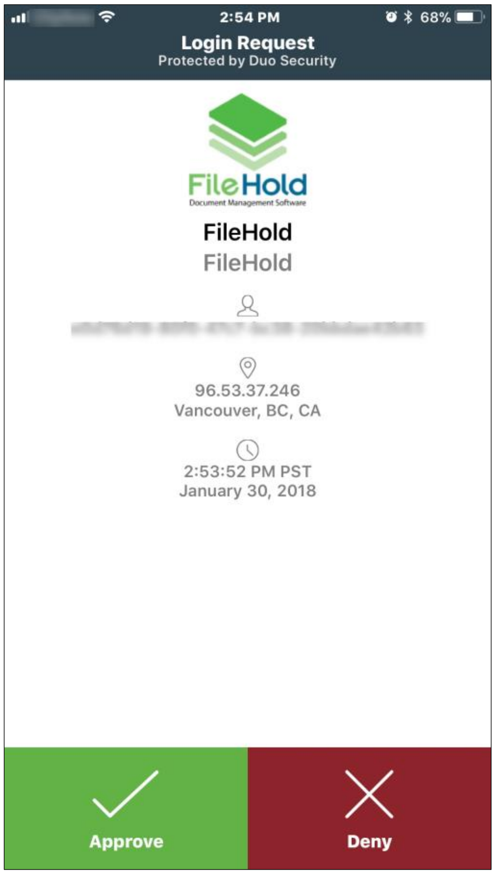
- Duo Push – Pushes a login request to your phone or tablet (if you have Duo Mobile installed and activated on your iOS, Android, or Windows Phone device). Just review the request and tap Approve to log in.
- Call Me – Authenticate via phone callback.
- Passcode – Log in using a passcode, either generated with Duo Mobile, sent via SMS, generated by your hardware token, or provided by an administrator.



Multi-factor authentication settings

Authentication is required. Please confirm your identity.

Choose an authentication method



Example of Duo Push authentication method – notification sent to iOS Duo app

7. Once authenticated, a message "*Connection test to provider is successful. Enable multi-factor authentication now.*" Click the link to enable the MFA feature or select the **Options** tab.
8. In the Options tab, select any of the following options:

Option	Description
Login is open to all users Login is restricted to library administrators and higher Login is restricted to system administrators	Click **Change login restrictions** to change who can currently access FileHold. Update the Restricted Access area in the **Library Configuration > Settings > General** page. See the *Library Administration Guide* for more information. Click **Update** to save login changes.
Enable multi-factor authentication	This option is disabled by default. A successful test must be completed before this check box can be enabled. Clearing the check box does not affect the settings, but it renders them unused by the login process for all users.
Require multi-factor authentication when Integrated Windows Authentication is used.	For domain users. This option is enabled by default.
Require multi-factor authentication for external users.	External users are those users who do not have a registered user account, such as external Courier users. This option is disabled by default.
Require multi-factor authentication for portal alias users.	The user account set up for the Anonymous portal. This option is disabled by default.
Require multi-factor authentication for limited registered users.	A user account that has been assigned to a group with a role of limited. This option is enabled by default.

9. Click **Save settings**. Users now need to use Duo to authenticate their login.

13.3. 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:

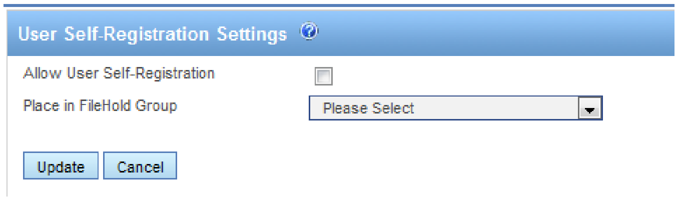
- The system is being deployed for the general public and user registration needs to be self-serve.
- The system is being used by an organization that does not have or plan to use Active Directory to manage the users. This provides access while limiting administrator burden to create user accounts.
- 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 need to assign self-registered users to a group. This controls 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 appears 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 > User Management > 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 is visible on the logon page of the Web Client. You cannot self-register from the FileHold Desktop Application (FDA).

14. DOCUMENT REPOSITORY LOCATIONS

The document repository is where the files in the library and library archive are stored. By default, there is one document repository which is created when FileHold is installed on the server.

The document repository can be split into multiple locations to improve scalability. See Enhanced repository locations for more information.

To access the repository locations

1. In the Web Client, go to **Administration Panel > System Configuration > Document repository locations.**
2. The following information is displayed. Columns can be added or removed and columns can be filtered and sorted in ascending/descending order by clicking on the filter icon ⋮.

By default, a single Default repository group and location are shown. If the Enhanced repository feature has been purchased, additional groups and locations can be added and/or managed.

Column heading	Description
Group status	Since threshold values can differ if there are more than one location in the group, the status for the group is based on the sum of the absolute value for the locations. If there is only one location, then the group status and location status are the same. • Green – space available • Yellow – space available but below warning threshold • Red – no space available. Documents cannot be added.
Group name	The name of the group. The group is named “Default repository group” by default when FileHold is installed.
Preference (Group)	The type of preferred contents: • Default – used when no preferred group matches the file being added. “Default” is the default value when FileHold is installed. • Archive – library archive documents. • Cabinet – a specific cabinet location or the location where the cabinet’s contents are archived. When a file is added to FileHold, the list of preferences is checked to see which group it belongs in. If there is no matching group, the file is placed in the default group. Document version associated files such as markups or cached files are placed according to their document version. Attachments not related to specific documents such as workflow or Courier attachments are placed in the default group.
Locations (Group)	The number of locations in the group.
Available space (Group)	Since threshold values can differ if there are more than one location in the group, the available space for the group is based on the sum of the absolute value for the locations. If there is only one location, then the group and location available space are the same.
Location status	The status of the location: • Green – space available • Yellow – space available but below warning threshold • Red – no space available. Documents cannot be added.
Location name	The name of the location. The location is named “Default repository” by default when FileHold is installed.
Path (Location)	The path to the repository location.
Allow new files (Location)	• Yes – The Allow new files check box is enabled in the location properties. • No – The Allow new files check box is disabled in the location properties.

Column heading	Description
Available space (Location)	The amount of space available in the location.

14.1.1. Editing group and location properties

Repository groups and locations properties can be modified or viewed.

To edit group properties

1. Select the check box in the group row and click **Edit**.
2. In the **Definition** tab, modify the group name. The group is named “Default repository group” by default when FileHold is installed.
3. Set the document preference. This setting cannot be modified if the enhanced repository feature was not purchased.
   - Default – Used when no preferred group matches the file being added. "Default" is the default value when FileHold is installed.
   - Archive – Library archive documents.
   - Cabinet – A specific cabinet location or the location where the cabinet's contents are archived.
4. The gauge displays the amount of available space. The values for the group gauge are based on the sum of the absolute values for the locations. Green indicates available space, yellow indicates space but approaching the threshold, and red indicates no usable space.
5. Below the gage is the total size of the disk space. The size is displayed in KB, MB, GB, or TB depending upon the size of the space.
6. A table displays the repository locations in the group. See the table above for more information on the column headings.
7. Click **Save settings** to save any changes.
8. In the **Info** tab, the group repository composition is displayed. A pie chart shows the percentage of current versions, prior versions, attachments, markups, files pending deletion, and cached documents.
9. Click **Close** ☒ to exit the group properties.

To edit location properties

1. Select the check box in a location row and click **Edit**.
2. In the **Definition** tab, modify the location name. The location is named “Default repository” by default when FileHold is installed.
3. The location path can be modified. Cut and paste the location into the field. To refresh the logical drive for the path, click **Refresh** ↻. To restore the previous location, click **Restore** ↩.

WARNING: The Full Text Search index is re-initialized after applying any changes such as a change in repository path.

4. The **Allow new files** check box is enabled by default. This allows FileHold to add new files to the locations. If disabled, files cannot be added to the location. For example, if the location no longer has free space, then the check box should be disabled.
5. The gauge displays the amount of available space. The values for the group gauge are based on the sum of the absolute values for the locations. Green indicates available space, yellow indicates space but approaching the threshold, and red indicates no usable space. The colours on the gauge changes depending upon the free space and warning thresholds.
6. Below the gage is the total size of the disk space. The size is displayed in KB, MB, GB, or TB depending upon the size of the space.
7. The Free space threshold sets how much space must left on the disk before it is considered full. When the location reaches the threshold, it is not possible to add any files to the system. The free space threshold cannot be set lower than 10% of the total space. See Free Space Threshold for more information. A value can be entered directly in the field or the slider can be used to set the value.
8. The Warning threshold determines how much space is left before the system administrator receives a warning message about running out of repository space. See Free Space Threshold for more information. A value can be entered directly in the field or the slider can be used to set the value.
9. Click **Save settings** to save any changes.
10. In the **Info** tab, the location composition is displayed. A pie chart shows the percentage of current versions, prior versions, attachments, markups, files pending deletion, and cached documents. The Info tab appears once a document has been added to the repository.
11. On the **Actions** tab, location files can be moved or deleted. This feature is only available if the Enhanced repository feature has been purchased. See Enhanced repository locations for more information.
12. Click **Close** ☒ to exit the location properties.

14.2. IMPORTANT CONSIDERATIONS WHEN PLANNING REPOSITORIES

1. Do not use file and or folder compression on any of the FileHold data directories such as the document repository, full text search index, or the user role manager data.
2. The FileHold service account must have full access to the repository location.
3. Once a repository location has been added, new files are added to it immediately. Repositories containing files cannot be deleted.
4. End users should never have access to the document repository locations for any reason. This is a location that only server administrator, data backup, and the FileHold service users should have access to. It is the responsibility of each FileHold customer to secure all the FileHold data locations so that end users are not able to directly modify documents. Damage caused by failure to protect the FileHold data locations is not covered by FileCare and results in consulting charges if FileHold is asked to attempt to repair the damage.
5. The FileHold data directories must be backed up nightly, along with the four (4) SQL Databases and four (4) SQL Log files that comprise the FileHold system. Please refer to the FileHold backup and recovery guide located here for more information on backups.

14.3. FREE SPACE THRESHOLD

The free space threshold is the point at which files can no longer be added to a repository location. The warning threshold is the point at which a system administrator receives a warning message that the repository is running out of space. When a location reaches the threshold, it is not possible to add any files to the system and all uploads fail with an error message.

The free space threshold minimum value can be changed by a Windows administrator. By default, it is set to 10%. The threshold value cannot be set lower than 10%. To set the minimum threshold level, modify the key “MinimumFreeSpaceThreshold” in the web.config file in *C:\Program Files\FileHold Systems\Application Server\DocumentRepository*.

TIP: It is generally considered important to leave space free on your drive to ensure it is operating with good performance. The actual amount of space needed varies depending on a number of factors. You should consult with your drive supplier to determine the best value for minimum free space. There are a number of Internet discussions available on the topic of minimum free space.

If the Enhanced repository feature has been purchased, a new location can be added to the system or an administrator can increase the amount of free space on one of the disks if using a virtual server environment. Repositories should be regularly monitored to ensure they have enough space to accommodate the needs of users. Contact FileHold support for remedies for a full repository.

TO CHANGE THE THRESHOLD OF THE REPOSITORY LOCATION

1. Go to **Administration Panel > System Configuration > Document Repository Locations**.
2. Select the location and click **Edit**.
3. Enter a new value in the **Free space threshold** field or use the slider. The value can be a percentage or absolute size. The unit of measure KB, MB, GB, or TB can be added to an absolute value to control the units. If an absolute size is entered it shows in megabytes. This cannot be less than 10% of the total space of the repository. The default is set to 10% 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. Enter a new value in the **Warning threshold** field or use the slider. The unit of measure KB, MB, GB, or TB can be added to an absolute value to control the units. If an absolute size is entered it shows in megabytes. By default, the warning threshold value is 15%.
5. The colours on the gauge changes depending upon the free space and warning thresholds. Green indicates available space, yellow indicates space but approaching the threshold, and red indicates no usable space.
6. Click **Save Settings**.
7. Click **Close** ☒ to exit the location properties.

14.4. ENHANCED REPOSITORY LOCATIONS

The document repository can be split into multiple locations to improve scalability. A system administrator can define the physical location for the documents in the library. For example, documents in a particular cabinet, such as Human Resources, can have its own repository location. The library archive can also have a separate repository location defined since they may fall under IT policies that allow for less expensive storage and backup. The ability to have multiple repository locations is controlled by a licensing option “Enhanced Repository”.

Groups are created to categorize the repository locations. Each group can have preferred contents:

- The library archive.
- A specific cabinet or the location when the cabinet's contents are archived.
- One group must be defined as the default group to use when no preferred group matches the file being added

When a file is added to FileHold, the list of preferences is checked to which group it belongs in. If there is no matching group, the file is placed in the default group. Document version associated files such as markups or cached files are placed according to their document version. Attachments not related to specific documents such as Workflow or Courier, are placed in the default group.

Repositories that have been marked as read only do not have files added to them; files can only be downloaded.

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

Files in a particular repository location can be moved to a preferred or default group. Files are moved as a batch and can be viewed in the Batch Jobs report.

14.4.1. Adding groups and locations

This feature requires "Enhanced repository" to be enabled in the license. Contact sales@filehold.com to purchase this feature.

To add a repository group

1. In the Web Client, go to Administration Panel > System Configuration > Document repository locations.
2. Click **Add** ➕ and select Group.
3. Enter a **Group name**.
4. Select a **Document preference**. This is the type of preferred contents. When a file is added to FileHold, the list of preferences is checked to see which group it belongs in. If there is no matching group, the file is placed in the default group. Document version associated files such as markups or cached files are placed according to their document version. Attachments not related to specific documents such as workflow or Courier attachments are placed in the default group.

- Default - used when no preferred group matches the file being added. "Default" is the default value when FileHold is installed.
- Archive - library archive documents.
- Cabinet - a specific cabinet location or the location where the cabinet's contents are archived.

5. Click **Add**.
6. Click **Close** ☒ to exit the group properties.

To add a repository location

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

2. Click **Add** ➕ and select **Location**.
3. Enter a **Location name**.
4. Enter the path to the location. To refresh the logical drive for the path, click **Refresh** ↻.

   NOTE: The FH Service account may need full control permissions to this location.
5. Click **Add**. The screen is modified automatically to show the Definition tab.
6. The **Allow new files** check box is enabled by default. This allows FileHold to add new files to the locations. If disabled, files cannot be added to the location. For example, if the location no longer has free space, then the check box should be disabled.
7. The gauge displays the amount of available space. The values for the group gauge are based on the sum of the absolute values for the locations. Green indicates available space, yellow indicates space but approaching the threshold, and red indicates no usable space. The colours on the gauge changes depending upon the free space and warning thresholds.
8. Below the gage is the total size of the disk space. The size is displayed in KB, MB, GB, or TB depending upon the size of the space.
9. The Free space threshold sets how much space must left on the disk before it is considered full. When the location reaches the threshold, it is not possible to add any files to the system. The free space threshold cannot be set lower than 10% of the total space. See Free Space Threshold for more information. A value can be entered directly in the field or the slider can be used to set the value.
10. The Warning threshold determines how much space is left before the system administrator receives a warning message about running out of repository space. See Free Space Threshold for more information. A value can be entered directly in the field or the slider can be used to set the value.
11. If adjustments were made, click **Save settings**.
12. Click **Close** ☒ to return to the document repository list.

14.4.2. Deleting repository groups or locations

Repository groups can only be deleted if it contains no repository locations. A repository location can only be deleted if it is empty; in other words, there are no files.

If you attempt to delete a non-empty location or group, an error message is displayed.

If you need to delete a location but it is not empty, move the documents from the location to another location.

To delete a repository group or location

1. Select the repository group from the list.
2. Click **Delete** ✖.

14.4.3. Moving repository locations

There must be two or more groups before a repository can be moved. Multiple locations can be moved at once to another group. Groups cannot be moved.

When moving repositories, the “job” is placed into a queue to be processed. The batch job can be viewed in the Batch jobs report. Batches are sized for a combination of processing efficiency and responsiveness to commands. The size of the batch can be controlled by the parameter “EnhancedRepositoryMoveJobSize” in the web.config file in *C:\Program Files\FileHold Systems\Application Server\LibraryManager* which has a default of 500. By default, the actual move could happen at any time, but the queue can be set to process operations according to the scheduled task “FH process batch jobs”.

The Full Text Search index is not initialized after applying any changes such as moving files.

To move a location

1. From the Manage repository groups page, select the check box for the location to be moved.
2. Click **Move** .
3. In the Manage repository location screen, select the Action:
   - Move all files – Moves all files from that location.
   - Move non-preferred files – Moves only non-preferred files from that location.
4. Select the Destination group:
   - Preferred group
   - *<Group name>*
5. Click **Calculate** to calculate the number of files to be moved and the total size of the files.
6. Click **Add to queue**.
7. The documents are placed in a queue and are moved once processed. A summary of the batch move is displayed. Click **View batch job** to view the progress. See the Batch jobs report for more information.
8. Click **Close** ☒ to exit.

To pause or cancel a move

1. From the Manage batch job screen or the Batch jobs report, do one of the following:
   - Click **Cancel job** to cancel the move.
   - Click **Pause job** to postpone the move for a period of time.
2. Do one of the following:
   - Click **Close** in the Manage batch job screen to return to the summary.
   - Click **Details…** in the Batch jobs report to return to the job summary.
3. To resume a paused job, go to the Batch Jobs report and click **Resume job**.

15. CLIENT OPTIONS

The Client Options 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 are 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 are not overwritten upon saving the settings, unless the option is set to enforced.

Any changes made in the client options area are 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.

15.1. 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

See the *End User Guide* for more information on setting up alerts and reminders.

TO SET THE GLOBAL ALERT PREFERENCES

1. In the Web Client, go to **Administration Panel > System Configuration > Client Options > 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 are not able to modify this setting in their personal alert preferences. Administrators may be able to override any enforced preferences which is dependent upon the setting in System Configuration > 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 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 are 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 are changed and locked down (meaning they cannot be modified by the end user) except for possibly library administrators or higher.

15.2. 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 > System Configuration > Client Options > 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
Notification when transmission initiated by user is completed or completed. (This is a Courier notification)	Enabled Disabled	Enabled
Notification when transmission initiated by user is overdue. (This is a Courier notification)	Enabled Disabled	Enabled
Notification when one-time review is added to a workflow user is an observer of	Enabled Disabled	Enabled

Option	Values	Default Value
Notification when one-time review is added a workflow user initiated	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 are not able to modify this setting in their personal workflow preferences. Administrators may be able to override any enforced preferences which is dependent upon the setting in System Configuration > 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 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 are pushed out to all end users unless their workflow preferences have been previously modified. If the option is set to “enforced” then their preferences are changed and locked down (meaning they cannot be modified by the end user) except for possibly library administrators or higher.

15.3. 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 client options.

TO SET THE GLOBAL FASTFIND PREFERENCES

1. In the Web Client, go to **Administration Panel > System Configuration > Client Options > FastFind Preferences**.
2. Use the following table to set the global FastFind preferences for the document management software:

Option	Description	Values	Default Value
Enable FastFind	Enables the FastFind feature	Enabled Disabled	Disabled
Update FastFind templates when user logs in to FileHold	Updates any FastFind templates	Enabled Disabled	Disabled
Enable mouse search	Enables an on-the-fly screen scraper	Enabled Disabled	Disabled

Option	Description	Values	Default Value
Enable selection search	Enables a selection search where the highlighted word or phrase is searched on	Enabled Disabled	Disabled
Enable clipboard search	Enables a clipboard search	Enabled Disabled	Disabled
Enable screen OCR search	Enables a search based on the Click to Tag functionality.	Enabled Disabled	Disabled
Search using	File and metadata –When selected, a full text search is performed when a FastFind search is invoked. *<Saved quick search name>* – Select the quick search name from the list. This quick search is performed when a FastFind search is invoked.	File and metadata *<Saved quick search name>*	File and metadata

3. Select the **Enforce** check box next to the preference you want to be imposed on all users. Users are not able to modify this setting in their personal FastFind preferences. Administrators may be able to override any enforced preferences which is dependent upon the setting in System Configuration > 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 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 are pushed out to all end users unless their FastFind preferences have been previously modified. If the option is set to “enforced” then their preferences are changed and locked down (meaning they cannot be modified by the end user) except for possibly library administrators or higher.

15.4. 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 > System Configuration > Client Options > Misc Preferences**.
2. Use the following table to set the global miscellaneous preferences for the document management software:

Option	Description	Values	Default Value
Time zone	Set the default time zone for end users	<All time zones>	The time zone the local computer is set to use.
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
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
Short date format	Set the default short date format for the system and end users. See the Date and Time Format Identifiers table in the Knowledge Base for more information.	• M/d/yyyy • dd/MM/yyyy • yyyy-MM-dd	M/d/yyyy
Long date format	Set the default long date format for the system and end users. See the Date and Time Format Identifiers table in the Knowledge Base for more information.	• dddd, MMMM d, yyyy • dd MMMM yyyy • MMMM d, yyyy	dddd, MMMM d, yyyy
Short time format	Set the default short time format for the system and end users. See the Date and Time Format Identifiers table in the Knowledge Base for more information.	• h:mm tt • HH:mm • HHmm	h:mm tt

Option	Description	Values	Default Value
Long time format	Set the default long time format for the system and end users. See the Date and Time Format Identifiers table in the Knowledge Base for more information.	- h:mm:ss tt - HH:mm:ss - HHmmss	h:mm:ss tt

3. Select the **Enforce** check box next to the preference you want to be imposed on all users. Users are not able to modify this setting in their User preferences. Administrators may be able to override any enforced preferences which is dependent upon the setting in System Configuration > 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 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 are pushed out to all end users unless their User preferences have been previously modified. If the option is set to “enforced” then their preferences are changed and locked down (meaning they cannot be modified by the end user) except for possibly library administrators or higher.

15.5. 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 > System Configuration > Client Options > FDA Advanced Settings**.
2. Use the following table to set the global FDA Advanced Settings preferences for the document management software:

Option	Description	Values	Default Value
Show Welcome Screen at Startup	The screen that is displayed upon logging into the application	Enabled Disabled	Enabled
Default screen at startup	Determines the window that is displayed after log in	Blank Simple Search Advanced Search Inbox Tasks Calendar Dashboard	Blank

Option	Description	Values	Default Value
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	Documents are deleted from the working folder on your local machine after they are added to the library	Enabled Disabled	Disabled
By default delete documents that a user Checks In to FileHold	Documents are deleted from the working folder on your local machine after they are checked into the library	Enabled Disabled	Disabled
Prompt for Download Location when a user Makes Copies of Files	Allows you to select a location on your local machine to save your copied files	Enabled Disabled	Enabled
Prompt for Download Location when a user Checks Out Files	Allows you to select a location on your local machine to save your checked out files	Enabled Disabled	Enabled
Prompt user to remove files when sending them from the Inbox	A prompt asks you if you want to remove the files from your local machine when sending them from the Inbox	Enabled Disabled	Enabled
Automatically clean up user's working documents	Documents in the working documents folder are cleaned up automatically or with a prompt message depending if the option “Prompt before automatically cleaning up user’s working documents” is enabled. Local files that are in use by another process are not deleted and remain in the working documents and are processed the next time there is a trigger condition. Local files associated with electronic documents that are modified are not deleted. These files should be managed using manual check in or the working documents synchronization tool. Once the documents have been checked in / synchronized they are subject to the automatic deletion rules.	Enabled Disabled	Enabled

Option	Description	Values	Default Value
Prompt before automatically cleaning up user's working documents	A prompt asks the user if they want to remove the files in their working documents folder. The option "Automatically clean up user's working documents" must be enabled for this option to work. The prompts are dependent on the conditions enabled in the "Clean up working documents extended conditions" area or when a user exits the FDA.	Enabled Disabled	Disabled
Clean up working documents extended conditions	Documents are automatically cleaned up or the user is prompted to clean up their working documents upon the following if any of the following conditions are enabled. If no options are selected, then the working documents are removed when a user exits the FDA.	• When the FDA is minimized to the system tray. • When the user logs out. • When the FDA detects it has been disconnected from FileHold server. • When the FDA receives a message from Windows to shutdown.	Disabled
By default close documents that a user Adds/Checks In to FileHold	Documents are closed in their native application when it is checked in or added to the library	Enabled Disabled	Disabled
Auto-Send documents to Auto-Tagged folders	Documents in the Inbox are automatically sent to their location in the library if the folder is Auto-tagged. You do not need to click the Auto-File button.	Enabled Disabled	Disabled
Auto-Send documents after completing metadata	Documents in the Inbox are automatically sent to their location in the library after the metadata has been sent. You do not need to click the Send or Send All button.	Enabled Disabled	Disabled

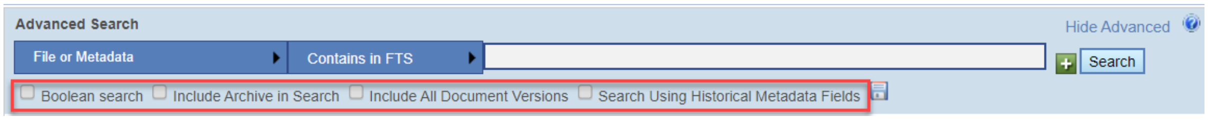
Option	Description	Values	Default Value
Move to recycle bin instead of permanently deleting	Documents that are set to be deleted after checking in or adding to the library are moved to the Recycle Bin on your local machine instead of being deleted.	Enabled Disabled	Disabled
Automatically open in the Viewer selected document in Inbox	Any selected document in the Inbox opens in the Viewer automatically. If this option is selected, only one tab is opened at a time. This prevents users from opening several tabs at a time and using up a lot of system memory in the process.	Enabled Disabled	Disabled
Automatically open in the Viewer selected document in folders and search results	Any selected document in the folder view or search results opens in the Viewer automatically. If this option is selected, only one tab is opened at a time. This prevents users from opening several tabs at a time and using up a lot of system memory in the process.	Enabled Disabled	Disabled
Open documents in the Document Viewer using separate tabs	Documents are opened in multiple tabs in the viewer	Enabled Disabled	Disabled
Allow opening one document in multiple tabs	A single document can be opened several times in multiple tabs using both Brava and PDF/Image viewers. *Starting in 2017, Brava viewer licenses are no longer available for new purchases. This information is retained for existing users only.*	Enabled Disabled	Disabled
Enable Smart Check In and Smart Check Out messages	Smart messages are the messages that appear when checking in and out a document using Microsoft Office applications.	Enabled Disabled	Enabled

Option	Description	Values	Default Value
Enable Click to Tag	When enabled, the Click To Tag button appears in the metadata pane and allows you to “click” or “rubber band” text, numbers, dates, etc. on the screen and inserts the value into the metadata field of the schema. If disabled, the Click to Tag button does not appear in the metadata pane.	Enabled Disabled	Disabled
Orientation of the thumbnail view - determines the location of the thumbnail position when using the PDF/Image viewer	Select the position of the thumbnails in the FileHold FDA viewer: Top, Bottom, Right or Left.	Top Bottom Left Right	Bottom
Format of document imports	If integrating with SmartSoft Capture, set to "Capture". If integrating with EMC Captiva QuickScan Pro, set to "Quick Scan Pro"	QuickScan Pro Capture	QuickScan Pro
Remain logged in even if no activity is performed	This option keeps your account logged into the system even if you are not using the client by sending a message to the server every minute to simulate user activity	Enabled Disabled	Disabled
Enable the old FDA PDF/Image viewer. This viewer is end-of-life. Transition your users to the FileHold viewer as soon as possible.	By default, the PDF/Image viewer is disabled in FileHold 16.2. To allow users to continue to use the PDF/Image viewer, enable this setting.	Enabled Disabled	Disabled

3. Select the **Enforce** check box next to the preference you want to be imposed on all users. Users are not able to modify this setting in their personal User preferences. Administrators may be able to override any enforced preferences which is dependent upon the setting in System Configuration > 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 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 are pushed out to all end users unless their preferences have been previously modified. If the option is set to “enforced” then their preferences are changed and locked down (meaning they cannot be modified by the end user) except for possibly library administrators or higher.

15.6. ADVANCED SEARCH OPTIONS

The Advanced Search options allow 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
Hide Advanced
File or Metadata
Contains in FTS
Search
□ Boolean search □ 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 > System Configuration > Client Options > 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
Boolean search	Searches using Boolean search options such as AND, OR, AND NOT. See the *End User Guide* for more information.	Enabled Disabled	Disabled
Include Archive in Search	Searches the documents in the library archive and includes any matches in the results. FileHold searches 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 only searches 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 are not able to modify this setting in their personal Advanced Search options. Administrators may be able to override any enforced preferences which is dependent upon the setting in System Configuration > 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 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 are 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

are changed and locked down (meaning they cannot be modified by the end user) except for possibly library administrators or higher.

16. SYSTEM ADMINISTRATION DASHBOARD

The system administration dashboard provides metrics about the operation and usage of the system. The elements or tiles in the dashboard displays a consolidated view of the following information

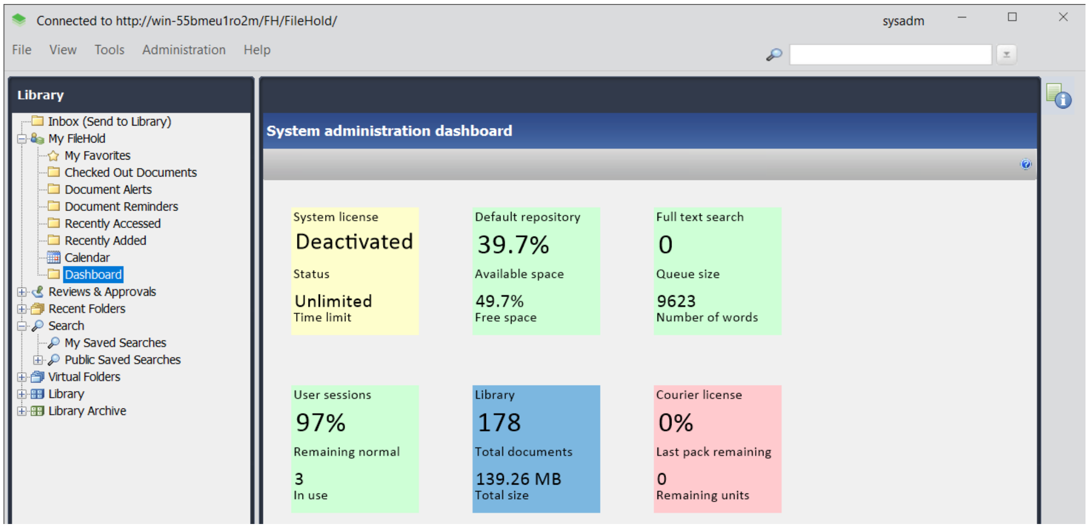
- System license
- Repository
- Full text search
- User sessions
- Library statistics
- Courier license

The colour of the tiles depends on the status of the dashboard element:

- Problem — red
- Warning — yellow
- Normal — green
- No thresholds — blue

The dashboard is located under My FileHold in both the FDA and Web Client. The dashboard can be made viewable by all users by enabling a permission setting. When enabled, the dashboard elements are hyperlinked for a user who belongs to the corresponding system role:

- System license — Links to licensing page and accessible to System Administrators role only
- Default Repository — Links to document repository locations and accessible to System Administrators role only
- Full text search — Links to full text search status page and accessible to Library Administrators role and above
- User sessions — Links to Manage users page and accessible to System Administrators role only
- Library — Links to library level statistics and accessible to Read only role and above
- Courier license — Links to list of Courier licenses and accessible to System Administrators role only



System administration dashboard

System license
Deactivated
Status
Unlimited
Time limit

Default repository
39.7%
Available space
49.7%
Free space

Full text search
0
Queue size
9623
Number of words

User sessions
97%
Remaining normal
3
In use

Library
178
Total documents
139.26 MB
Total size

Courier license
0%
Last pack remaining
0
Remaining units

To access the dashboard

1. In the FDA or Web Client, sign in as a system administrator. Note that the dashboard can be made viewable by all users by enabling a permission setting. See the following section.
2. Go to **My FileHold > Dashboard**. The following information is displayed:

Element	Description	Status/Threshold
System license	Status - Status of the license.	Activated (Green) Deactivated (Yellow) Disabled (Red)
	Time Limit- Date when the current license expires. Unlimited indicates that there is no date limit on license	
Repository	Available space – Percentage of total repository space (not including threshold) divided by the usable repository space (includes threshold) in bytes.	Normal threshold- greater or equal to 5%(Green) Warning threshold - between 1 to 5% (Yellow) Problem threshold - less than 1% (Red)
	Free space – Percentage of total repository storage space divided by the free storage repository space in bytes.	
Full text search	Queue size – Number of documents in the full text search queue.	Normal – less than or equal to 2 documents (Green) Warning – between 2 and 50 documents (Yellow) Problem – greater than or equal to 50 documents (Red)
	Number of words – Total number of words in the full text search index.	

Element	Description	Status/Threshold
User sessions	Remaining normal – Percentage of the number of licensed concurrent sessions divided by the actual concurrent sessions in use now. Guaranteed sessions count as in use.	Normal – greater than or equal to 10% (Green) Warning – between 2% and 10% (Yellow) Problem – less than or equal to 2% (Red)
	In use – Total number of concurrent sessions currently in use. Includes guaranteed sessions.	
Library	Total documents – Total number of documents in library. Does not include library archive or previous versions.	No threshold (Blue)
	Total size – Total size of the documents in the library. Does not include library archive or previous versions.	
Courier license	Last pack remaining– Percentage of last added Courier pack size divided by the available Courier units	Normal – greater than or equal to 25% (Green) Warning – between 15% and 25% (Yellow) Problem – less than 15% (Red)
	Remaining units – Number of Courier units available across all license packs. Does not include locked or cancelled packs.	

TO ENABLE THE DASHBOARD FOR ALL USERS

1. In the Web Client, go to **Administration Panel > System Configuration > Settings > General**.
2. In the Dashboard Settings area, select the **Allow dashboard to be visible to non-administration users**. When enabled, the dashboard can be seen by all users in their My FileHold area.

INDEX