# ownCloud File Firewall

## Policy-based protection from unauthorized actions

Network firewalls, SSL and encryption at rest are all part of a traditional security envelope. However, in the age of increasing IT complexity, global collaboration, and the need for syncing and sharing files online, these security approaches are no longer sufficient.

Further, enforcing file-sharing policies can be a huge 'burden on systems administrators. Manual checks and balances are error-prone, and system generated code is often time-consuming to establish and challenging to maintain. What IT administrators need is a mechanism for intelligently deciding which users can access files based on who, what, when and how.

This level of control is available with ownCloud File Firewall. The ownCloud File Firewall removes the heavy burden by allowing complex rule sets to be automatically enforced at the application level based on defined attributes.

## Capabilities

File Firewall prevents execution of ownCloud internal code for requests that violate a set of admin-defined rules. This allows administrators to exclude user behaviors based on many criteria, including geographic location, size of request, app accessed, group memberships and much more.

There are two types of commands applicable to the File Firewall: conditions and operators. Conditions compare request criteria to specific pre-set values. Their results determine whether the firewall allows the pass-through of a request. Operators combine the results of conditions, and allow a rule set to accommodate different types of requests under different circumstances. Both positive & negative behaviors are supported.

Using this flexible framework of conditions and operations administrators can easily:

- Eliminate bandwidth concerns by limiting activities related to very large files to a certain IP range. This limits the amount of data that can be transferred to the server from outside the system, and can prevent unwanted large files from being uploaded over limited bandwidth.
- Control network traffic during peak usage by limiting pre-defined requests to execution within a specific time range, outside peak times.
- Limit user capabilities based on their membership in a specific group or groups.
- Allow critical requests to be processed only when the user is logged into the system to ensure a complete audit trail.
- Restrict requests to process only if the request originates from within the pre-defined server's IP address.
- Allow only those requests that successfully match specific request criteria to be executed.

## Technical specifications

- Requires ownCloud 6 Enterprise Edition or higher.

## About ownCloud Inc.

Based on the popular ownCloud open source file sync and share community project, ownCloud Inc. was founded in 2011 to give corporate IT greater control of their data and files – combining greater flexibility, openness and extensibility. Company headquarters are in Lexington, MA, with European headquarters in Nuremberg, Germany. For more information, visit: https://www.owncloud.com.

## Benefits

- Restrict file sharing from unauthorized devices or locations
- Limit external file access to specific groups, and file uploads to certain characteristics
- Eliminate the risk of access from undesirable geographies
- Guard against unauthorized file sharing

**ownCloud, Inc.**
57 Bedford Street
Suite 102
Lexington, MA 02420
United States

www.owncloud.com/contact
phone: +1 (877) 394-2030

**www.owncloud.com**

@ownCloud
facebook.com/owncloud
gplus.is/owncloud
linkedin.com/company/owncloud