FILECLOUD

FileCloud Best Practices for Ransomware Protection

whitepaper

FileCloud combines the benefits of collaboration and productivity with the security you require to protect your Intellectual Property anywhere it goes in the course of doing business.

This whitepaper explores some of the best practices organizations can follow to maximize productivity by collaborating securely.

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.

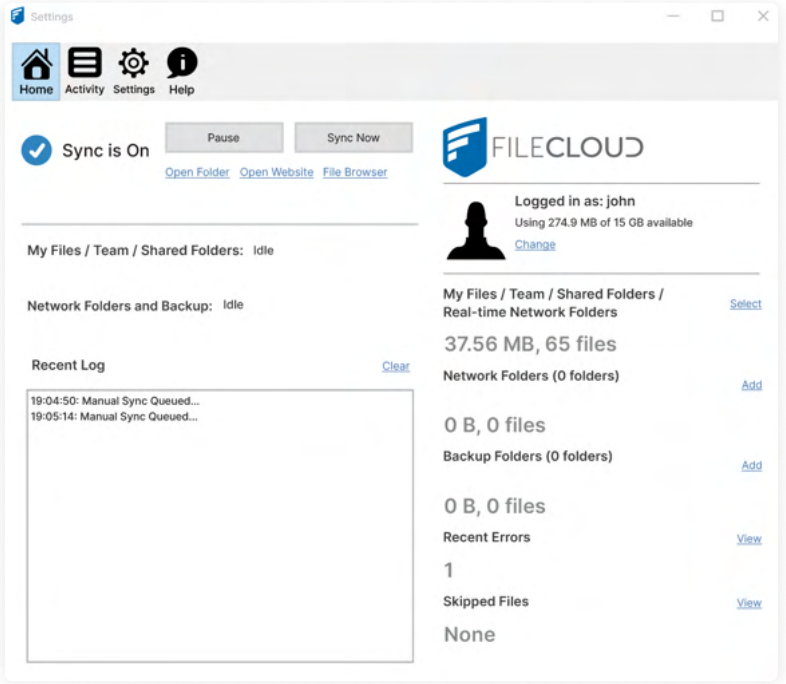
Sync allows you to easily open the User Portal if you need to.

You can configure Network Folders to be automatically synchronized to your client.

You can back up Sync files for safekeeping.

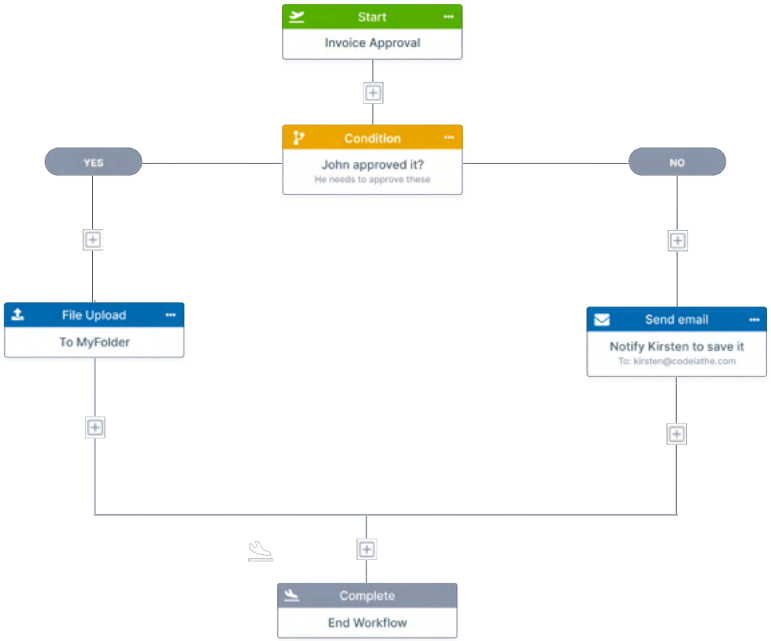
Sync includes an assistant to make it easy to access Sync files from Microsoft applications. In FileCloud Server version 18.2 and later.

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.



Integrate ClamAV or use ICAP to Integrate with your Antivirus

You can configure FileCloud to scan uploaded files using ClamAV, an 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.

FileCloud gives you maximum flexibility when choosing an antivirus product to scan uploaded files as well. 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

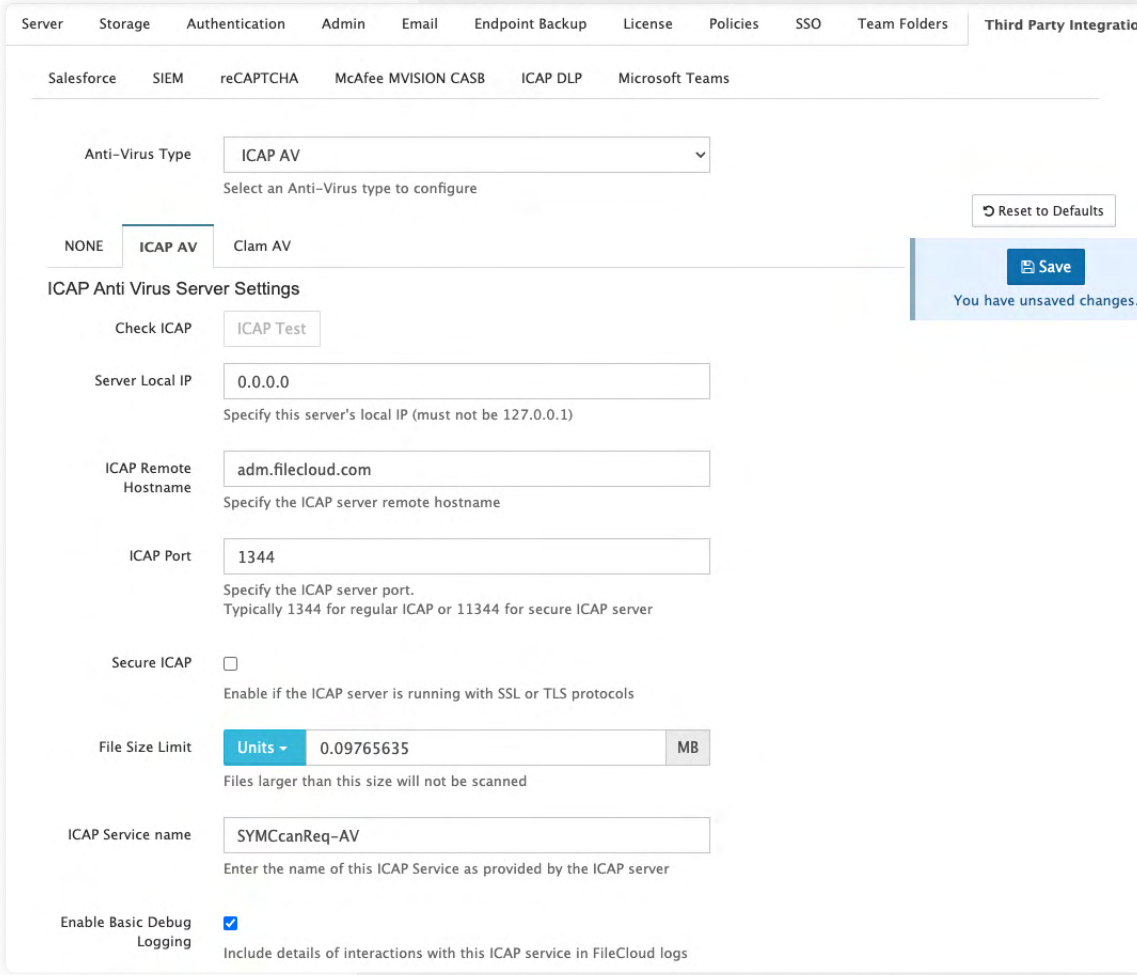
Scanning is scheduled "inline" as soon as the file upload is completed

Is part of FileCloud server itself

Triggers virus scanning only for uploaded files, that is - when files are uploaded to a FileCloud server instance

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.

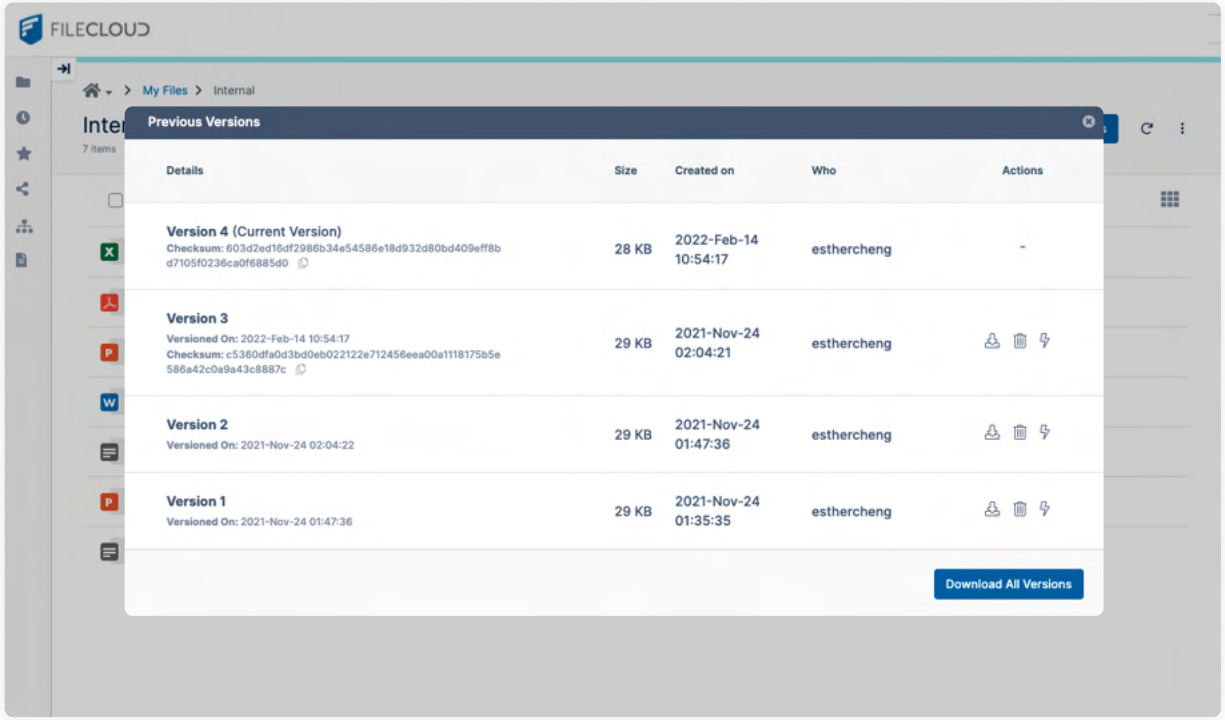
Recovering your Data after an Attack



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.

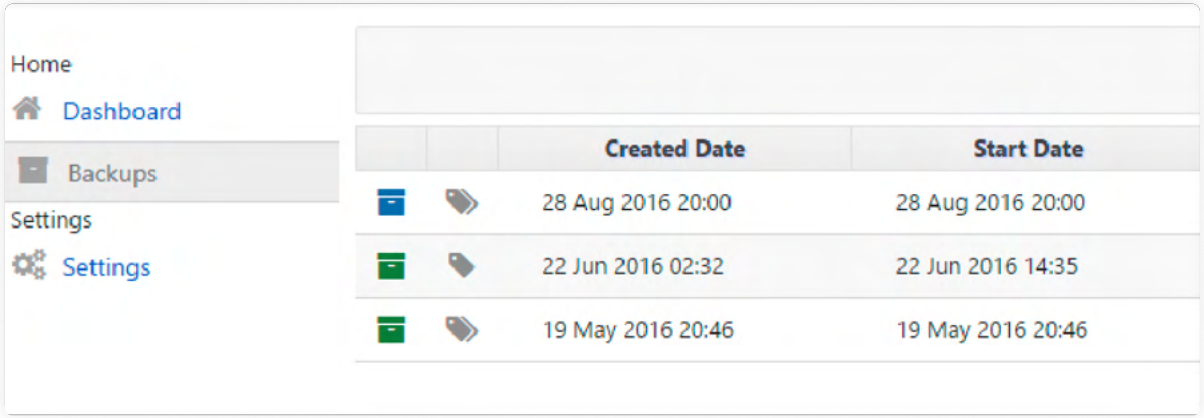


Restoring your Data using The FileCloud Server Backup Tool

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.



About Us

A privately held software company, headquartered in Austin, Texas, USA, FileCloud is helping organizations thrive by providing hyper-secure content collaboration and processes solutions. FileCloud is used by millions of customers around the world, ranging from individuals to Global 1000 enterprises, educational institutions, government organizations, manufacturing companies, managed service providers and more.

1M+
USERS

3000+
ENTERPRISES

100+
RESELLERS

90+
COUNTRIES

13785 Research Blvd, Suite 125
Austin TX 78750, USA

Phone: U.S: +1 (888) 571-6480
Fax: +1 (866) 824-9584

support@filecloud.com
https://www.filecloud.com

CMS CENTERS FOR MEDICARE & MEDICAID SERVICES
REUTERS
US Army Corps of Engineers
NASA
COLUMBUS REGIONAL HEALTH
TOYOTA
Deloitte.

Copyright Notice

While all reasonable care has been taken in the preparation of this document, no liability is accepted by the authors, FileCloud, for any errors, omissions or misstatements it may contain, or for any loss or damage, howsoever occasioned, to any person relying on any statement or omission in this document.