



FileHold

Document & Record Lifecycle Software

SYSTEM ADMINISTRATION GUIDE

VERSION 12

Copyright ©2012 FileHold Systems Inc. All rights reserved.

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

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

Proprietary Notice

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

TABLE OF CONTENTS

1. OVERVIEW	3
1.1. SKILLS REQUIRED TO ADMINISTER THE SYSTEM	3
1.2. RESPONSIBILITIES OF THE SYSTEM ADMINISTRATOR.....	3
1.3. SETTING UP FILEHOLD SECURITY	4
2. LOG IN	5
3. SETTING UP USERS AND GROUPS	6
3.1. OVERVIEW	6
3.2. MANAGING ACCESS TO THE SYSTEM	7
3.3. CREATING LOCALLY MANAGED USERS	8
3.4. SYNCHRONIZING DOMAIN (ACTIVE DIRECTORY) USERS AND GROUPS	10
3.4.1. ADDING A DOMAIN USER / GROUP TO FILEHOLD	11
3.5. CREATING FILEHOLD GROUPS.....	12
3.5.1. USER ROLES AND ACCESSING THE LIBRARY	12
3.6. ADDING USERS TO GROUPS	14
3.7. VIEWING USER PROPERTIES	17
3.8. VIEWING GROUP PROPERTIES.....	18
3.9. SEARCHING FOR USERS.....	18
3.10. DELETING USERS.....	19
3.11. DELETING GROUPS	20
3.12. GUARANTEED USER ACCESS	20
3.13. RESET USER PASSWORD	21
3.14. SET VIEWER LICENSE.....	22
3.15. ENABLING AND DISABLING ACCOUNTS	22
4. LOGON AND PASSWORD SECURITY	23
5. USER SELF-REGISTRATION.....	24
6. GLOBAL SETTINGS.....	25
6.1. SETTING THE DEFAULT DOMAIN.....	25
6.2. REMOVING LICENSES FROM DISABLED USERS IN THE DOMAIN.....	26
6.3. SETTING OUTBOUND EMAIL SETTINGS.....	26
6.4. ENABLING THE DOCUMENT AND VERSION CONTROL FIELDS.....	27
6.5. DOCUMENT SHORTCUTS.....	27
6.6. SETTING THE PERMISSION SETTINGS	28
6.7. EVENT SCHEDULE SETTINGS.....	28

6.8. INSUFFICIENT CAL NOTIFICATION SETTINGS29

 6.8.1. INSUFFICIENT CAL LOG.....29

7. REPOSITORY LOCATIONS30

8. LICENSING31

9. ACTIVITY LOG32

10. SYSTEM AUDIT LOG32

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 [activity reports](#)

1.1. SKILLS REQUIRED TO ADMINISTER THE SYSTEM

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

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

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

1.2. RESPONSIBILITIES OF THE SYSTEM ADMINISTRATOR

System Administrators create the roles, groups and security settings that define the system in terms of permissions, access, and user rights. Library Administrators use these foundational

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

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

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

- Understand the document management systems System Administration by reading the System Administration guide and reviewing the training demos.
- Work with the Library Administrators on the creation of groups and permissions and roles these groups are assigned. Keep things simple at first. Remember it is easier to give users the minimum role required rather than retracting permissions in the future.

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

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

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

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

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

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

1.3. SETTING UP FILEHOLD SECURITY

You will need to evaluate the users of the system and group them into logical groups, such as Accounting, Marketing, Sales, and so on. You will also need to decide what level of access that

each group requires and assign the appropriate role to the group. For the list of security roles, see [User Roles and Accessing the Library on page 12](#).

FileHold has three levels of security:

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

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

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

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

2. LOG IN

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

The System Administration features in FDA include:

- Users
- FileHold Groups

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

TO LOGIN TO SYSTEM ADMINISTRATOR VIA THE WEB CLIENT

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

FileHold
Document & Record
Lifecycle Software.

Login *

Password *

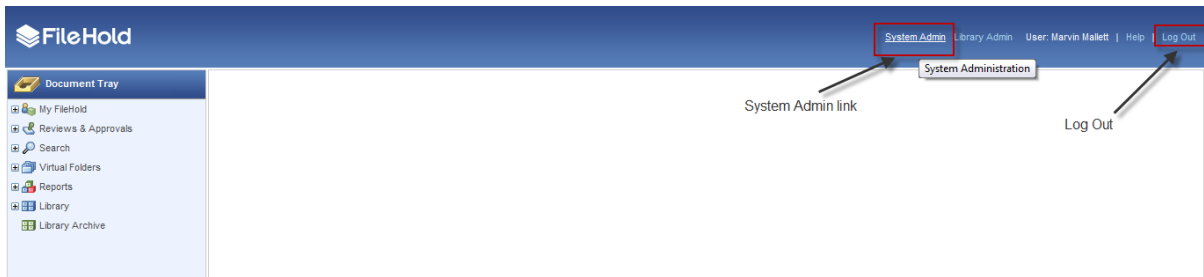
Domain * Local FileHold account

Log In

Logon with Windows Authentication

2. Enter your Login, Password, and select the domain (if required) and click [Log In](#).

3. Click the **System Admin** link at the top of the screen.



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

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

TO LOGIN AS SYSTEM ADMINISTRATOR VIA THE FDA

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

3. SETTING UP USERS AND GROUPS

System Administrators are responsible for the setting up and configuring of the FileHold users and group memberships. They create the roles, groups and security settings that define the document management system in terms of permissions, access and user rights. Library Administrators use these foundational settings to build the file structure and document categorization system that provides users with highly configurable schemas for different types of document.

The System Administrator should:

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

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

3.1. OVERVIEW

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

- Authentication identifies a user based on username and password.

- Authorization uses the authentication information to grant the appropriate level of access control to the content and other tools.

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

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

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

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

NOTE: If you are self-registering a group of people that have identical permissions and content access requirements internally then this temporary security precaution can be skipped entirely.

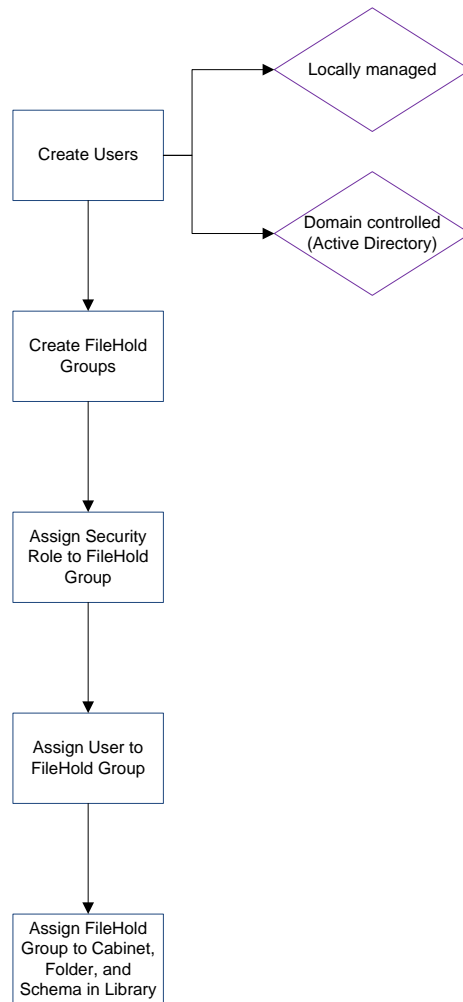
- Active Directory Synchronized Users are users that called FileHold Domain Users. Groups synchronized with Active Directory are called FileHold Domain Groups. The users and groups behave the same way as locally managed users when interacting FileHold. The difference is that the properties (contact information,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

3.2. MANAGING ACCESS TO THE SYSTEM

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

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

The following flowchart depicts how users and groups are set up in the system.



3.3. CREATING LOCALLY MANAGED USERS

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

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

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

A concurrent user is the total number of people allowed to use FileHold at the same time.

List of all FileHold users **Click a letter to filter by last name**

[A](#)
[B](#)
[D](#)
[G](#)
[I](#)
[L](#)
[M](#)
[N](#)
[O](#)
[P](#)
[Q](#)
[R](#)
[S](#)
[T](#)
[U](#)
[.....](#)

	Enabled	Guaranteed	Shared	Total
Registered Users	34	8	27	100
Concurrent Sessions				35
Insufficient CALs Events	0			
Enterprise Office Viewer Licenses	1	4		5
Enterprise Office Viewer With CAD Support Licenses	0	5		5
Enterprise Office Viewer (Engineering Edition) Licenses	2	3		5
PDF/Image Viewer Licenses	4	1		5
Guest User Sessions	5			
FileHold SP Client Sessions	5			

License summary area

Name	FileHold Account	Guaranteed Access	Viewer License	Source	FileHold Group	Last Modified
<input type="checkbox"/> alfonso AND ▶	Enabled	No	No Viewer	Locally managed account		11/24/2011 9:56:24 PM GMT
<input type="checkbox"/> alfonso basic user ▶	Enabled	No	No Viewer	Locally managed account		10/6/2011 7:58:23 PM GMT
<input type="checkbox"/> Alfonso ipad ▶	Enabled	Yes	No Viewer	Locally managed account System Administrators		10/6/2011 7:58:23 PM GMT
<input type="checkbox"/> Alfonso Safari ▶	Enabled	Yes	No Viewer	Locally managed account System Administrators		10/14/2011 4:50:18 PM GMT
<input type="checkbox"/> Basie Pie ▶	Enabled	No	No Viewer	Locally managed account Organizers		10/6/2011 7:58:23 PM GMT

TO CREATE A LOCALLY MANAGED USER

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

Add Locally Managed User

General	Account Settings	Member Of	Contact Information
<p>General</p> <p>First Name * <input type="text" value="Deborah"/></p> <p>Last Name * <input type="text" value="Dixon"/></p> <p>User Logon Name * <input type="text" value="ddixon"/></p> <p>E-mail * <input type="text" value="ddixon@filehold.com"/></p> <p>Default Language <input type="text" value="English"/></p> <p>Source <input type="text" value="This is a locally managed user account."/></p>			<p>Initials <input type="text" value="DD"/></p>

- Enter the password for the user twice and click **OK**.
- Select **Account Settings** and enter the following information under FileHold Account Options:
 - FileHold account is enabled for this user — Select this check box if the user account should be enabled.

- User has guaranteed system access — Select this check box if the user should have access to the system at all times. See Guaranteed User Access on page 20 for more information.
 - User must change password at next logon — Select this option if the user is to set their own password the next time they log into the system. This option is recommended.
7. In the FileHold Desktop Application Viewer Options area, select the viewer license (if purchased) for the user. For detailed information about the viewers, see www.filehold.com/help/home.
 - A viewer is not licensed for this user.
 - PDF/Image Viewer
 - Viewer 1 – Microsoft Office, PDF, and Image formats only
 - Viewer 2 - Microsoft Office, PDF, Image and AutoCAD formats
 - Viewer 3 – Microsoft Office, PDF, Image and all CAD formats
 8. In the Account Expiration area, select a date for the user account to expire or leave the default Never for the account to remain active indefinitely.
 9. Click **OK**.
 10. In the Member Of window, you will need to add the user to a group. See [Adding Users to Groups](#) for more information.
 11. Select Contact Information and enter the user's contact information such as addresses, phone numbers, and company information. This information is optional.
 12. Click **OK**.

3.4. SYNCHRONIZING DOMAIN (ACTIVE DIRECTORY) USERS AND GROUPS

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

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

Domain groups can be assigned to FileHold Groups that can in turn be given access (membership) to specific content located throughout the Library. Synchronization of a domain group will allow a new user added to the domain group at the Active Directory level to be automatically provisioned to all areas of FileHold based on the pre-defined permissions of their FileHold groups.

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

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

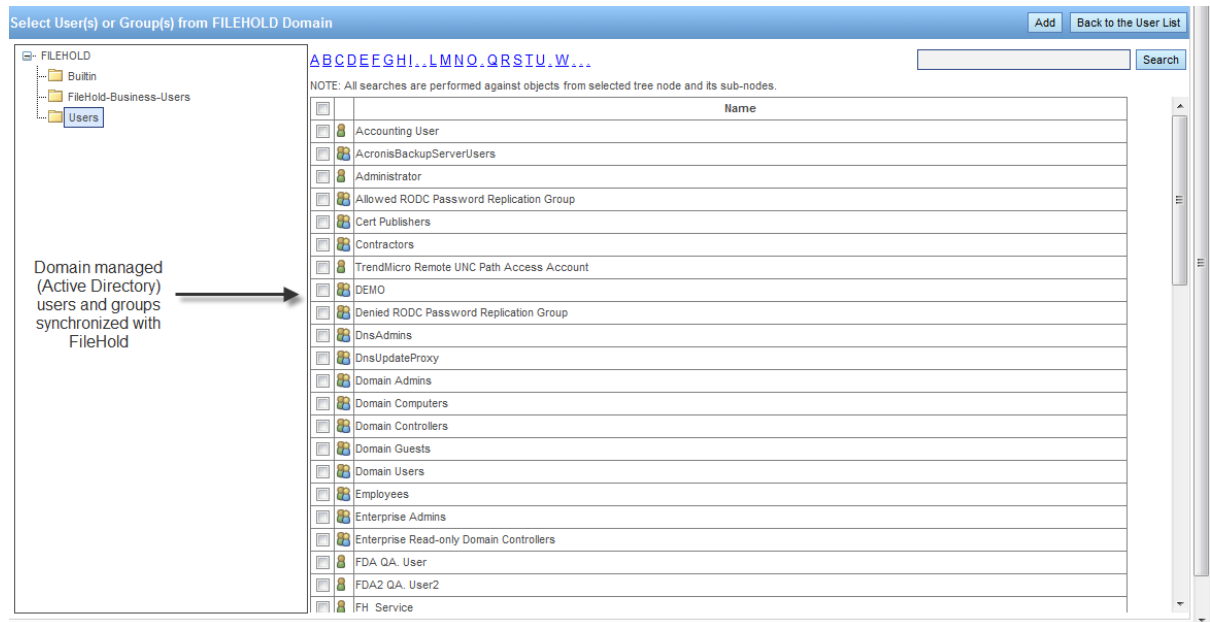
3.4.1. Adding a Domain User / Group to FileHold

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

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

TO ADD A DOMAIN USER OR GROUP TO FILEHOLD

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



- In the Add Domain Group Options, select one of the following and click **OK**:
 - Add the group and the group members. Keep both synchronized with the domain.
 - Add just the group members and do not add the group. Only the user accounts will still be synchronized with the domain.
- At the Add User(s) and Group(s) Confirmation, click **OK**.
- Continue to add more users and groups to FileHold.

10. To return to the user list, click [Back to the User List](#).

3.5. CREATING FILEHOLD GROUPS

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

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

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

TO CREATE A FILEHOLD GROUP

1. In the Web Client, log in to the System Admin area and select [User and Group Management > FileHold Groups](#).
 - Alternatively, in FDA, log in with System Administrator rights and go to [Administration > User & Group Management > FileHold Groups](#).
2. Click [Add Group](#).

The list of FileHold groups that come standard with the product are shown. 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 deleted once your own groups are created.
3. Enter the following information:
 - Group Name — Enter a name for the group.
 - Description — Enter a description for the group.
 - Role — Select a role from the list. See [User Roles and Accessing the Library for descriptions](#).
 - Notes — Enter any additional information about the group.
 - FileHold Group Members — Select [Display all members on one page](#) check box to display all the members on a single page. Click [Add Members](#) to add user to the group. See [Adding Users to Groups](#) for more information.
 - Restrictions — Select the [Disable emailing documents](#) check box if users will not be able to email documents from FileHold.
4. Click [OK](#). The group is added to the list.

3.5.1. User Roles and Accessing the Library

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

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

User Role	Description
Guest User	<p>A Guest User has read-only rights. Guest user accounts allow you to share a single account with multiple users. You can log into FileHold or a Guest Portal (Self-Service Portal) with a guest user account.</p> <p>The Guest Portal is an optional module that allows people to access the document repository without the need to purchase a fully registered license. You can purchase guest user licenses in blocks of 50. You can configure the portal so that it does not require a login. The user simply visits the URL and the portal page appears. For more information on the Guest Portal, see the FileHold website.</p>
Read Only	A Read-Only user role may only download or open and read documents from FileHold. They cannot edit, delete, or create documents. They can email documents if given this functionality by system administrators.
Document Publisher	Document Publisher user role can read, add documents that are owned by them, check-in/check-out, and edit documents and metadata. They cannot delete any documents including those which they have added to the system.
Document Publisher + Delete	Document Publisher Plus Delete user role can do everything a Document Publisher can do and delete their documents.
Publisher	<p>Publisher user role can do everything a Document Publisher can do plus:</p> <ul style="list-style-type: none"> • Create new folders and folder groups. • Copy or move folders and folder groups they have already created. • Clone folders and folder groups created by other users and become the owners of the folders / folder groups. <p>Publishers cannot delete existing documents, folders or folder groups including those which they have added /created. All documents and folders created by the Publisher will be owned by them and they cannot change the ownership.</p>
Publisher + Delete	Publisher plus Delete user role can do everything that a Publisher can do plus delete documents, folders and folders group owned (created) by them.
Organizer	<p>Organizer role user can:</p> <ul style="list-style-type: none"> • Move all documents (which they have an access to) in other places in the library including the documents which they do not own. • Move, copy or clone all folders and folder groups regardless of their ownership. In case of cloning they will become the owners of folder / folder groups. In case of copying and moving the original ownership of folders / folder groups is preserved. • Add folders / folder groups (they are the owners) and rename folders and folder groups. • Organizers can delete their own documents. <p>The Organizer role is for users who are responsible for organizing documents that are scanned or imported into the system or who are assigned to organize documents added by other users. For example, organizers would move the documents generated by scanner operators to their correct folder in the library. Only trusted personnel should be given this role.</p>

User Role	Description
Organizer + Delete	Organizer plus Delete role can do everything that Organizers can do plus delete all documents, folders and folder groups regardless of their ownership. This organizer and delete role can only do this within Cabinets, Folders and Schemas that they are a member of. This role should be used by trusted personnel only.
Cabinet Administration	Cabinet Administrators can only administer the cabinets that they own; they cannot create cabinets for themselves. They can: <ul style="list-style-type: none"> • Create, edit, and delete drawers, folder groups and folders and manage their properties (i.e. membership structure). • Access all documents (in Publisher and Delete capacity) from anywhere in the library structure unless they are restricted from that area of the library structure. If they do not have access to the Cabinet, Folder and Schema, they will not be able to access the documents.
Library Administration	Library Administrators can perform, within their cabinets, the same functions as Cabinet Administrators plus: <ul style="list-style-type: none"> • Create cabinets and manage them in the Library. • Full access to FileHold's Library Administrator where they can manage metadata fields, schemas, events, set up workflow templates, manage numerous global settings (i.e. viewer permissions, search engine settings, reporting services permissions and more), perform various managerial functions such (as check-in for user, change document owner, recover deleted document etc.) and access many useful reports and usage logs. <p>Library Administrators cannot create cabinets for Cabinet Administrators to own.</p>
Senior Library Administration	Senior Library Administrators have full control of the FileHold library itself and Library Administration area. Senior Library Administrators can create cabinets to be managed by any Library Administrator or Cabinet Administrator.
System Administration	System Administrators have complete control of the system. They can perform all of the functions of all other roles. However, the main tasks of the System Administrators are to add users to the system (including assigning the initial password and setting requirements for all new passwords and ability to self register), assign users to their appropriate groups, enable document control numbers and version control numbers, manage user accounts, user groups and the system license pool. The System Administrator also has access to various global settings (outbound email, system wide configurations for managing the various documents format conversion permissions etc.) and as well as user activity reports.

NOTE: All roles provide document emailing capability. This can be disabled on a role by role basis by a System Administrator in the FileHold Groups area.

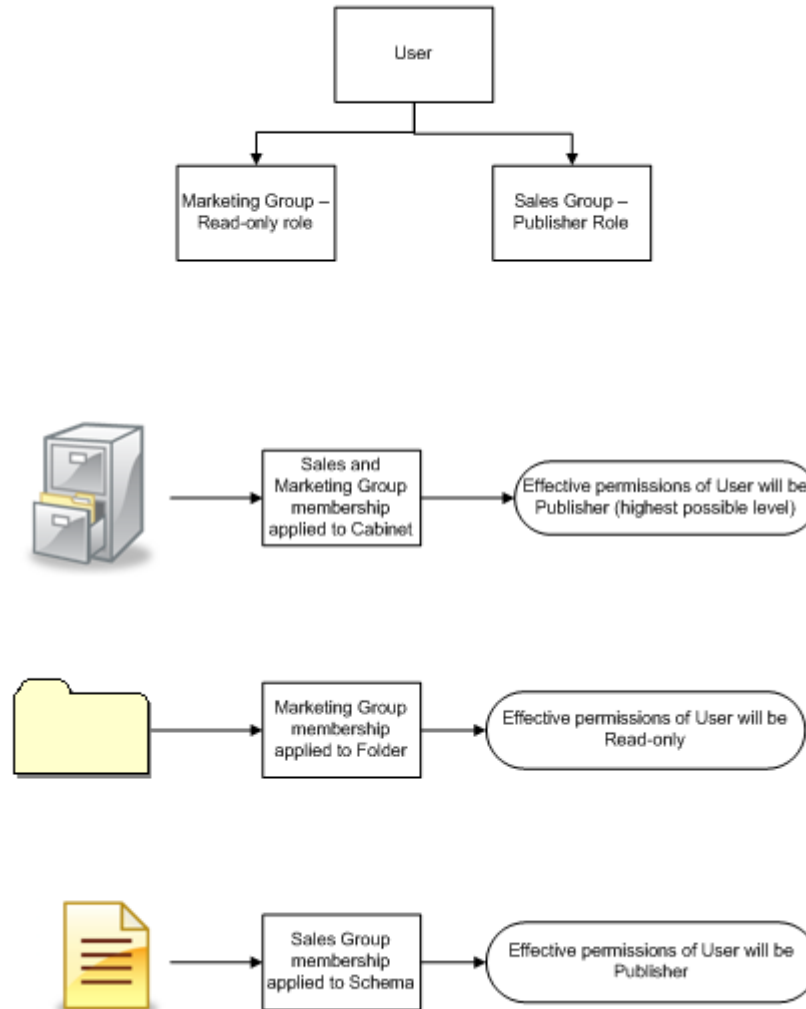
3.6. ADDING USERS TO GROUPS

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

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

easier to add and remove users from groups than it is to locate the Cabinets, Folders, and Schemas of individual users.

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



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

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

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

- [Selecting a group from the FileHold Group list and selecting Add Members.](#)
- [Selecting a group from the FileHold Group list and selecting Properties > Add Members.](#)

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

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

FileHold Group Name	Role	Description
<input checked="" type="checkbox"/> Accounting Dept	Publisher	Accounting group
<input type="checkbox"/> Cabinet Administrators	Cabinet Administration	
<input type="checkbox"/> Document Editors	Document Publisher & Delete	
<input type="checkbox"/> Document Publishers	Document Publisher	
<input type="checkbox"/> Editors	Publisher & Delete	
<input type="checkbox"/> Guest Users	Guest User	
<input type="checkbox"/> Library Administrators	Library Administration	
<input type="checkbox"/> Organizers	Organizer	
<input type="checkbox"/> Organizers & Delete	Organizer & Delete	
<input type="checkbox"/> Publishers	Publisher	
<input type="checkbox"/> Read Only	Read Only	
<input type="checkbox"/> Senior Library Administrators	Senior Library Administration	
<input type="checkbox"/> System Administrators	System Administration	

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

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

FileHold Group Name	Role	Description
Library Administrators	Library Administration	

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

TO ADD USERS TO A GROUP FROM THE GROUP LIST

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

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

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

TO ADD USERS TO GROUP USING THE GROUP PROPERTIES

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

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

3.7. VIEWING USER PROPERTIES

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

TO VIEW USER PROPERTIES

1. In the System Administration area, go to **User and Group Management > Users** and click on a user name.
 - Alternatively, in the Web Client, you can select **Properties** from the drop-down menu.

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

3.8. VIEWING GROUP PROPERTIES

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

TO VIEW GROUP PROPERTIES


- In the System Administration area, go to **User and Group Management > FileHold Groups** and click on a group name.
 - Alternatively, in the Web Client, you can select **Properties** from the drop-down menu.
- Update or view the group name, description, role, notes, group members and restrictions for the user and click **OK**.

3.9. SEARCHING FOR USERS

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




TO SEARCH FOR A USER

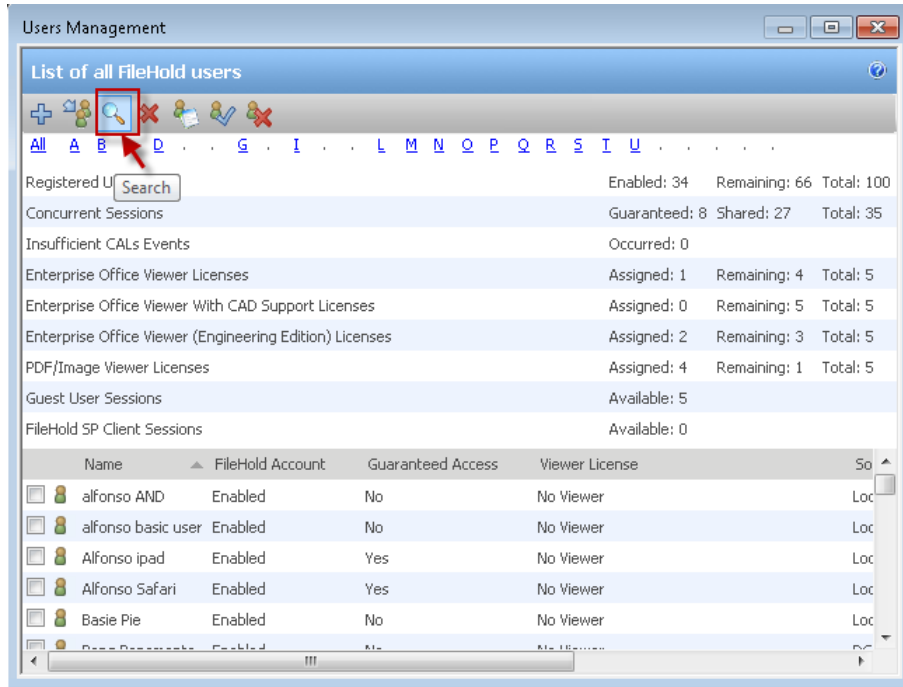
- In System Administration area in both the Web Client and FDA, go to **User and Group Management > Users** and click **Search**.

List of all FileHold users 

[A,B,D,.....LMN,P,RS,....Y.](#)

Registered Users	Enabled: 16	Remaining: 74	Total: 90
Concurrent Sessions	Guaranteed: 2	Shared: 28	Total: 30
Enterprise Office Viewer Licenses	Assigned: 2	Remaining: 8	Total: 10
Enterprise Office Viewer With CAD Support Licenses	Assigned: 1	Remaining: 9	Total: 10
Enterprise Office Viewer (Engineering Edition) Licenses	Assigned: 2	Remaining: 8	Total: 10
Guest User Sessions	Available: 5		
FileHold SP Client Sessions	Available: 5		

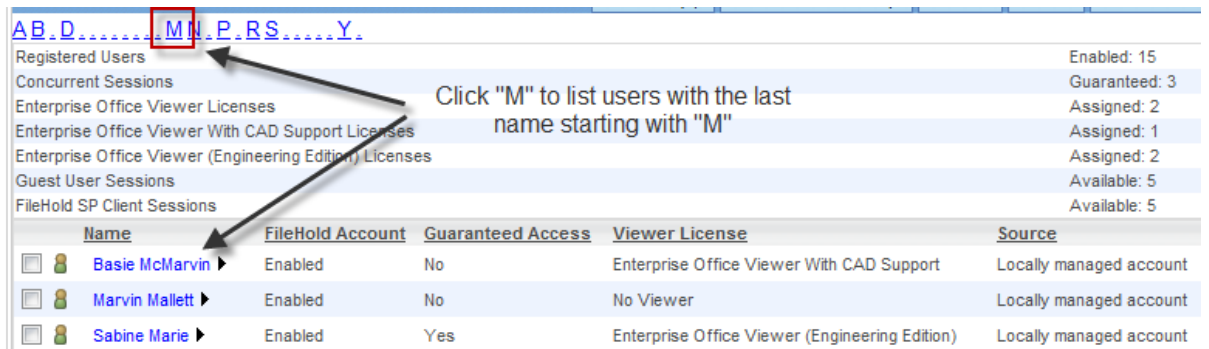
Name	FileHold Account	Guaranteed Access	Viewer License	Source	FileHold Group	Last Modified
 Administrator ▶	Enabled	No	No Viewer	FILEHOLD Domain		2/28/2011 5:05:18 PM GMT
 Basie McMarvin ▶	Enabled	No	Enterprise Office Viewer With CAD Support	Locally managed account	Accounting Dept, Library Administrators	2/16/2011 10:40:12 PM GMT
 Cabinet Administrator ▶	Enabled	No	No Viewer	Locally managed account	Cabinet Administrators	12/6/2010 9:05:03 PM GMT



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

TO SEARCH BY LAST NAME

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



3.10. DELETING USERS

Deleting a user from the system removes the user account and any ownership of their documents. It is recommended that you do not delete a user because their files may not be visible to any other users. Instead, you should [disable](#) a user account.

NOTE: If you must delete the user account, be sure to use the Change Document Owner and Change Cabinet/Folder Owner features in the Library Administration area to give the cabinets,

folders, and documents a new owner. See the *Library Administration Guide* for more information.

TO DELETE A USER ACCOUNT

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

3.11. DELETING GROUPS

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

TO DELETE A GROUP

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

3.12. GUARANTEED USER ACCESS

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

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

TO GUARANTEE A USER ACCOUNT

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

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

→ Status will change to Yes

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

Users Management

List of all FileHold users

Registered Users: Enabled: 34 Remaining: 66 Total: 100

Concurrent Sessions: Guaranteed: 8 Shared: 27 Total: 35

Insufficient CALs Events: Occurred: 0

Enterprise Office Viewer Licenses: Assigned: 1 Remaining: 4 Total: 5

Enterprise Office Viewer With CAD Support Licenses: Assigned: 0 Remaining: 5 Total: 5

Enterprise Office Viewer (Engineering Edition) Licenses: Assigned: 2 Remaining: 3 Total: 5

PDF/Image Viewer Licenses: Assigned: 4 Remaining: 1 Total: 5

Guest User Sessions: Available: 5

FileHold SP Client Sessions: Available: 0

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

TO REMOVE GUARANTEED USER ACCOUNT ACCESS

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

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

→ Status will change to No

3.13. RESET USER PASSWORD

You can reset a user password if they have lost or forgotten it.

TO RESET A USER PASSWORD

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

3.14. SET VIEWER LICENSE


FileHold has an option to license a Brava viewer to open, preview make annotations or mark up documents. In order to use the document viewer feature, users will have to be issued a license.

There are three types of viewer licenses:

- Level 1 — Enterprise Office Viewer for viewing of Microsoft Office, PDF, and image file formats.
- Level 2 — Enterprise Office Viewer with CAD support for viewing of Microsoft Office, PDF, image file, and AutoCAD formats.
- Level3 — Enterprise Office Viewer Engineering Edition for viewing of Microsoft Office, PDF, image file, and all CAD formats

In order to be granted a license for the Brava Document Viewer a user must first be added to the system.

TO SET A VIEWER LICENSE FOR A USER

1. In Web Client, go to **User and Group Management > Users** and do one of the following:
 - Click the ► next to the user name and select **Properties > Account Settings**.
 - Select the check box next to a user name and click **Set Viewer License**.
2. In FDA, go to **Administration > User & Group Management > Users**.
 - Select the check box next to the user name and click **Set Viewer License** .
3. Select one of the license options from the list:
 - A viewer is not licensed for this user.
 - Viewer 1 – Microsoft Office, PDF, and Image formats only
 - Viewer 2 - Microsoft Office, PDF, Image and AutoCAD formats
 - Viewer 3 – Microsoft Office, PDF, Image and all CAD formats
4. Click **OK**.

3.15. ENABLING AND DISABLING ACCOUNTS

When an employee joins or leaves an organization they will need to have a user account enabled or disabled. In other situations, users may continue to work for an organization but simply no longer need access to FileHold. Enabling and disabling user accounts lets the


Systems Administrator create and disable user access to the system without having to [delete user accounts](#).

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


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

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

TO ENABLE A USER ACCOUNT

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

TO DISABLE USER ACCOUNT

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

4. LOGON AND PASSWORD SECURITY

The logon settings allow the System Administrator to manage the number of logon attempts before the account is locked and the time-out settings for user sessions.

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

TO SET THE LOGON AND PASSWORD SECURITY SETTINGS

1. Go to **User and Group Management > Logon and Password Security**.
2. Enter the number of logon attempts allowed. The user will be locked out of the system after the number of login attempts has been exceeded.
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 licenses for other users.

WARNING: The following section applies to only locally managed users.

4. In the Password Settings for Locally Managed Users area, enter the minimum number of characters for the password.
5. Select one or more of the following options:
 - Must contain a number
 - Must contain a special character
 - Must contain at least one upper case letter
 - Must contain at least one lower case letter
 - Allow password re-use
6. Enter the number of days that the password expires. Enter 0 if the password is not to expire.

The screenshot shows a configuration window titled "Logon & Password Security Settings". It is divided into two main sections. The first section, "Logon & Password Security Settings", contains two input fields: "Logon attempts allowed" with a value of 10 and "Log inactive users off after" with a value of 200. The second section, "Password Settings for Locally Managed Users", contains a "Minimum number of characters" field with a value of 5, and five checkboxes: "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", and "Allow password re-use". Below these is a "Password expires after" field with a value of 0 days, and a note: "Please enter 0 (zero) in this field if you want the password to Never Expire". At the bottom of the window are "Update" and "Cancel" buttons.

7. Click **Update**.

5. USER SELF-REGISTRATION

System Administrators can allow users to self-register an account in the FileHold system. 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.

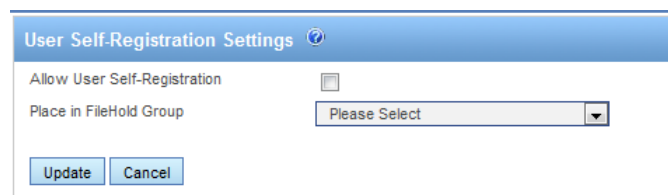
- The system is being used by a small organization that does not have or plan to use Active Directory to manage the users. This provides access while limiting administrator burden to create user accounts.
- The system is occasionally accessed by casual users who may only logon a few times per year. On-demand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

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

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

TO SET UP SELF-REGISTERED USERS

1. Go to User and Group Management > FileHold Groups.
2. Create a new group for the self-registered users. See [Creating FileHold Groups on page 12](#) for more information.
3. Go to [User and Group Management > User Self-Registration](#).



The screenshot shows a dialog box titled "User Self-Registration Settings". It has a blue header bar with the title and a help icon. Below the header, there are two settings: "Allow User Self-Registration" with a checked checkbox, and "Place in FileHold Group" with a dropdown menu showing "Please Select". At the bottom of the dialog are two buttons: "Update" and "Cancel".

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

6. GLOBAL SETTINGS

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

6.1. SETTING THE DEFAULT DOMAIN

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

Log In

FileHold
Document & Record
Lifecycle Software.

Login *

Password *

Domain * FILEHOLD

Log In

TO SET THE DEFAULT DOMAIN

1. Go to **Global Settings > General**.
2. In the Select Default Domain area, select a domain from the list or “none selected”.
3. Click **Update**.

6.2. REMOVING LICENSES FROM DISABLED USERS IN THE DOMAIN

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

TO REMOVE A LICENSE FROM A DISABLED DOMAIN USER

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

6.3. SETTING OUTBOUND EMAIL SETTINGS

FileHold requires access to your SMTP server which is part of an Email server. FileHold uses the SMTP port / service to relay messages. Setting the outbound email settings allows user to receive alerts and reminders on folders and documents via email. Alert settings for users can be set in **File > Preferences & Settings > Alert Preferences** from the FileHold Desktop Application. See the *User Guide* for more information.

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

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

TO SET THE OUTBOUND EMAIL SETTINGS

1. Go to **Global Settings > General**.
2. In the Outbound Email Settings area, enter the FileHold account name. The email account FileHold uses to send outbound emails will need to be created in your email server settings.
3. Enter the outgoing SMTP server address.
4. Enter the SMTP server port number.

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.

5. Select the SMTP Server Requires Authentication check box, if applicable.

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 SMTP Authentication Settings**.
10. Test your work. Go to the Web Client, and test emailing a document from FileHold to yourself. If you do not get the email, then you should work with your email and network administrator to further troubleshoot your configuration.

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

6.4. ENABLING THE DOCUMENT AND VERSION CONTROL FIELDS

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

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

TO ENABLE CONTROL FIELDS

1. Go to **Global Settings > General > Document/Version Control Fields** area.
2. Select the Enable Document Control Fields check box, if applicable.
3. Select the Enable Version Control Fields check box, if applicable.
4. Click **Update**.

6.5. DOCUMENT SHORTCUTS

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

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

There are several workarounds for shortcuts such as:

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

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

TO DISABLE/ENABLE DOCUMENT SHORTCUTS

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

6.6. SETTING THE PERMISSION SETTINGS

Permission settings allow users to do certain functions such as convert between electronic documents and records, convert offline documents to electronic documents, archive and remove documents from the archive, and allow non-document owners to initialize workflows.

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

TO SET USER PERMISSION SETTINGS

1. Go to **Global Settings > General > Permission Settings** area.
2. Select the following options:
 - Enable converting between electronic documents and records
 - Enable converting offline documents to electronic records
 - Enable converting electronic documents to offline documents
 - Enable manually archiving documents
 - Enable manually unarchiving documents
 - Allow non document version owners to initialize workflows - Allows users that are not owners of a document to kick-off a workflow.
 - Enable editing document metadata when workflow is active - Allows metadata to be edited for a document that is under the workflow process.
 - Allow the creator of a document to modify the initial value of read-only fields – Allows the document creator (owner) to modify a read-only custom date or blank date metadata field after the document has been added to the Library. For more information, see the *Library Administration Guide* or the [Knowledge Base](#).
3. Click **Update**.

6.7. EVENT SCHEDULE SETTINGS

You can configure the system to automatically delete, archive, or convert documents to records for a particular schema.

- Delete — “Soft” deletes a document based on the event schedule date. The document can still be recovered in the “soft” deletion state. For more information on deleting documents, see the *Library Administration Guide*.
- Archive — The document is moved to the Library Archive in the hierarchy.
- Convert to Record — The document is no longer editable but remains in the library.


In order to use the events features, the System Administrator must enable them. Library Administrators can then create and apply events to schemas.

TO ENABLE EVENT SCHEDULES

1. Log in as System Administrator, and go to **System Admin > Global Settings > General**.
2. In the Event Schedule Settings area, select the following check boxes, if applicable:
 - Enable Convert to Record Events — Select to allow documents to be automatically converted to a record after a specified period of time.
 - Enable Archive Events — Select to allow documents to be automatically sent to the archive after a specified period of time.
 - Enable Delete Events — Select to allow documents to be automatically deleted after a specified period of time.
3. Click **Update**.

6.8. INSUFFICIENT CAL NOTIFICATION SETTINGS

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

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

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

TO SET THE EMAIL NOTIFICATION OF INSUFFICIENT CALS

1. Go to **System Administration > Global Settings > General > Insufficient CAL Notification Settings**.
2. In the Notification Interval field, select **Daily** or **Weekly**.
3. In the Recipients field, select **None**, **System Administrators Only**, or **Library and System Administrators**.

6.8.1. Insufficient CAL Log

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

TO RUN THE INSUFFICIENT CAL LOG

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

7. REPOSITORY LOCATIONS

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

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

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

When all locations reach the threshold, it is not possible to add any files to the system and all uploads fail with an error message. The System Administrator should immediately add a new location to the system or to provide more free space on one of the disks.

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

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

TO ACCESS THE REPOSITORY LOCATIONS

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

TO ADD A REPOSITORY LOCATION

1. Click [Add Repository](#).
2. Enter the following information and click **OK** when finished:

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

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

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

8. LICENSING

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.

In order to process the sales request, you will need to send your FileHold server's unique hardware key to sales@filehold.com. You will receive a license file and can upload the key in the License Information area.

The License Information area displays all the enabled features, number of licenses, number of viewers, the software version, hardware key, and other information pertaining to the license.

System information ?

Is system activated	True
System Version	FileHold 12.0.0
Build	FileHold12_20111004.1
Hardware key	195836112491901240479725
Machine name	QA-2008R2STD64Q
Domain name	DC2008.QA

Send a copy of the Hardware key to sales@filehold.com to get a new license

Information about the license

Please visit this help article page to learn how to license the system after installation, or to request a new license. [?](#)

You must send the hardware key and details to sales@filehold.com as per the support article instructions to receive a license.

Registered to	Quality Assurance
Concurrent sessions	35
Named user number	100
Guest user sessions	5
FileHold SP Client sessions	5
Workflow module	enabled
Active Directory module	enabled
Redaction module	enabled
FastFind module	enabled
Print-to-FileHold	disabled
Multi Document Repository	enabled
Allow server plug-ins	enabled
Allow FDA plug-ins	enabled
Allow rebranding of the Web Client	enabled
Allow rebranding of the FDA	enabled
License issued	10/5/2011, 4:09 PM
License time limit	unlimited

Document Viewer Licenses

Number of Enterprise Office Viewer named licenses	5 (for viewing of MS Office, PDF and Image file formats only)
Number of Enterprise Office Viewer With CAD Support named licenses	5 (for viewing of MS Office, PDF, Image file and AutoCAD formats)
Number of Enterprise Office Viewer (Engineering Edition) named licenses	5 (for viewing of MS Office, PDF, Image file and All CAD formats)
Number of PDF/Image Viewer named licenses	5 (for viewing of PDF and Image file formats)

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

TO ADD A LICENSE KEY

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

9. ACTIVITY LOG

The Activity log displays the user name, which client they logged into (FDA or Web Client), and the time and date they logged in and out of the system.

For more detailed reporting, FileHold uses Microsoft SQL 2005 Reporting Services integration. See the *Library Administration Guide* for more information.

TO VIEW THE ACTIVITY LOG

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

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

10. SYSTEM AUDIT LOG

The System Audit Log logs activities performed by a System Administrator. It is accessible in the System Administration area in the Web Client.

The following information is recorded in the log:

- Adding local and domain users

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

To ACCESS THE SYSTEM AUDIT LOG:

1. Log into the **Web Client > System Admin** and go to **Logs and Reports > Audit Log**.
2. To filter by username and/or date range, enter the information into the filter fields and click **Apply Filter**.

INDEX

- A**
- Active Directory, 3, 10, 11, 26
 - activity log, 32
 - audit log. *See* system audit log
- C**
- Cabinet Administration, 14
 - CALs. *See* licenses
 - concurrent users, 8
- D**
- default domain
 - setting, 25
 - document control fields
 - enabling, 27
 - Document Publisher, 13
 - Document Publisher + Delete, 13
 - document shortcuts, 27
 - domain groups, 10
 - domain users, 4, 7, 10
 - adding, 11
- E**
- email
 - outbound mail settings, 26
 - event schedule, 28
 - archive, 28
 - convert to record, 28
 - delete, 28
 - enabling, 29
- F**
- FDA, 5
 - FileHold Domain Groups, 10
 - FileHold Domain Users, 10
 - FileHold groups. *See* groups
- G**
- global settings, 25
 - groups, 12
 - adding users, 14
 - creating, 12
 - deleting, 20
 - permissions diagram, 15
 - user roles, 12
 - viewing properties, 18
 - guaranteed users, 8, 20
 - Guest User, 13
 - guest user licenses, 8
- I**
- insufficient CALs, 29
 - log, 29
 - notification settings, 29
- L**
- Library Administration, 14
 - Library Administrator, 3, 15
 - licenses
 - adding additional licenses, 31
 - removing from disabled domain users, 26
 - viewers, 22
 - locally managed users, 4, 7, 8
 - creating, 9
 - log in, 5
 - logon security, 23
- M**
- Microsoft Active Directory Toolkit, 10
 - Microsoft SharePoint, 8
 - Microsoft SQL 2005 Reporting Services, 32
- O**
- Organizer, 13
 - Organizer + Delete, 14
- P**
- password security, 23
 - passwords
 - resetting, 21
 - permission settings, 28
 - Publisher, 13
 - Publisher + Delete, 13
- R**
- Read Only, 13
 - repository locations, 30
 - add repository, 30
 - reset passwords, 21
 - responsibilities, 3
- S**
- security, 4
 - problems, 5
 - self-registered users, 24
 - setting up, 25
 - Senior Library Administration, 14
 - shortcuts, 27
 - skills required, 3

synchronizing
 domain users, 10
System Administration, 14
System Administrator
 responsibilities, 3
 skills required, 3
system audit log, 32

T

time-out settings, 23

U

user roles, 12
user self-registration, 7
users
 adding to groups, 14
 deleting, 19

 disabling accounts, 22
 enabling accounts, 22
 reset password, 21
 searching for, 18
 viewing properties, 17
users and groups
 flowchart, 8
 managing access, 7
 overview, 6
 setting up, 6

V

version control fields
 enabling, 27
viewer licenses, 8
viewers
 licenses, 22