

Another SFTP server

A very useful feature of SFTP.cloud is that it can be used as a cloud-native secure front-end to **bridge traffic to another (often on-prem) SFTP server, without opening up such SFTP server to the world.**

Easy to do with SFTP.cloud. Just deploy the Storage Connector on or near the SFTP server you want to protect, then create a VFS that points to it. The Storage Connector connects to the SFTP.cloud SaaS only outbound so you can keep all your inbound firewall ports closed and your original SFTP server safe.

Here's an example of how to configure a VFS that points to an SFTP server. Note: even though your auth data is stored encrypted in the Connector's DB, and even though all traffic between Connector and your internal SFTP server is on private LAN, using PKI auth is still the strongly recommended way.

SFTP cloud Connector

EARLY ACCESS

Dashboard

STORAGE

Virtual file systems

ACCESS

Users

Folder sets

AUTOMATION

Scripts

Event handlers

Schedules

Transfers

Secrets

MONITORING

Activity

Log integrity

SYSTEM

Settings

Network

Administrators

Updates

Search or jump to

Ctrl K

Storage

Virtual file systems

Encryption keys

Virtual file systems map your storage (a folder, a bucket, a container, a remote server) into names users can be given access to.

Search

NAME	TYPE	TARGET
bulk	Imported	Disk /opt/Syncplify/sc-conn-data/devfs/legacy/bulk
devfs	Disk	/opt/Syncplify/sc-conn-data/devfs
imp94986hash	Imported	Disk /opt/Syncplify/sc-conn-data/devfs/legacy/imp94986hash
imp94986keys	Imported	Disk /opt/Syncplify/sc-conn-data/devfs/legacy/imp94986keys
imp94986none	Imported	Disk /opt/Syncplify/sc-conn-data/devfs/legacy/imp94986none
imp94986plain	Imported	Disk /opt/Syncplify/sc-conn-data/devfs/legacy/imp94986plain
imp95089hash	Imported	Disk /opt/Syncplify/sc-conn-data/devfs/legacy/imp95089hash
imp95089keys	Imported	Disk /opt/Syncplify/sc-conn-data/devfs/legacy/imp95089keys
imp95089none	Imported	Disk /opt/Syncplify/sc-conn-data/devfs/legacy/imp95089none
imp95089plain	Imported	Disk /opt/Syncplify/sc-conn-data/devfs/legacy/imp95089plain
linode-bucket	S3	s3://my-fancy-test-bucket
my-amazon-s3	S3	s3://syncplify3testbucket
my-minio	S3	s3://my-minio-bucket
my-rustfs	S3	s3://my-rustfs-bucket
seed-000	Disk	/opt/Syncplify/sc-conn-data/devfs/seed/seed-000
seed-001	Disk	/opt/Syncplify/sc-conn-data/devfs/seed/seed-001

Create virtual file system

Name

my-lan-sftp-server

Type

SFTP

CONNECTION

Host

syncplify.com

Port

22

Remote path (optional)

The starting directory on the remote server. Leave blank for the server root.

CREDENTIALS

Username

Password

Set

Private key (optional)

PEM content, an alternative or complement to the password.

Configured

Replace

Remove

TRANSFER SPEED

Parallel connections to your cloud site

Standard (one connection)

More connections move more files at the same time between this Connector and your cloud site. They also use more of your internet upload bandwidth while transfers are running. Start with Standard; raise it only if transfers feel slow and your connection has room.

AT REST ENCRYPTION

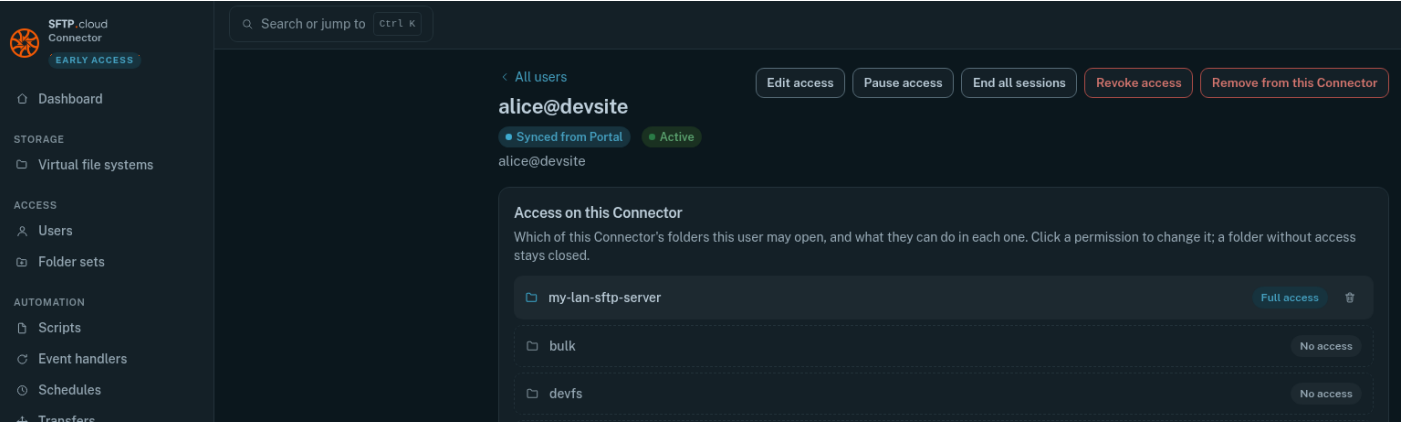
At rest encryption is not available for the SFTP type: the remote server owns that storage.

Advanced

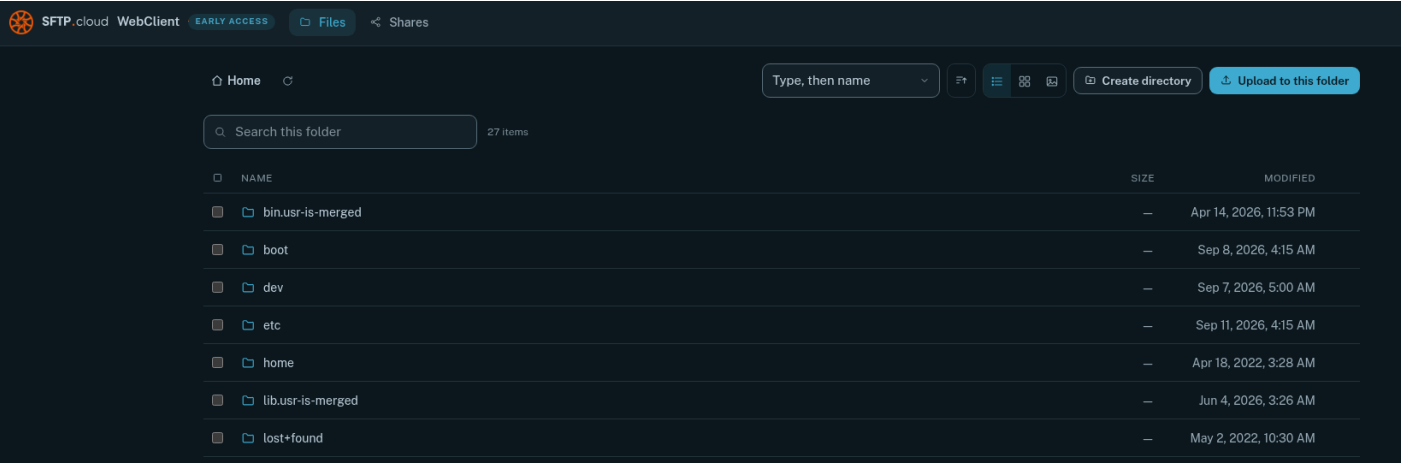
Cancel

Create

Once you've created the VFS, simply switch to the Users page, and grant access to the newly created VFS for all the transfer users you want to be able to access it.



Once that's done, the users you granted access to will be able to point their browser or SFTP client to your SFTP.cloud hostname, sign in, and interact with your now-fully-protected original SFTP server:



[Manual: [general information about storage back-ends](#)]