

McAfee CASB integration

Beginning with version 20.2, FileCloud supports integration with McAfee CASB.

This enables you to use McAfee CASB to apply extensive DLP rules when monitoring user events such as actions on files and folders and logins to the system. If a CASB DLP rule is violated, McAfee takes actions such as notifying a user, deleting a file, or removing a share.

For example, you could set up McAfee CASB to monitor the content of files when they are shared in a public FileCloud folder.

On this page:

- [McAfee CASB supported features](#)
- [FileCloud events and McAfee responses](#)

McAfee CASB supported features

User Activity	File Upload, File Update, File Download, File has been Shared publicly, Folder has been shared publicly
	User logged in
DLP Features	Content- aware Public Shared Link, or Pure Public Shared link Policy evaluation for Item Shared event
	Content-ware Policy evaluation for File Upload/Update event
	Response Actions: Incident
	Remove Shared link
	Email notification
	Send user notification
	Delete

FileCloud events and McAfee responses

To receive information about events, McAfee registers a webhook with FileCloud, which enables FileCloud to push information about events as they occur to McAfee CASB.

FileCloud pushes information to McAfee when a user performs one of the following actions:

- adds a file
- updates a file
- adds an external file
- downloads a file
- logs in successfully
- creates a share
- creates an account
- deletes an account

McAfee responds to events that may compromise security using FileCloud's API. FileCloud's API includes the following endpoints:

- register
- deregister
- getwebhook
- downloadfile
- upload
- deletefile
- getshareinformation
- removeuserfromshare
- removegroupfromshare
- deleteshare
- getuserinformation

For more information about using these APIs, see the API documentation at <https://fcapi.getfilecloud.com/>