



FILECLOUD

BY CODELATHE

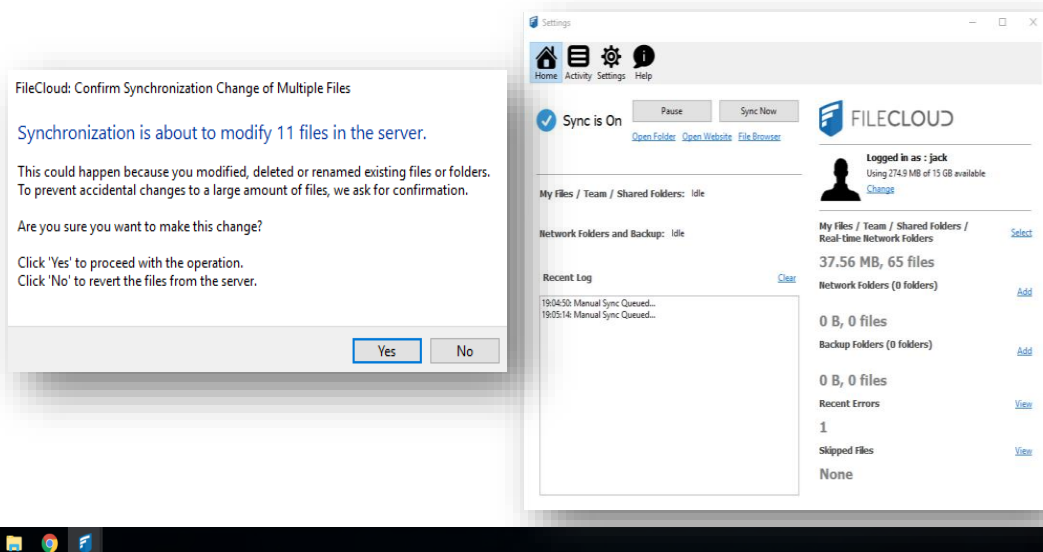


Using FileCloud Sync to Protect from a Ransomware attack

You can use FileCloud Sync to keep a folder on any computer that is synchronized with your FileCloud server.

- FileCloud Sync is a client application. This is because it allows you to access the FileCloud Server and the files you store there.
- You can access files in Sync like you do on a Windows PC in Windows Explorer or Mac OSX Finder.
- The same features that are available on the User Portal are also available in Sync.
- Sync allows you to easily open the User Portal if you need to.
- You can configure Network Folders to be automatically synchronized to your client.
- You can back up Sync files for safekeeping
- Sync includes an assistant to make it easy to access Sync files from Microsoft applications. In FileCloud Server version 18.2 and later.

FileCloud Sync can also be configured to detect large file changes and prevent this changes to be automatically synced to your FileCloud using our Centralized Device Management feature. When configured in the case of a Ransomware attack FileCloud Sync will pop-up a warning message requesting for your confirmation prior to uploading any compromised file. Using our sync client you can rest assured that even if your local computer is compromised your data in FileCloud is safe.



Use FileCloud Workflows to Protect your Data's Integrity

FileCloud Workflows you will be able to avoid users.Using uploading files which can compromise your data's integrity. If the workflow is triggered FileCloud will automatically Alert you and or Delete the file depending on your settings.

FILECLOUD

admin

Manage Workflows

Workflow

[Add Workflow](#)

Workflow Name	IF THIS	THEN THAT	Last Check	Last Action	Actions
Verify Integrity and Alert on Mismatch	If a file is added or updated	Verify file integrity and generate admin alert on mismatch	Never	Never	Edit Refresh Reset Delete
Verify Integrity and Delete if mismatch	If a file is added or updated	Verify file integrity and delete on mismatch	Never	Never	Edit Refresh Reset Delete

Page 1 of 1
2 rows



Integrate ClamAV or use ICAP to Integrate with your Antivirus

You can configure FileCloud to scan uploaded files using ClamAV, open-source antivirus software that is included with FileCloud.

When a virus is detected in an uploaded file, the following actions occur:

- The incoming file is deleted.
- An alert will be displayed in the Admin Portal.
- A toast will be displayed in the User Portal.
- An entry will be added in the audit log about virus detection in the file and subsequent deletion of the file.

As well FileCloud gives you maximum flexibility when choosing an antivirus product to scan uploaded files. FileCloud uses Internet Content Adaption Protocol (ICAP) to integrate with any antivirus product currently supporting ICAP.

FileCloud's ICAP integration features:

- Works on both Linux and Windows servers
- Triggers virus scanning only for uploaded files, that is - when files are uploaded to a FileCloud server instance
- Scanning is scheduled "inline" as soon as the file upload is completed
- Is part of FileCloud server itself
- Provides flexibility and scalability - the ICAP antivirus server does not have to be deployed on the same server as the one running the FileCloud server instance.





Recovering your Data after an Attack

Third Party Integrations

Misc

Anti-Virus

Salesforce

Reset to defaults

Anti-Virus Type

ICAP AV

Select an Anti-Virus type to configure

Save

You have unsaved changes.

NONE

ICAP AV

Clam AV

ICAP Anti Virus Server Settings

Check ICAP

ICAP Test

Server Local IP

0.0.0.0

Specify this server's local IP (must not be 127.0.0.1)

ICAP Remote
Hostname

toh.codelathe.com

Specify the ICAP server remote hostname

ICAP Port

1344

Specify the ICAP server port

Skip Scanning For Files
Greater Than

Units

0.09765625

GB

Skip files greater than this size (GB)

ICAP Service Name

SYMCSanReq-AV

ICAP Service name

Enable Debug for ICAP
client

Enable Debug for ICAP client

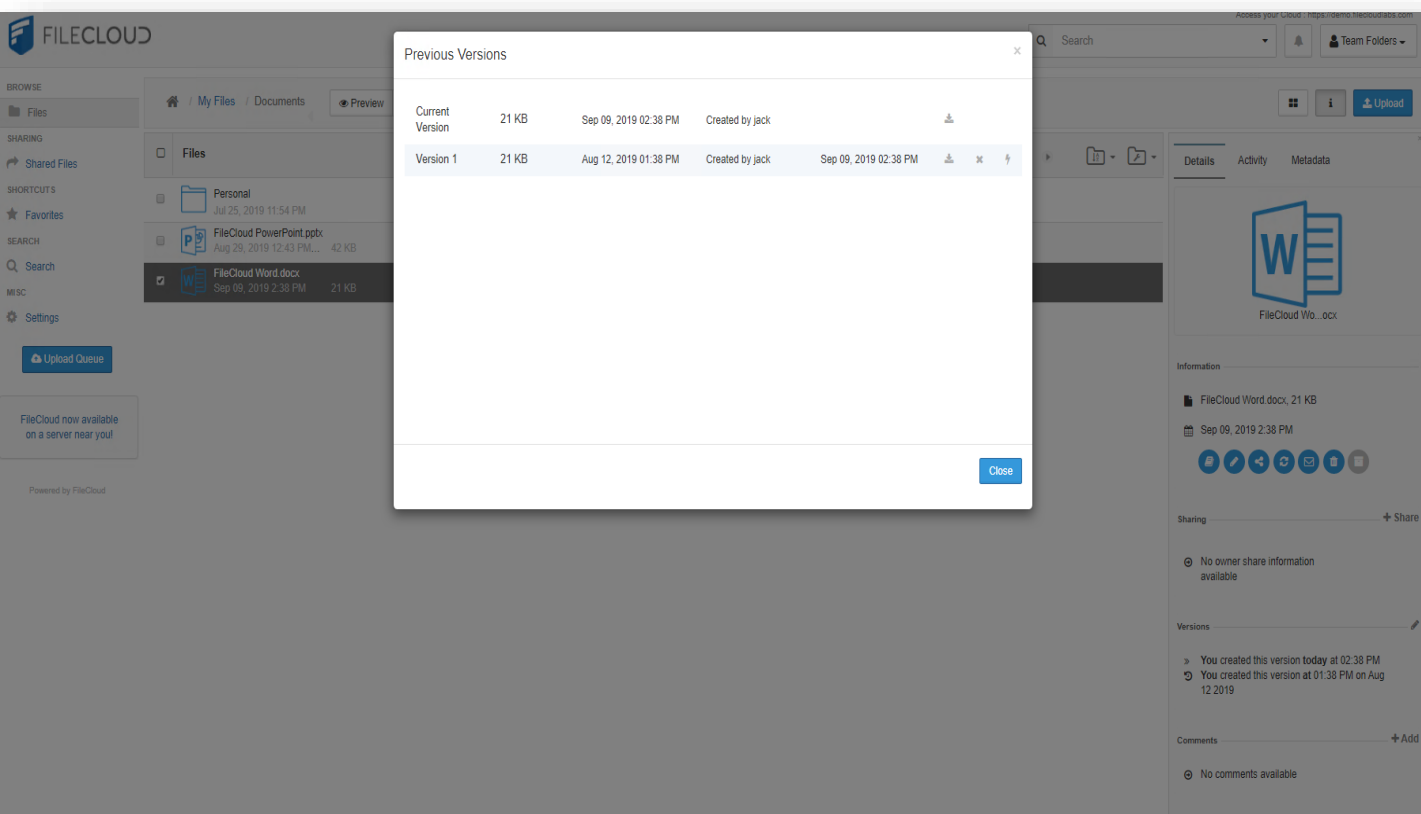
Enable Network Debug
for ICAP client

Enable Network Debug for ICAP client



FileCloud File Versioning Capability to Recover compromised files

FileCloud automatically maintains multiple versions of a file . The number of version kept is configurable by the system administrator. By default up to 3 versions are kept. If any older versions of a file is available, it can be accessed using the context menu. Previous versions are available only for Managed storage and Network Folders. If one or multiple files have been compromised you can restore them to a previously working version. In the event of a ransomware attack in a client computer, if the data had been versioned in FileCloud server, then the client computer data can be restored using older versions from the server. FileCloud offers unlimited versioning and endpoint backup to help companies develop effective anti-ransomware strategies.



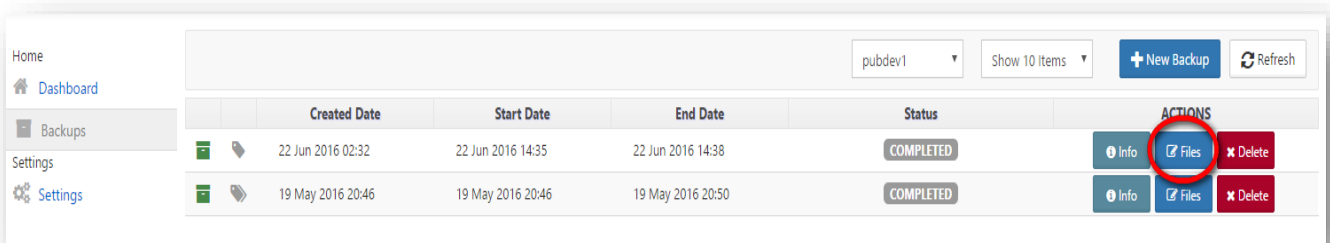
The screenshot displays the FileCloud web interface. A central dialog box titled "Previous Versions" is open, showing a table of file versions. The table has columns for version type, size, creation date, and creator. The current version is highlighted in blue. Below the table is a "Close" button. The background interface shows a file list with "FileCloud Word.docx" selected, and a right-hand sidebar with file details, sharing options, and version history.

Version	Size	Created	Created by
Current Version	21 KB	Sep 09, 2019 02:38 PM	Created by jack
Version 1	21 KB	Aug 12, 2019 01:38 PM	Created by jack



Restoring your Data using The FileCloud Server Backup Tool

FileCloud backup server supports restoring of files/folders from the backups. When a file/folder is selected for restore, it will be uploaded directly to its original location as found in the backup.

- You can restore user files and folders using Backup Server.
- You can restore databases and the entire cloud storage path manually, using the back ups you have created.



The screenshot shows the FileCloud backup server interface. On the left, there is a navigation menu with 'Home', 'Dashboard', 'Backups', 'Settings', and 'Settings'. The main area displays a table of backup records. The table has columns for 'Created Date', 'Start Date', 'End Date', 'Status', and 'ACTIONS'. The 'ACTIONS' column contains 'Info', 'Files', and 'Delete' buttons. The 'Files' button in the second row is circled in red.

	Created Date	Start Date	End Date	Status	ACTIONS
	22 Jun 2016 02:32	22 Jun 2016 14:35	22 Jun 2016 14:38	COMPLETED	Info Files Delete
	19 May 2016 20:46	19 May 2016 20:46	19 May 2016 20:50	COMPLETED	Info Files Delete





About Us

"FileCloud is used by 1000s of customers around the world including Global 2000 enterprises, government organizations, educational institutions, and managed service providers."

"We liked FileCloud's pricing, comprehensive feature set (branding, encryption) and the responsive support"

Stewart

A privately held software company, headquartered in Austin, Texas, USA. Our company offers two products – Tonido for consumers and FileCloud for businesses – used by millions of customers around the world, ranging from individuals to Global 2000 enterprises, educational institutions, and government organizations, and managed service providers.



To read more about how FileCloud can help keep your information secure as it is shared, visit www.getfilecloud.com

