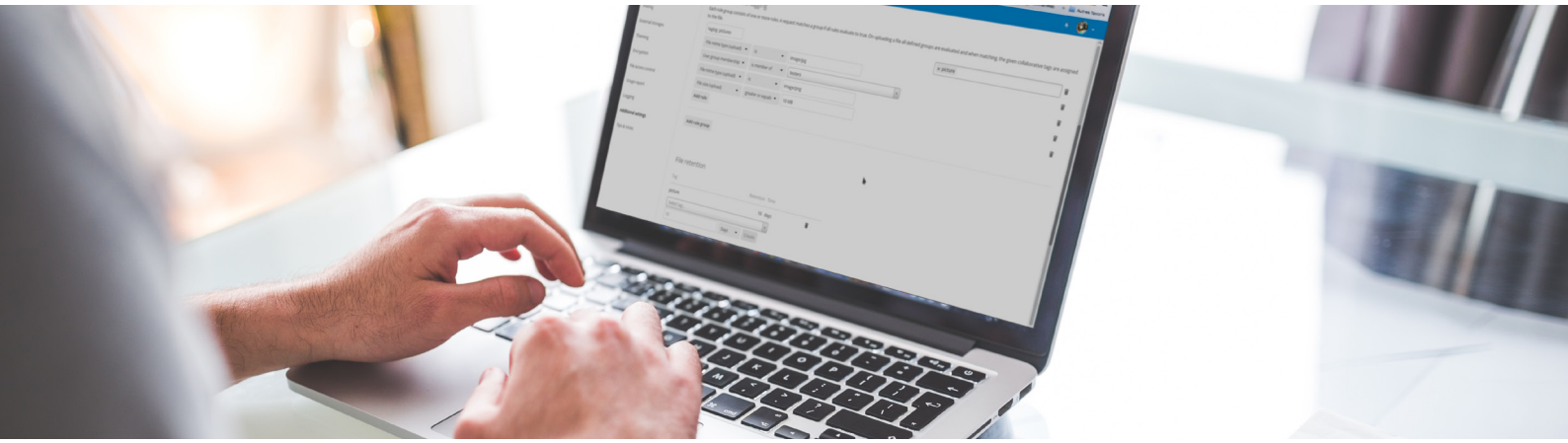
File Access Control and Retention

Align file access with enterprise policy



Controlling who has access to data and when is a core function of the IT Department security efforts. Traditionally this is done through a shared data directory with restrictive file access rights defining a complicated set of groups and access rights associated with them. In nearly all organizations this model has been informally 'augmented' with attachments sent around by email and, frequently, illicit use of public cloud solutions, evading security, privacy and retention policies. This brings significant legal, practical and financial risks, often impossible to solve with the usual encryption and firewall technologies.

Besides the workload and risks this causes for the IT team, users are less happy and productive in a restrictive environment. Rather than defining exactly who has access to which folder, codifying business and security policy in more general and business-aligned rules would save time and improve control.

Nextcloud File Access Control provides such a mechanism, removing the burden of manual management of folders and file access allowing rule sets around access and retention to be automatically enforced.

Nextcloud also offers ways to control the retention period of documents, useful for cleaning up data storage or ensuring sensitive data do not linger for too long.

Use cases

- Protect from unauthorized file access
- Enforce company policy and compliance requirements
- Limit and shape bandwidth usage by controlling upload file size at defined time ranges
- Control user capabilities based on group membership, geographical location or more
- Ensure files are preserved as long or short as required by business and legal needs

File Access Control

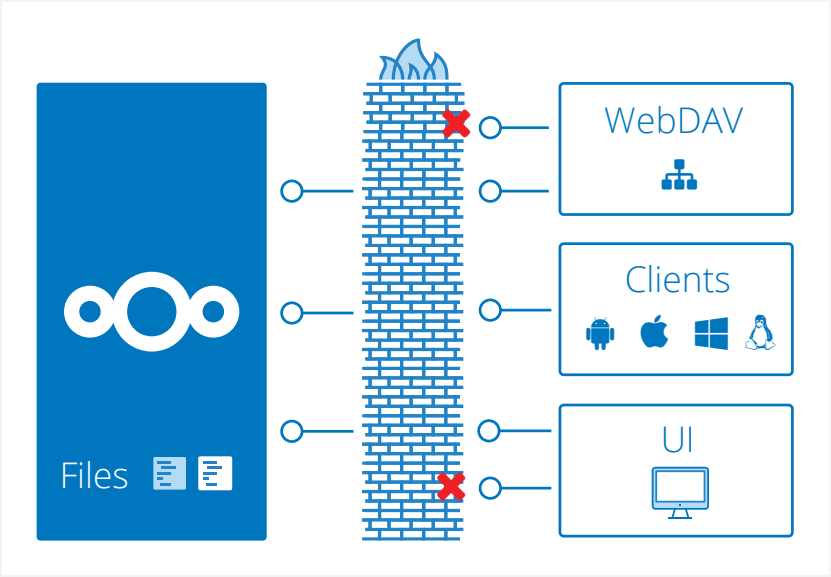
Through File Access Control functionality administrators can define strict rules that file access requests need to adhere to. If users in certain groups or IP ranges should not be given access to certain file types or if data with a specific tag should not be shared outside the company, administrators can make sure their Nextcloud instance enforces these rules.

Administrators can create and manage multiple groups consisting of one or more rules. If all rules of a group hold true, the group matches the request and access is being denied. The rules criteria range from IP address to user groups, collaborative tags, and more.

If access to a file has been denied for a user, the user cannot:

- Create/upload the file
- Modify the file
- Delete the file
- Download the file
- Synchronize the file with clients, such as the Nextcloud desktop and mobile clients

Additionally, it is possible to prevent files from being uploaded to Nextcloud when a set of rules applies.



Rules for File Access Control

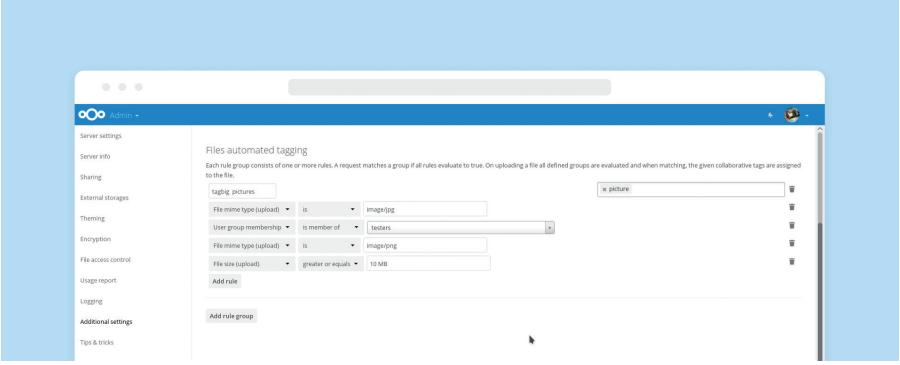
All rules can also be inverted (from 'is' to 'is not') using the operator option.

- File collaborative tag: either the file itself or any of the file owner's parent folders needs to be tagged with the tag
- File MIME type: the MIME type of the file, e.g. text/plain
- File size: the size of the file (Only available on upload)
- Request remote address: an IP range (either v4 or v6) for the accessing user
- Request time: Time span and time zone when the request happens
- Request URL: the URL which requests the file (this is the URL the file is served from, not the URL the user is currently looking at)
- Request user agent: the user agent of the user's browser or client. Nextcloud desktop, Android, and iOS clients are available as preconfigured options
- User group membership: whether the user is a member of the given group

Data Retention

With Data Retention, the longevity of data can be controlled based on manually or automatically assigned tags, ensuring that legal or practical requirements for the longevity of data lifespans can be enforced.

To control data retention, multiple rules can be defined setting specific retention times based on tags. Those tags are manually or automatically assigned. Files will be deleted automatically after the specified time period.



Automated Tagging

Through automatic file tagging, Nextcloud gives administrators a way to flag files upon upload for Retention, File Access Control or automatic execution of scripts based on specified criteria. For example, if DOCX files uploaded by members of the 'Collateral' group need to be automatically converted to PDF, a tag can be assigned based on those rules and the action triggered on files that have the tag set. The execution of actions based on tags has to be implemented through a Nextcloud app, using hooks provided by the Nextcloud API.

To define tags, administrators can create and manage a set of rule groups. Each rule group consists of one or more rules combined through operators. Rules can include criteria like file type, size, time and more. A request matches a group if all rules evaluate to 'true'. On uploading a file, all defined groups are evaluated and when matching, the given collaborative tags are assigned to the file.

Note that tags can also be set manually. Tags come in three varieties:

- Visible – visible and assignable by any user
- Restricted – only specified groups can assign these tags
- Invisible – only admins can see these tags

Automated tags are invisible system tags.

Available rules for Automated Tagging

All rules can also be inverted specifically or using a matching rule using the operator option. Options include 'is', 'is not', 'matches' or 'does not match'.

- File MIME type: the MIME type of the file, e. g. text/plain
- File system tag
- File size: the size of the file
- Request remote address: an IP range (either v4 or v6) for the accessing user
- Request time: time span and time zone when the request happens
- Request URL: the URL which requests the file (this is the URL the file is served from, not the URL the user is currently looking at)
- Request user agent: the user agent of the users' browser or client. Nextcloud desktop, Android and iOS clients are available as preconfigured options
- User group membership: whether the user is a member of the given group

Nextcloud

Conclusion

The combination of Automated Tagging, File Access Control and Retention gives administrators unprecedented, rule-based control over files being handled through their private cloud storage solution. API-based access offers potentially even more control and enables users to automate frequently required actions.

We can provide additional support and consulting when desired. Contact us!

Nextcloud GmbH
Kronenstr. 22A
70173 Stuttgart, Germany

Email hello@nextcloud.com
Phone +49 711 896656-0
Fax +49 711 896656-10

nextcloud.com