User Manual

A PRACTICAL GUIDE

Preface

FileAgo in a Nutshell
FileAgo is a secure file storage, file management, file sharing and collaboration platform.

FileAgo can be used in the cloud (FileAgo SaaS), or it can be installed on your server (FileAgo Self-hosted).

Contents

0.1 The Basics

0.1.1 Cloud Users

In order to access and store files in FileAgo, you'll need a User account.

There are 2 types of User accounts in FileAgo:

1. Normal User
2. Admin User

Normal User
A normal User can log into their Workspace with an email address as their username and use FileAgo as per the restrictions set by the the administrator. If they are a member of any groups, the User can access the group's Workspace and collaborate with other group members.

Admin User
The first User, the person who created an account with FileAgo is, by default, the administrator. This User can create and manage other Users and groups.

The admin user will not be listed anywhere, they will not appear in the User list.

The global administrator account does not have disk space of their own. This means that that admin user cannot upload files or be member of any groups.

The only purpose of admin user account is to make changes to the FileAgo configuration when required.

However, it's possible to grant administrator privileges to a normal User and that User can perform all admin tasks.

0.1.2 Self Hosted Users

In order to access and store files in FileAgo, you'll need a User account.

There are 2 types of User accounts in FileAgo:

1. Normal User
2. Admin User

Admin User
At the time of installation, the admin User is created automatically by the system. This is the global administrator account and can be used to create Users, groups, assign disk space and so on.

he admin user will not be listed anywhere, they will not appear in the User list.

The global administrator account does not have disk space of their own. This means that that admin user cannot upload files or be member of any groups.

The only purpose of admin user account is to make changes to the FileAgo configuration when required.

However, it's possible to grant Administrator privileges to a normal User and that User can perform all admin tasks.

See Appendix Three for a full list of the differences between Cloud use and Self Hosted.

0.1.3 Groups

Multiple Users who need to collaborate and share files can be placed into the same group.
A user can be a member of multiple groups.

privilege and are managed by Group Admins.

Group admins are normal Users who have privilege to manage a group and its members.

A user can see all of their group memberships in the Groups Menu. By clicking on any group, a member can access the group's Workspace and all of its files.

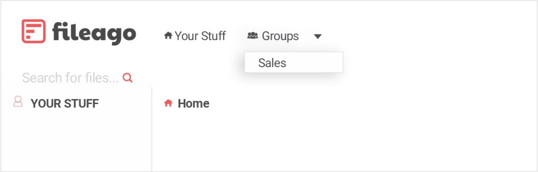


Figure 1:

All files uploaded into a group's workspace are owned by that group, not by the User who uploaded it.

0.1.4 Workspace

A User's home page is called the Workspace. This is where the User uploads files.

Your Workspace comes with several default folders. These folders have specific purposes and can be accessed through the left sidebar. They cannot be removed or renamed.

Home default folders are as follows:

Home Folder
This is where all files and folders are created and stored for a specific User. The Home Folder can only be accessed by its owner.

Incoming
This folder contains all files that were shared with you or to a group by other Users.[1] These files are owned by the User and take up allotted disk space.

Favorites For quick access to a file or folder, a User can mark it as a Favorite by clicking on the star.

Shared
This folder contains the list of files and folders which were shared with you or, in the case of a group Workspace, the groups.

Private Shares
This folder contains the list of files and folders which were shared with you or, in the case of a group Workspace, the group privately.

Public Shares
You can share files and folders with external Users by creating a Public Share.

Trash
When a file or folder is deleted, it's moved to the Trash Folder. You can restore items to the Home Folder within 30 days of deletion. Trash does not take up any space from the allotted disk quota for that user or group.

[1] Newly incoming shares are pending. Users have up to 7 days to accept files. Pending files do not take up any disk space quota. See disk space quota for details on allotted disk space.

0.1.5 Sharing User Owned Data

FileAgo implements a flexible permission model, with the core concept that permissions applied to a folder apply to all child resources inside that folder unless overridden.

Permissions applied to a folder or file are listed under the Permissions section in the right sidebar.

0.1.6 Sharing Group Owned Data

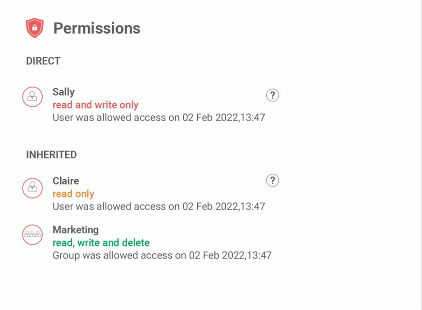
FileAgo implements a flexible permission model, with the core concept that permissions applied to a folder applies to all the child resources inside that folder unless overridden. [2]

For group owned files, the group admin can change permissions in the Security section of the Settings page in the Admin Panel. It's listed under only group permissions matter.

Only group permissions matter is a safer model to work with. Disabling it will force FileAgo to implement a stricter permission model, which may or may not be desirable for an organization. Disabling this function will force FileAgo to implement a stricter permission model which may or may not be desirable for an organization. [3]

When Enabled
If a User is part of multiple groups (Group A and B) and Group A shares a resource with Group B Group, permissions is assigned by group A's Admin.

When Disabled
If a User is part of multiple groups (Group A and B), group A Shares a resource with Group B, permissions is assigned by Group Admin B's admin.



Permissions

DIRECT

Sally
read and write only
User was allowed access on 02 Feb 2022,13:47

INHERITED

Claire
read only
User was allowed access on 02 Feb 2022,13:47

Marketing
read, write and delete
Group was allowed access on 02 Feb 2022,13:47

Figure 2: The Permissions section of John's Acme Inc folder might look like this.

See Appendix One for examples.

In Workspace
The permissions applied to a folder or file are listed under the Permissions section in the right sidebar.

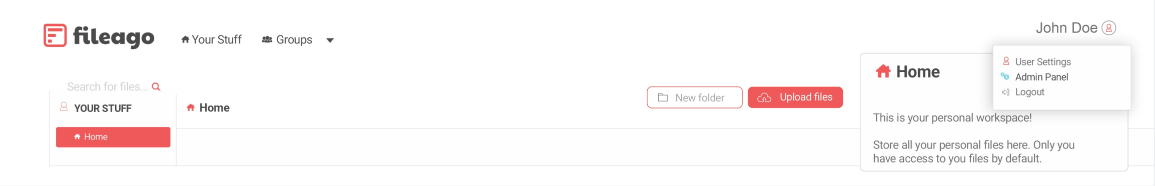
See Appendix One for examples.

[2] Only group permissions matter for group members is enabled by default.
[3] If you are a FileAgo Cloud customer who wants to disable this option, please contact Support.

0.2 Admin

0.2.1 Getting Your Toes Wet

The admin User, or any user who has Administrator privilege can access the Admin panel to managing Users and groups or configuring FileAgo.



This is your personal workspace!

Store all your personal files here. Only you have access to you files by default.

The admin User does not have any disk space of their own, and so they cannot be part of a group or upload any files. When an admin User logs into the Web Portal, the user is automatically redirected to the Admin panel.

If a normal user has administrator privileges, they can access the Admin panel by choosing the option Admin Panel from the top right dropdown menu.

Once inside the Admin Panel, you will see that it's divided into several sections:

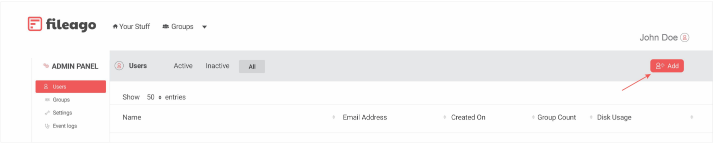
1. Users - for user management
2. Groups - for group management
3. Event Logs - to view log of all past events
4. About FileAgo - to know more information about FileAgo

The following sections are available in a FileAgo Self-hosted server:

1. Devices - for device management
2. Chat Server - for configuring the chat service
3. Settings - for configuring FileAgo
4. LDAP Settings - for integrating FileAgo with AD/LDAP server
5. SSO/SAML - for configuring FileAgo to work with SAML-based

0.2.2 Creating Users

Create New User From the Users section, click on the Add button. The add button is located in the top right corner.



Follow the prompts in the form and create a new User:

1. **Fullname**
   Enter the full name of the new User.

2. **Email Address**
   Enter the email address of the new User. This will also be their login ID.

3. **Password**
   Enter the desired password. A minimum of 8 characters is required. The password should be a combination of alpha-numeric and special characters with at least one in caps.

4. **Confirm Password**
   Enter the password again for confirmation.

5. **Enable Personal Space**
   In most cases, you should keep this option enabled so that you can set a disk quota [4]

6. **Disk quota**
   Enter 0 to allow unlimited storage space, or put in a numeric value and choose the appropriate unit (MB/GB) from the dropdown menu.

[4] Disabling this option ignores your disk quota selection and creates a User without the functionality to upload or receive documents. The User can, however, participate in groups and access private shares assigned to them.

0.2.3 Adding Users to Groups

From the Users section, click on the Add button.
The add button is located in the top right corner. Click on Add user button at the bottom to create the user.

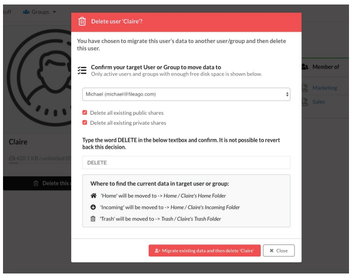
0.2.4 Removing Users from Groups

Deleting a User is irreversible and could result in loss of data. Please proceed with caution.

A User can be deleted the via Admin Panel through -> Users -> Name -> Delete this User.

FileAgo will ask if you'd like to delete the User and their data, or to move the existing data to some other User before proceeding with the delete request.

If you proceed with Delete this User along with their data, in the following confirm dialog type Delete to finalize the action.



Delete user 'Claire'?

You have chosen to migrate this user's data to another user/group and then delete this user.

Confirm your target User or Group to move data to
Only active users and groups with enough free disk space is shown below.

Michael (michael@fileago.com)

☑ Delete all existing public shares
☑ Delete all existing private shares

Type the word DELETE in the below textbox and confirm. It is not possible to revert back this decision.

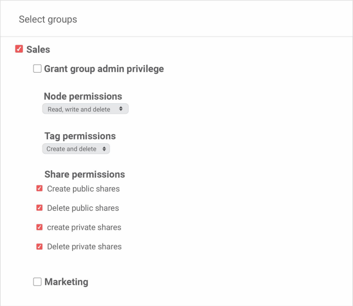
DELETE

Where to find the current data in target user or group:
'Home' will be moved to -> *Home / Claire's Home Folder*
'Incoming' will be moved to -> *Home / Claire's Incoming Folder*
'Trash' will be moved to -> *Trash / Claire's Trash Folder*

Selecting Delete this User only allows you to migrate their existing data into the Workspace of any other User or group. The target User or group should have enough disk quota available in order to move the data or the process will fail.

In the screenshot, the existing data of user named Claire will be moved into Michael's workspace first before it is removed.

0.2.5 Group Permissions



Select groups

☑ Sales

□ Grant group admin privilege

Node permissions: Read, write and delete

Tag permissions: Create and delete

Share permissions

☑ Create public shares

☑ Delete public shares

☑ create private shares

☑ Delete private shares

□ Marketing

Grant Group Admin Privilege
Selecting Yes creates a User with administrator privileges, For creating a normal user, select No.

If selected, this User will have group admin privileges for the group. With group admin privilege, the User can add/remove group members.

If there are existing groups, they will be displayed on the right side of the form. [5]

Node Permissions

This option sets the permissions for the User when accessing this group's files and folders. The permission schema is as follows:

1. **Read Only**
   The User can view the group's content.
2. **Read and Write**
   The User can view, create or update files and folders in the group's workspace.
3. **Read, Write and Delete**
   The new User can view, create/update and delete files. See Trash.

Tag Permissions
permission schema is as follows:

1. **Create Only** The User can create tags in the group and assign them to resources.
2. **Create and Delete** The User can create tags, edit or remove existing tags (even those created by other group members).

Share permissions
These settings determine whether the User can share group content or not.

1. **Create Public Shares**
   The User can share files/-folders.
2. **Delete Public Shares**
   The User can delete existing public shares.
3. **Create Private Shares**
   The User can delete private shares.
4. **Delete Private Shares**
   The User can delete existing private shares created by other group members. [6]

[5] It is possible to have multiple group admins in a group.

[6] belonging to group with a public user (a public share can be accessible by anyone who knows the share URL, and does not require any authentication).

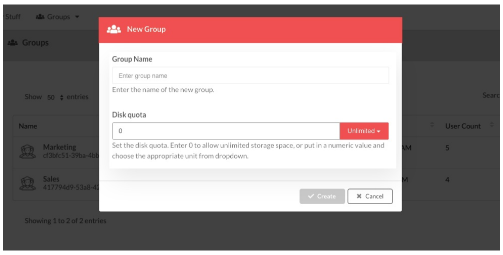
0.2.6 Creating a New Group

From the Groups section, click on the Add button at the top right corner to bring up the add group form popup.

Use the below information to fill in the form and create a new group;

1. **Group Name**
   Enter the name of the new group.

2. **Disk Quota**
   Set the disk quota of the group here. Enter 0 to allow unlimited storage space or enter a numeric value and choose the appropriate unit (MB/GB) from the dropdown menu.



New Group

Group Name

Enter group name

Enter the name of the new group.

Disk quota

0 Unlimited ▾

Set the disk quota. Enter 0 to allow unlimited storage space, or put in a numeric value and choose the appropriate unit from dropdown.

Click on Create to complete the process.

Note: Assign at least one User as the group admin (this is not a strict requirement, but it helps in delegating responsibility of managing a group).

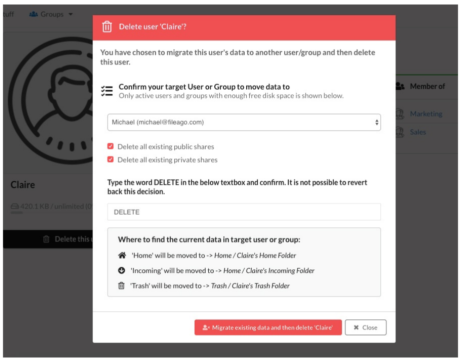
0.2.7 Delete a Group or Remove a User

An existing group can be deleted via Admin Panel To do so, got to-> Groups -> Name -> Delete this group.

FileAgo will ask you to confirm whether to delete the group and also its entire data or to move the existing data to some other group before proceeding with the delete request.

If you proceed with Delete this group along with its data, in the following confirm dialog type DELETE to finalize the action.

Selecting Delete this User only, allows you to migrate the existing data into the Workspace of any other User or group. The target user or group should have enough disk quota available in order to move the data or the process will fail.



Delete user 'Claire'?

You have chosen to migrate this user's data to another user/group and then delete this user.

Confirm your target User or Group to move data to
Only active users and groups with enough free disk space is shown below.

Michael (michael@fileago.com)

☑ Delete all existing public shares
☑ Delete all existing private shares

Type the word DELETE in the below textbox and confirm. It is not possible to revert back this decision.

DELETE

Where to find the current data in target user or group:

'Home' will be moved to -> *Home / Claire's Home Folder*
'Incoming' will be moved to -> *Home / Claire's Incoming Folder*
'Trash' will be moved to -> *Trash / Claire's Trash Folder*

Note: Deleting a group is irreversible and can result in loss of data. Please proceed with caution.

0.3 Configuration

0.3.1 Setting Up

Administrator can configure FileAgo by accessing Admin Panel -> Settings.

Hostname
Enter the hostname (FQDN) of your installation.

Among other things, this value is used to make URLs. If a hostname is not available, you can use an IP address instead.

Outgoing webhook
This setting is only required if you have an external service which needs to receive information when events happen in FileAgo. If not, simply leave the Endpoint URL field blank.

Endpoint URL
FileAgo will post all events related to files and folders as JSON data to the URL that you enter here.

It is highly recommended to use https protocol (with a valid certificate) and to refer the endpoint by its hostname. [7]

Document Revisions
Using this option, an administrator can configure how many days old versions of files are available, after which the original data file will be safely removed. It is possible to preserve all revisions (i.e., FileAgo will never remove any old revisions) by selecting the option Keep forever from the dropdown.

0.3.2 Email and SMTP Setup

Email Server
This section is used to configure the SMTP server which will be used by FileAgo to send email notifications to Users.

SMTP Server
Enter the hostname (FQDN) or IP address of the SMTP server to use.

SMTP Username
Enter the username to authenticate with the SMTP server.

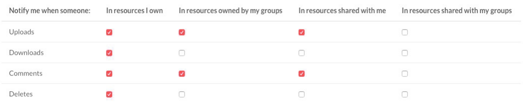
SMTP Port
Enter the port at which SMTP your server is listening. Usually, it’s 25 or 587, but can vary.

[7] If you are a FileAgo Cloud customer who wants to configure an outgoing webhook url, please contact Support.

0.3.3 Email Notification Setup

Send email notifications as (FROM:)
Email notifications will have this email address as its source (FROM: address).

Enable email notifications
This option needs to enabled (along with a working SMTP server configuration) in order for FileAgo to send outgoing email notifications.



Notify me when someone:	In resources I own	In resources owned by my groups	In resources shared with me	In resources shared with my groups
Uploads	☑	☑	☑	□
Downloads	☑	□	□	□
Comments	☑	☑	☑	□
Deletes	☑	□	□	□

Configure Notifications
The first row can be interpreted as alert User by email if files are uploaded which satisfy any of the below conditions:

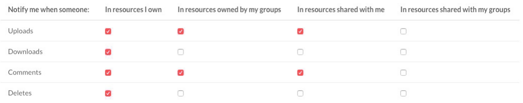
The file is uploaded to a folder owned by the User.

The file is uploaded to a folder owned by one of the groups in which this User is a member.

The file is uploaded to a folder shared with the User.

0.3.4 Realtime Notifications

This option needs to enabled in order for FileAgo to display realtime notifications (a small popup that notifies the user of any event on the web UI).



Notify me when someone:	In resources I own	In resources owned by my groups	In resources shared with me	In resources shared with my groups
Uploads	☑	☑	☑	□
Downloads	☑	□	□	□
Comments	☑	☑	☑	□
Deletes	☑	□	□	□

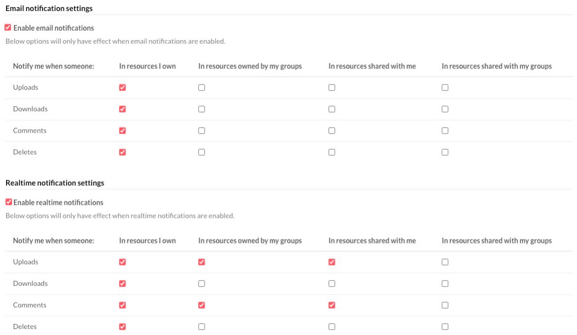
Configure Realtime Notifications
The first row can be interpreted as notify a User by realtime notification if satisfy any of the below conditions:

The file is uploaded to a folder owned by the User.

The file is uploaded to a folder owned by one of the groups in which this User is a member.

The file is uploaded in a folder shared with the User.

Default notification settings in FileAgo Cloud
The notification settings configured in FileAgo Cloud servers are shown below. If required, users can override these settings in User Settings -> Notifications.



Email notification settings

☑ Enable email notifications

Below options will only have effect when email notifications are enabled.

Notify me when someone:	In resources I own	In resources owned by my groups	In resources shared with me	In resources shared with my groups
Uploads	☑	□	□	□
Downloads	☑	□	□	□
Comments	☑	□	□	□
Deletes	☑	□	□	□

Realtime notification settings

☑ Enable realtime notifications

Below options will only have effect when realtime notifications are enabled.

Notify me when someone:	In resources I own	In resources owned by my groups	In resources shared with me	In resources shared with my groups
Uploads	☑	☑	☑	□
Downloads	☑	□	□	□
Comments	☑	☑	☑	□
Deletes	☑	□	□	□

Figure 3: Options for realtime notifications.

0.3.5 Security

Administrator can configure FileAgo by accessing Admin Panel -> Settings.

CORS Access-Control-Allow-Origin Header
Enter * or hostname if you have 3rd party applications or mobile applications that needs to connect to FileAgo using an API. If not, leave the field empty.

Only group permissions matter when group members try to access files owned by a group
This option is enabled by default. Disabling this will result in stricter permission checks for a User when trying to access resources owned by a group. [8]

Temporary ban for failed login attempts
Enable to temporarily ban IP to prevent password guessing. Additional settings are as follows:

1. **Max failed logins**
   Enter the number of failed logins that will trigger a ban (default: 5).
2. **Interval (in minutes)**
   Enter the interval of time during which maximum failed logins should occur from an IP to trigger a ban (default: 1).
3. **Ban duration (in minutes)** Enter the period for which a temporary ban must last (max: 120 minutes, default: 15). [9]

[8] If you are a FileAgo Cloud customer and wants to disable this option, please contact Support

[9] In a FileAgo Cloud server, the temporary ban is always set enabled with the default settings.

0.3.6 LDAP/AD

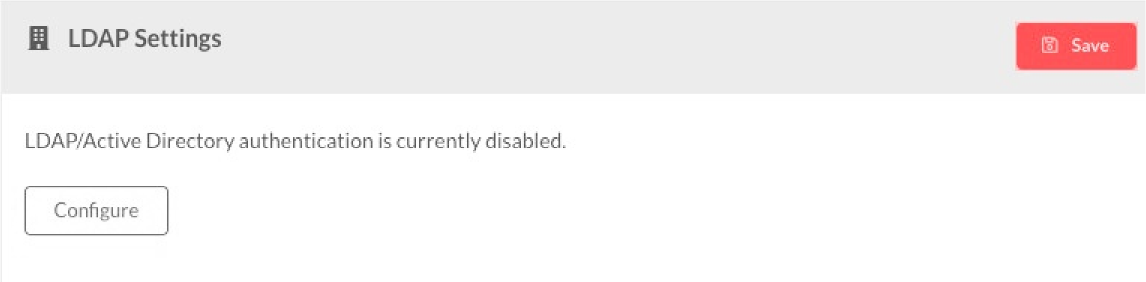
Administrator can integrate FileAgo with an LDAP/AD server via Admin Panel through -> LDAP Settings, after which FileAgo will:

Fetch Users and groups from LDAP/AD and create them in FileAgo.

Sync changes or fetch new Users/groups from LDAP/AD every 5 minutes.

Confirm username/password credentials with LDAP/AD before allowing access.

Configuration
Click on Configure to input LDAP/AD settings. [10]


LDAP Settings

LDAP/Active Directory authentication is currently disabled.

1. **LDAP Server Host**
   Enter the hostname (FQDN) of your LDAP/AD server.

2. **Port**
   Enter the port number. The default LDAP port is 389.

3. **User DN**
   The Distinguished Name (DN) of a user who has permissions to perform searches in the LDAP directory e.g. uid=systemuser,cn=sysusers,dc=mycompany,dc=com).

[10] Active Directory and LDAP are usually on-premise services, and for this reason, this feature is not supported in FileAgo Cloud.

4. **Keep LDAP passwords**
   If this option is enabled, the User's last known working LDAP password is stored and the password given during authentication is matched with it if the LDAP server is not accessible or is down at that time. When an LDAP server is available, User authentication of FileAgo is performed by the LDAP server. This setting only has effect when the LDAP server is unreachable.

User Accounts
Contact your LDAP/AD Administrator for assistance.

Base User Tree
The base DN of LDAP from where all Users can be reached (eg. cn=users,dc=mycompany,dc=com).

Groups
Contact your LDAP/AD Administrator for assistance.

Group Permissions Configures the permissions a User will have when they are added to a group during LDAP sync.

Sync Groups from LDAP Select Yes if you wish to sync groups from the LDAP server.

0.3.7 LDAP Filter User

Filter User By
You can either use a valid object class (eg. inetOrgPerson) or any custom filter like:

```
(&(objectClass=inetOrgPerson(memberOf=cn=fileagousers ,ou=groups ,
dc=my−company , dc=com ) )
```

The above custom filter will only fetch those users who are member of cn=fileagousers,ou=groups,dc=my-company,dc=com group.

Username Attribute (case sensitive)
The attribute which uniquely identifies a user in LDAP (eg. uid or sAMAccountName).

Display Name Attribute (case sensitive)
The attribute which stores the name of the User in LDAP (eg. sn, or displayName).

Email Attribute (case sensitive) This stores the email of the User in LDAP eg. mail, or mailPrimaryAddress.

Default User Disk Quota (in bytes)
During the creation of a User, set to 0 for unlimited disk quota.

Exclude Users list
Enter the DN of those Users who should not be added into FileAgo in each line eg.uid=john,cn=users,dc=my-company,dc=com/uid=james,cn=users,dc=my-company,dc=com).

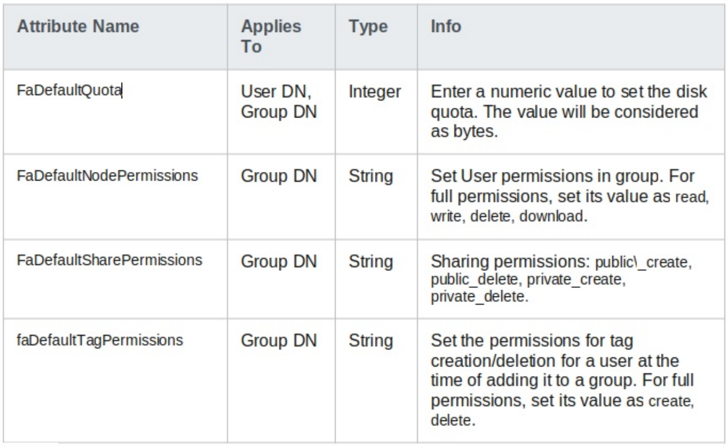
Note: The above custom filter will only fetch those groups which are under cn=groups,dc=my-company,dc=com path.

0.3.8 LDAP Custom Attributes

LDAP Custom Attributes
It is possible to create custom attributes in LDAP that override certain default values which are configured in the previous section.

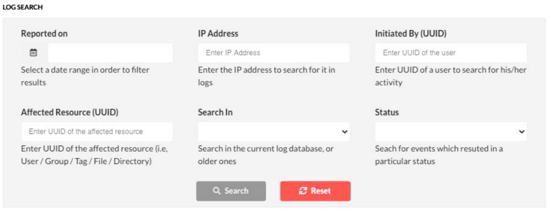
For example, the default disk quota for a user or group can be overridden by setting an integer value for the faDefaultQuota attribute in the DN.

The complete list is given above.



Attribute Name	Applies To	Type	Info
FaDefaultQuota	User DN, Group DN	Integer	Enter a numeric value to set the disk quota. The value will be considered as bytes.
FaDefaultNodePermissions	Group DN	String	Set User permissions in group. For full permissions, set its value as read, write, delete, download.
FaDefaultSharePermissions	Group DN	String	Sharing permissions: public_create, public_delete, private_create, private_delete.
faDefaultTagPermissions	Group DN	String	Set the permissions for tag creation/deletion for a user at the time of adding it to a group. For full permissions, set its value as create, delete.

If these attributes exist in LDAP with invalid values, then the default values (configured above) will be used instead.



LOG SEARCH

Reported on

Select a date range in order to filter results

IP Address

Enter the IP address to search for it in logs

Initiated By (UUID)

Enter UUID of a user to search for his/her activity

Affected Resource (UUID)

Enter UUID of the affected resource (i.e, User / Group / Tag / File / Directory)

Search In

Search in the current log database, or older ones

Status

Seach for events which resuted in a particular status

Figure 4: Event Logs help organizations track everything and maintain complete vigilance over their corporate data. All activities like User/group creation, file uploads, configuration changes and etc are tracked and reported here

0.3.9 Event Logs

An administrator can see event logs through the Admin Panel. To do so, go to Admin -> Event Logs.

Searching Logged Data

Date Range
Pick a From and To date from the Reported on field and click on Search in order to see all activities that happened in between that time period.

Search Activities For an IP Address
Enter the IP address in the IP Address field and hit Search in order to see all activities which were initiated from that IP address.

Search for Activities by a User
In order to find all activities performed by a particular User, enter the User's UUID into the field Initiated by (UUID) and hit Search.

A user's UUID can be located in this way:

Browse to Admin Panel -> Users

Click on the name of the desired User

The UUID will be dislpayed

under User Info section

Search for all activities which happened on a file/folder Type in the UUID of the target resource in the Affected Resource (UUID) field and click on Search to get a list of all activities related to it. In order to find the UUID of a file/folder, follow the mentioned steps: [11]

Browse to the file or folder

Click on Actions -> Properties

The UUID will be displayed in the popup dialog.

Searching Old Logs

FileAgo rotates the log database periodically, but will still preserve the old databases for search and retrieval when required. In order to search for something in your old logs, simply select a log from Search in the dropdown and click on Search.

Search for particular status Select the status from the Status dropdown list and hit Search in order to search and retrieve logs that matches the status. For e.g., you can use this option to display all logs with status Error or Success.

[11] FileAgo creates Version 4 UUID (eg.251c908d-ded5-4a4f-8505-99f638a84b44) to represent Users, groups, tags, files and folders internally in its database.

0.4 Appendices

0.4.1 Appendix One

As shown in the image, Sales consists of 4 members: John, Sally, Claire and Michael. Permissions for those Users are shown in the image.

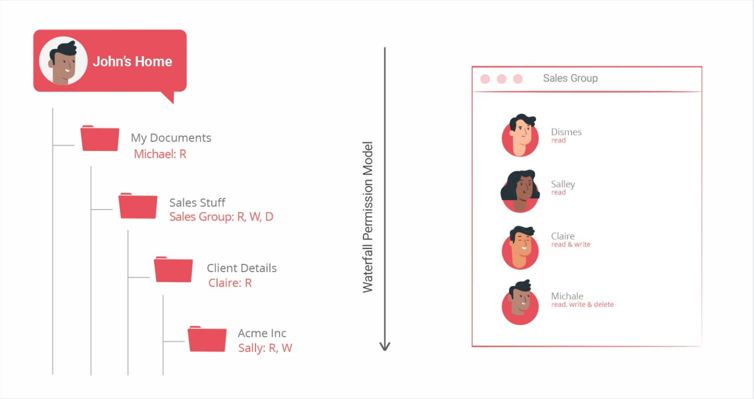


Figure 5:

John has full access. He can read, write and delete file in all folders. John is the owner of the folders.

The folder My Documents is shared with Michael with read permission. Claire and Sally are not be able to access the My Documents folder.

John has shared the Sales Stuff folder with Sales group with read, write and delete permissions. However, Sally is a member of Sales group with read permissions only. Therefore, Sally has only read permissions in this folder.

Likewise, Claire has read and write permissions in the group and these are the permissions Claire receives in the Sales Stuff folder.

In the case of Michael, he has full permissions in the group and therefore has full permissions in this folder as well.

Coming to the Client Details folder, Sally has read permission, but John has overridden Claire's permissions in this folder and set it to read only. Michael's permissions on the parent folder apply here too.

And finally, John has overridden permissions for Sally in Acme Inc folder and granted her read and write access. Permissions for Claire and Michael in Acme Inc are the same as its parent folder.

0.4.2 Appendix Two

Although the folder names and structure are same as in the first example, in this case they are owned by the Sales Group, and not by a User. We also have another group called the Marketing Group with the same set of Users, but different permissions.

By default, The Users Sally, Claire and Michael have access to the Sale's group Home folder. However, their permissions vary according to that which they were granted by the User admin or group admin.

Only group permissions matter for group members = enabled

In the case of My Documents folder, group permissions applies for the Users Sally (read) and Claire (read, write). Group permissions for Michael is overridden and he only has read permissions in this folder. Since John is not a member of the Sales group, he has no access.

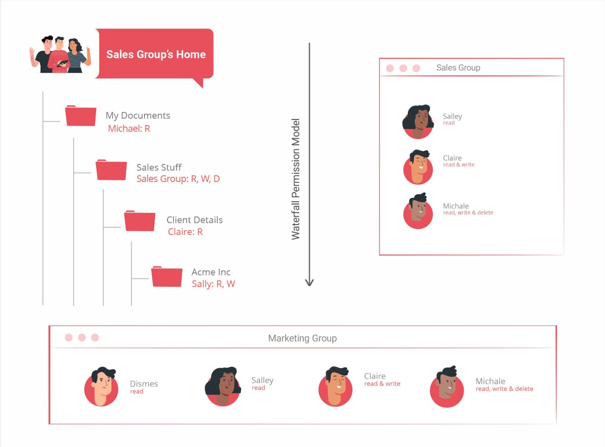


Figure 6:

For the Sales Stuff folder, the Marketing Group has been allowed full access. However, since only the current group permissions matter for group members, Sally, Claire and Michael will still be granted access as per its parent folder.

In the case of John, he is not a member of the Sales group, so his permissions are based on the permissions that were assigned to him in the Marketing Group (which is read, write).

Claire has read permissions in Client the Details folder. The rest of the users have the same permissions as in the parent folder.

Similarly, Sally has given read/write permissions in the Acme In folder. The rest of the users continue to have the same permissions as they do in the folder above it.

Only group permissions matter for group members = disabled
In this case, when determining the permissions of Sally, Claire and Michael, their permissions in Marketing Group will also be taken into account beginning with the Sales Group folder.

Starting with My Documents folder, the group permissions applies for users Sally (read) and Claire (read, write). Group permissions for Michael is overridden and he only has read permissions in this folder. Since John is not a member of the Sales group, he has no access.

For Sales Stuff folder, we see that Marketing Group has been allowed full access to it, and that determines the permissions for Sally, Claire and Michael as well along with John who is a member of Marketing Group.

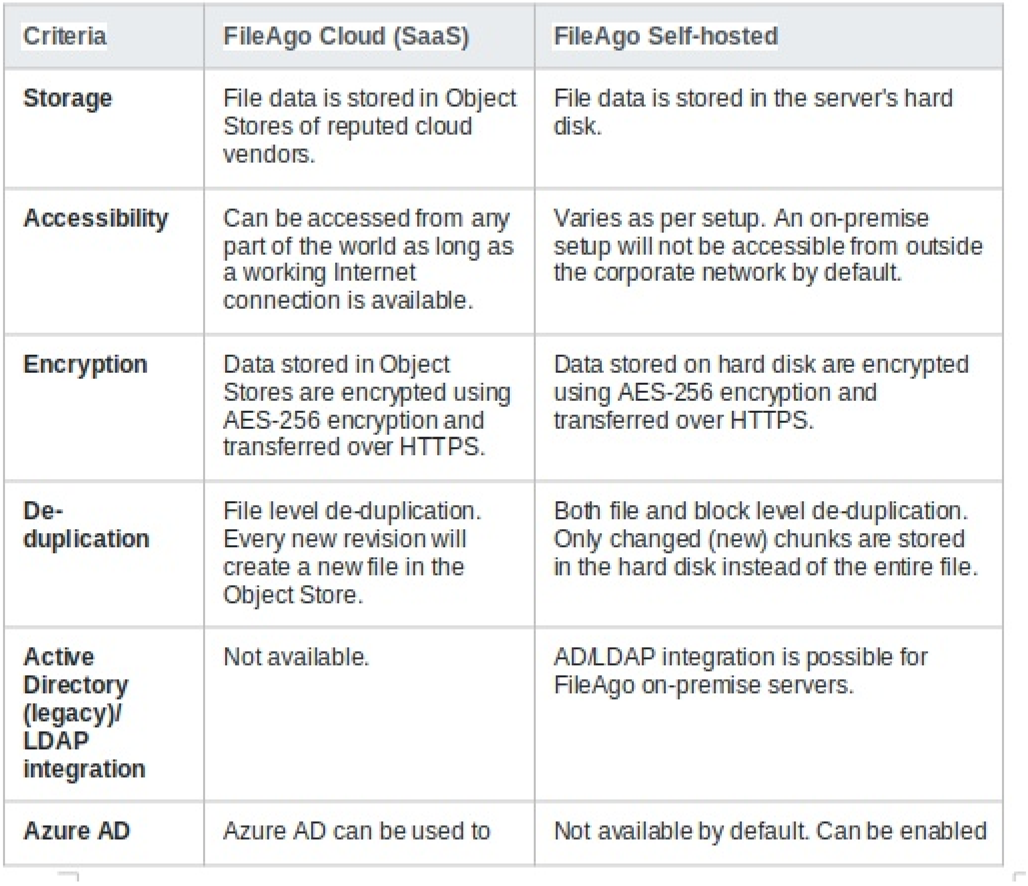
Sally and Claire has full permissions in Marketing Group, so they receive full access in Sales Stuff folder as well. Permissions of Michael and John are read, write in Marketing group, so that is the permissions they will have in this folder.

Claire has been assigned read permissions in Client Details folder, so that is the permission she will have to be content with. Sally, Michael and John will have the same permissions that they had in the folder just above this one. In Acme Inc folder, Sally has been assigned read, write permissions, and that is the permission she will be having. Claire, Michael and John will be the same permissions that they had in the parent folder (Client Details).

0.4.3 Appendix Three

In FileAgo Cloud, your data resides on the cloud. We manage the infrastructure to ensure that the service is up and running at all times. In FileAgo Self-hosted, you install FileAgo on your own server.

Belos is a complete list of the differences and similarities between the services.



Criteria	FileAgo Cloud (SaaS)	FileAgo Self-hosted
Storage	File data is stored in Object Stores of reputed cloud vendors.	File data is stored in the server's hard disk.
Accessibility	Can be accessed from any part of the world as long as a working Internet connection is available.	Varies as per setup. An on-premise setup will not be accessible from outside the corporate network by default.
Encryption	Data stored in Object Stores are encrypted using AES-256 encryption and transferred over HTTPS.	Data stored on hard disk are encrypted using AES-256 encryption and transferred over HTTPS.
De-duplication	File level de-duplication. Every new revision will create a new file in the Object Store.	Both file and block level de-duplication. Only changed (new) chunks are stored in the hard disk instead of the entire file.
Active Directory (legacy)/ LDAP integration	Not available.	AD/LDAP integration is possible for FileAgo on-premise servers.
Azure AD	Azure AD can be used to	Not available by default. Can be enabled