How to Enable FIPS Encryption in FileCloud

FileCloud is pleased to offer a FIPS-certified (CMVP certificate #3338) solution for defense agencies, the public sector, and government contractors.
A special FileCloud license is required for this configuration, which enforces FIPS-certified cryptographic modules to secure data at rest (256-bit AES) and in transit (TLS 1.3).

These step-by-step instructions should be implemented by the IT administrator who will be configuring the FileCloud installation.
For additional support or to add FIPS to your FileCloud license, please contact us.

Enable FIPS in FileCloud for Data at Rest

Note: Data must be decrypted with each access (slower performance)

Step 1 – Check Prerequisites

Confirm that memcached has been installed. If the default path for openssl.cnf has been changed, you must set your custom path to the SSL configuration file by overriding the config value of *SSL_CONF_FILE in cloudconfig.php*.

Step 2 – Enable the Encryption Module

With FIPS Mode Activated	Without FIPS Mode Activated
Enable the FIPS admin banner	Enable the FIPS admin banner
Open file: WEBROOT/config/localstorageconfig.php	Open file: WEBROOT/config/localstorageconfig.php
Add: define("TONIDOCLOUD_FIPS140_ENABLED", 1)	**Add:** define("TONIDO_LOCALSTORAGE_INCLUDEENCRYPTION", 1);

Step 3 – Manage Storage Encryption

Navigate to Admin portal → Settings → Storage → My Files.

An “Encryption” option is now available.

Admins can set an optional password while enabling encryption, as well as a recovery key that can reactivate the encrypted system if the password is lost. The recovery key is only available for download once.

Step 4* – Enable Encrypted Files

If your local storage already contains files, click “Encrypt All.”

*If your local storage did not have any files, this button will not appear.

Read the full Documentation

Enable FIPS in FileCloud for Data in Transit

1 Enable Dracut modules in CentOS

Run Command:
yum install dracut-fips
yum install dracut-fips-aesni
dracut -v -f

2 Add the FIPS flag to the Grub Configuration

Open file: /etc/default/grub and add: “fips=1” to GRUB_CMDLINE_LINUX.

e.g.,GRUB_CMDLINE_LINUX=”crashkernel=auto rd.lvm.lv=centos/root rd.lvm.lv=centos/swap rhgb quiet fips=1

3 Regenerate the Grub Configuration

(Disable prelinking first if enabled on this server)

Run Command:
grub2-mkconfig -o /etc/grub2.cfg

4 Reboot the Server

Once the server is rebooted, confirm that FIPS is active in this file: cat/proc/sys/crypto/fips_enabled

[root@cnfc ~]# cat /proc/sys/cryto/fips_enabled1

5 Install FileCloud

Run Command:
yum install wget
wget http://patch.codelathe.com/tonidocloud/live/installer/filecloud-liu.sh && bash filecloud-liu.sh

Alternative Options

Install OpenSSL Certificate

If SafeLogic modules are required, FileCloud supports FIPS-enabled OpenSSL certificates.By default, FileCloud FIPS mode installs CentOS FIPS-enabled packages.

Run Command:
yum install unzip
wget http://patch.codelathe.com/tonidocloud/live/3rdparty/fipsopenssl/fipsopenssl.zip
unzip -q fipsopenssl.zip -d /root/fipsopenssl
rpm -Uvh –nodeps /root/fipsopenssl/*.rpm

Enable TLS 1.2/TLS 1.3 in Apache SSL configuration

Run Command:
#SSLProtocol all -SSLv2 -SSLv3
SSLProtocol -all +TLSv1.2 +TLSv1.3
#SSLCipherSuite HIGH:3DES:!aNULL:!MD5:!SEED:!IDEA
#SSLCipherSuite HIGH:!aNULL:!MD5
SSLCipherSuite HIGH:!MEDIUM:!LOW:!EXP:!aNULL:!MD5:!EXPORT:!eNULL:!kECDH:!aDH:!RC4:!3DES:!CAMELLIA:!PSK:!SRP:!KRB5:@STRENGTH

Read the full step-by-step guide on our blog!

Read Guide

+1 (888) 571-6480