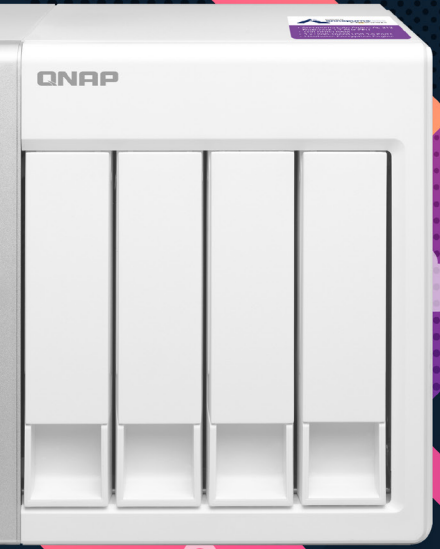


QNAP

Protect your confidential data, Share securely with

QENC encryption on QNAP NAS

Coming Soon!
Will be released with QTS 4.4.1

Outline

1. The importance of encryption
2. What is QENC
3. How to secure files with QENC
4. Demo: File Station, Qfiling

1

The importance of encryption

Do you know...

McAfee made a survey to 30 million Skyhigh cloud service users

18% of files uploaded to cloud-based file-sharing and collaboration services contain sensitive data*

Technology media CSO from IDG pointed

58% of senior managers had accidentally sent the wrong person sensitive information

Ponemon Institute (U.S.) released a survey at 2019

54% rank employee mistakes as the top threat to sensitive data; more than external hackers(30%) and malicious insiders(21%) combined

*** Categories of sensitive data**

Confidential (44.4%)
- Financial records, business plans

Personally identifiable information (3.9%)
- ID numbers, dates of birth

Password (3.2%)

Payment information (2.3%)
- Credit and debit card numbers

Protected health information (1.6%)
- Patient diagnoses, medical treatments

Protect data, prevent from risk

Protecting data is a responsibility to the enterprise.

- Customer information, employees personal data, trade secrets, and new product plans.
- Data breach causes loss of money and reputation, furthermore, legal responsibility.
- The GDPR became effective in 2018. The CCPA becomes effective on 2020. How to process and store personal data need to follow the regulations.

So do individuals

- Financial and medical data as well as credit card number and health records.
- It would cause a huge loss if sensitive personal data was stolen or used in illegal way.

QENC - File Encryption on QNAP NAS

Existing encryption features

Disk Encryption

Share Folder Encryption

Disk and Share Folder Encryption protect data from unauthorized access even if the hard drives or the entire NAS were stolen.

New Feature:

QENC File Encryption

File Encryption

Encrypted qenc files can't be read or open. Are secured when shared.

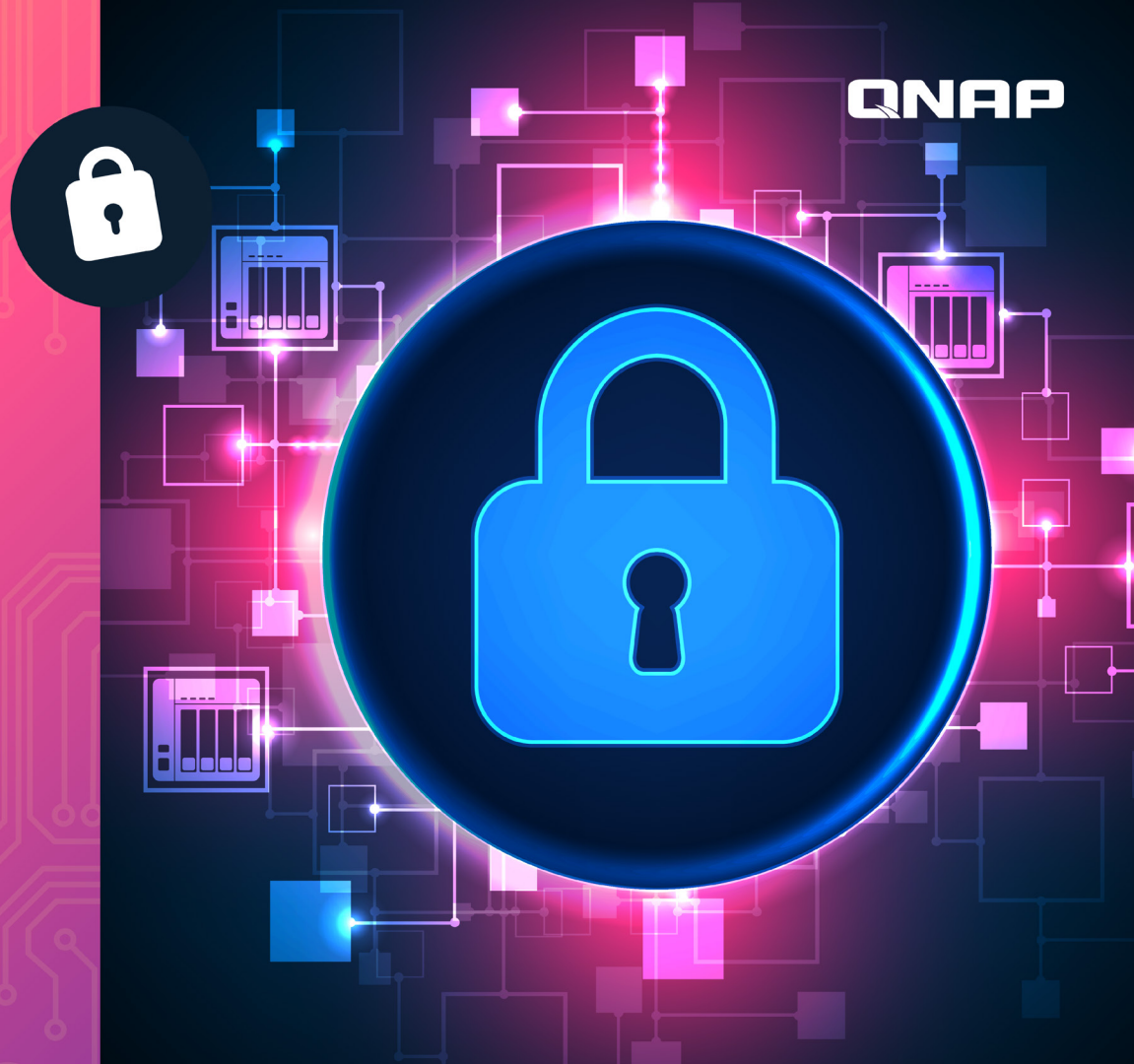
Coming soon with QTS 4.4.1!

Encrypt Files to Safely Share Them!

- When sharing files via Email, communication app, files leave the protection of QNAP NAS.
  - Providing health records to your doctor
  - Send ID via LINE to apply for a loan.
    (Taiwan government listed Communication App into financial examination.)
- You might do it very carefully. But, how to make sure every recipient never makes mistake to send sensitive data to unwanted parties?
- QENC protects files even if the files are breached.

2

What is QENC



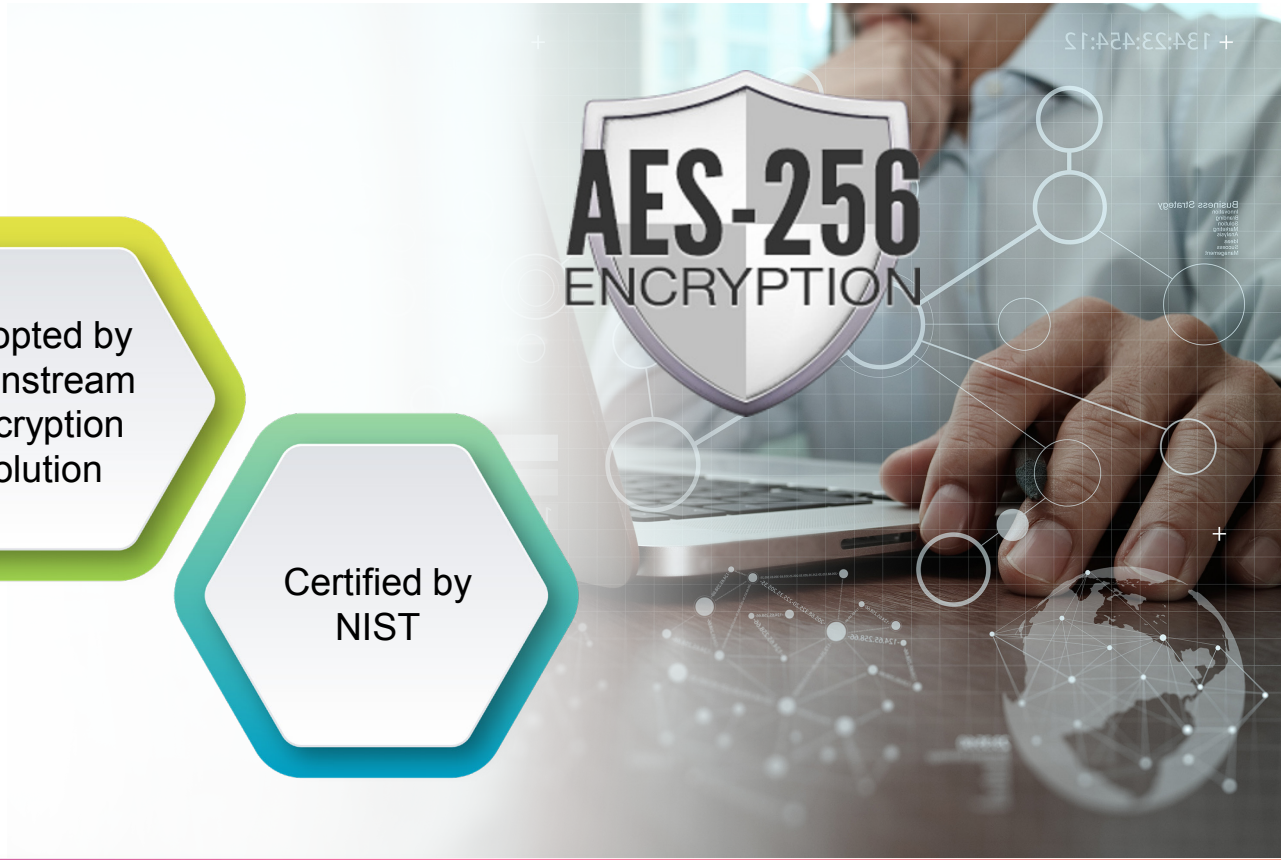
QENC, A File Encryption Module for QTS

Specially designed for QNAP NAS, QENC encrypts files so that no one can open or view until they input the correct password. Encrypted files become QENC files. You can tell them by the file name extension.

- Encrypted file extension: .qenc
- Encryption algorithm: AES 256
- Password length: Up to 32 characters, special characters allowed.

Adopt AES as encryption algorithm

- Efficient in encryption
- Adopted by mainstream encryption solution
- World most widely used
- Certified by NIST



AES: NIST Certified Encryption Standard

- Adopted by the U.S. government.
- The U.S. National Institute of Standards and Technology, NIST published AES as FIPS 197 in 2001
- More efficient than DES (Data Encryption Standard, the former encryption standard). Less memory requirements .

Source: http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

AES is widely used in mainstream encryption

Operation Systems

- ✓ Microsoft EFS (Encrypting File System)
- ✓ Apple macOS

Cloud Storages

- ✓ Google Drive
- ✓ Dropbox

All use AES-256 and AES-128 as algorithm to encrypt files.

Encryption software

- ✓ World famous encryption software use AES too.

Software name	Download times	algorithm
AxCrypt	20M	AES
Folder Lock	1M	AES
Folder Password Lock Pro	143K	AES
VeraCrypt	41K	AES

3 benefits of encrypting in QNAP NAS

1. Fasten another Lock to sensitive files

- ✓ Encrypted files cannot be read without the password.
- ✓ If a QNAP NAS is a bank, QENC is a portable safe box.

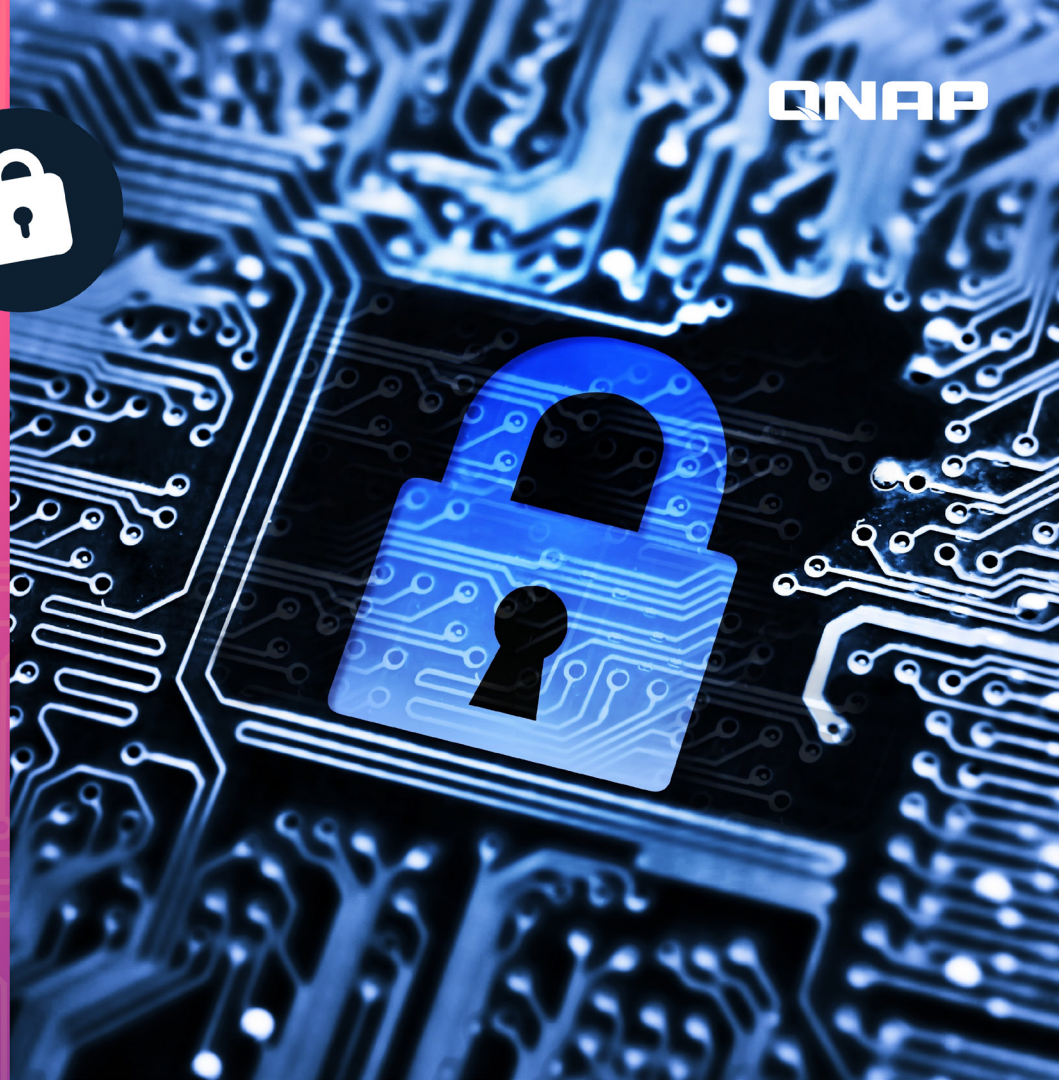
2. Solve file level encryption demands on QTS

- ✓ Decrease the risk when transfer files to other site or device
- ✓ No need to install any other software.

3. Support decryption on Windows, macOS and Mobile devices.

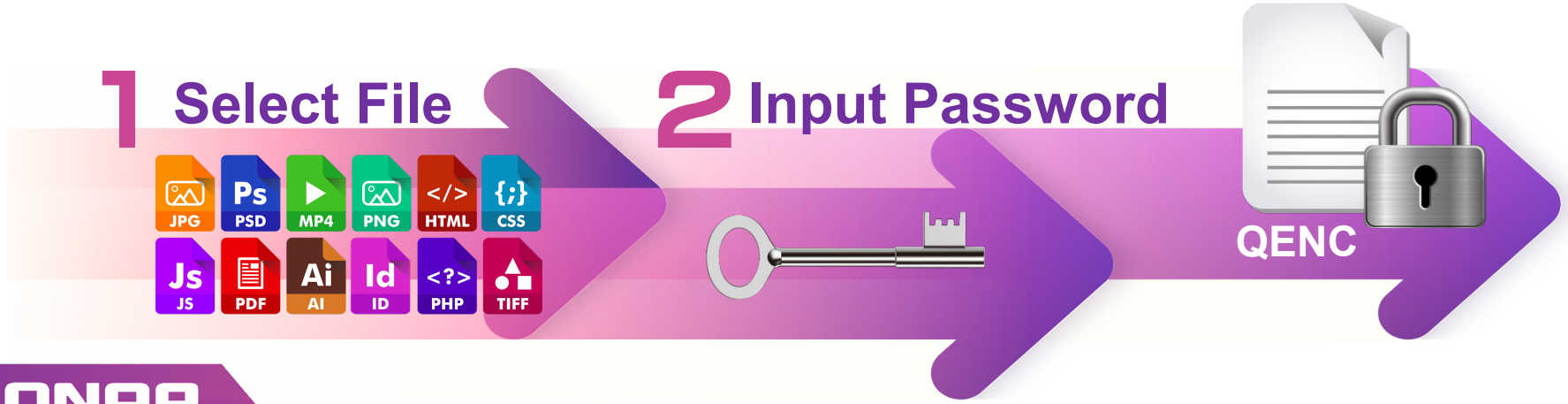
3

How to secure files with QENC



2 Steps to Encrypt, Securely Share

- From QTS 4.4.1, you could encrypt, decrypt in File Station
- Any type of file can be encrypted
  - ✓ Photos, document, sheets, audios, videos, web page ...



4 ways to encrypt or decrypt

File Station
Manage, encrypt, share
Qfiling
Organize files and batch encrypt

Using QTS

Qfile
Encrypt and share
anytime, anywhere

Using Mobile Device

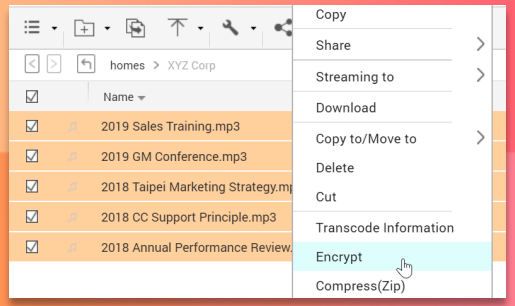
QENC Decrypter
Decrypt files on Windows
mac Device

Can't connect to the NAS/
Share files to those that don't
own a NAS

File Station - Manage files and Encrypt/Decrypt

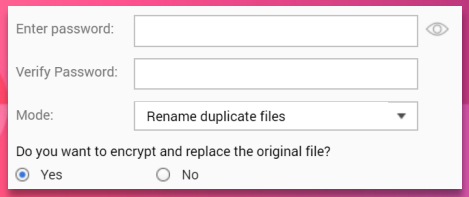
Step 1.

Select files, Right click and choose “Encrypt”.



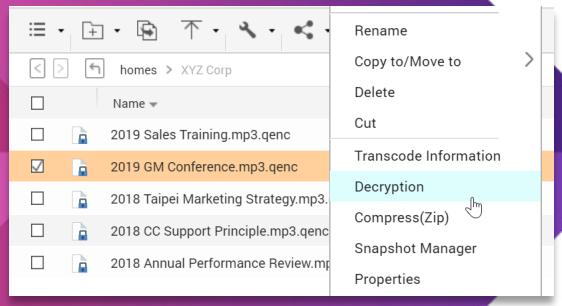
Step 2.

Input password: up to 32 characters, special characters allowed.



Step 3.

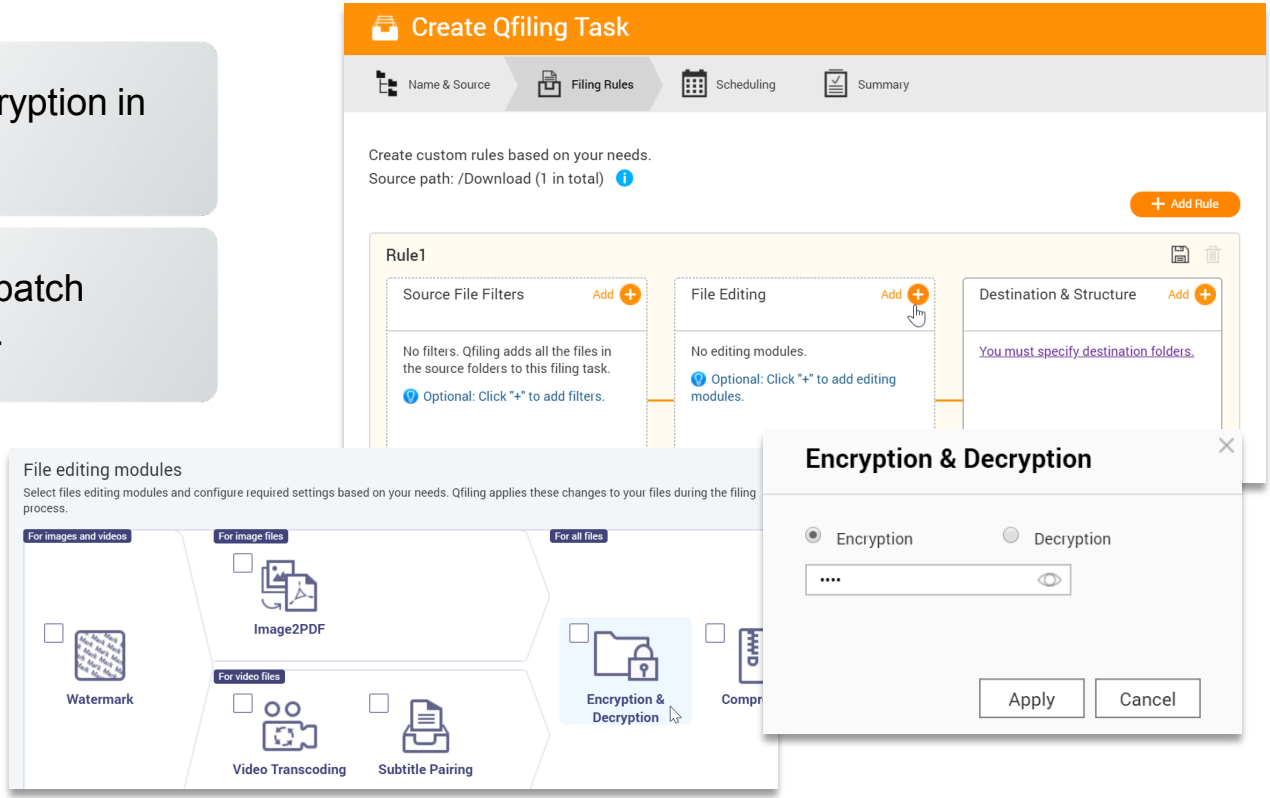
Encryption finished. Filename extension became qenc.



Qfiling - Organize files and batch encrypt

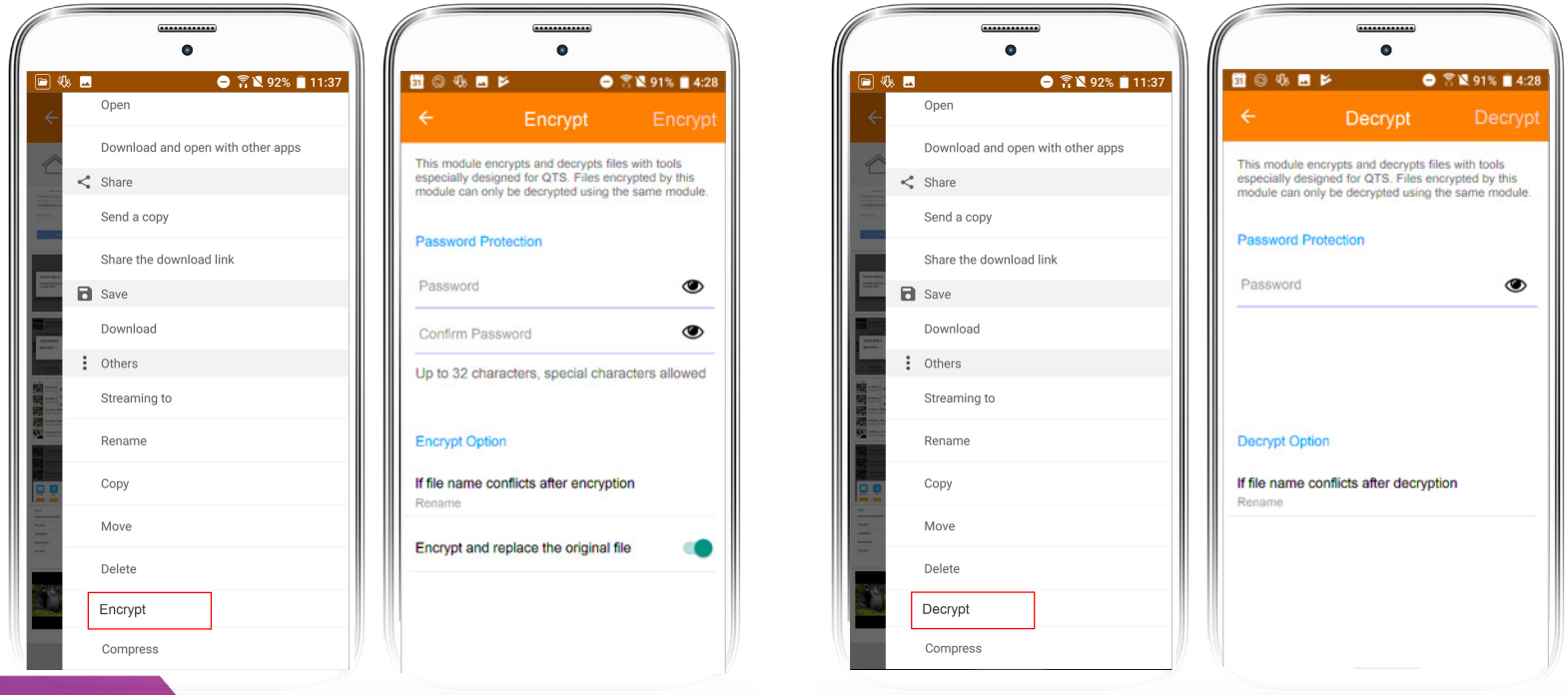
1. Select Encryption/Decryption in File Editing Modules.

2. Input password to set batch Encryption/Decryption.



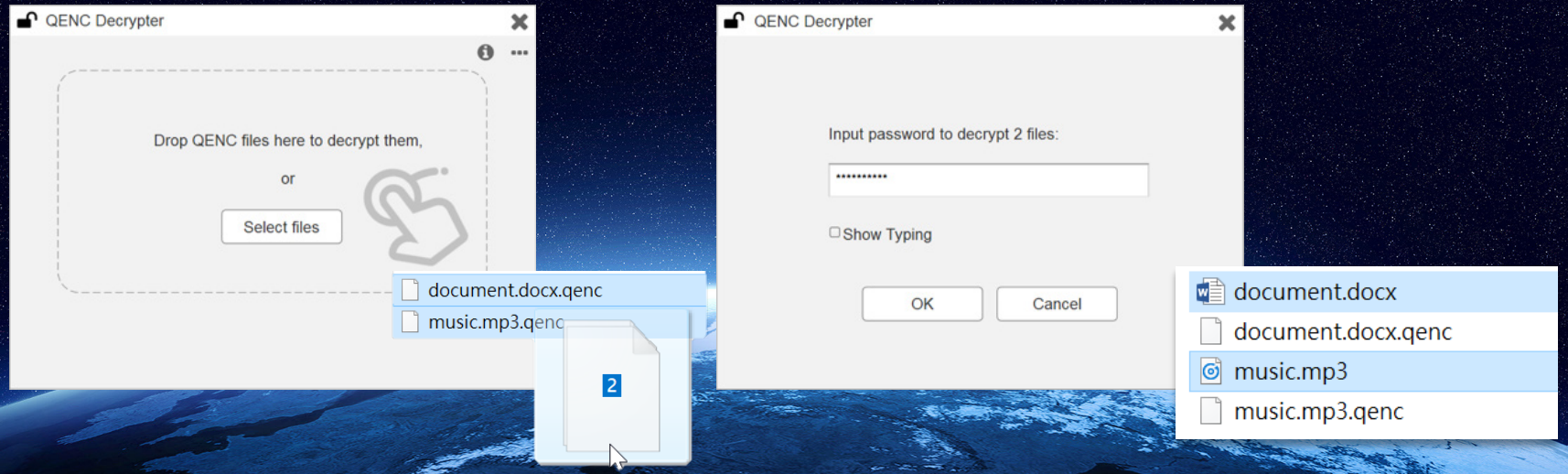
Qfile – Encrypt/Decrypt and share anytime, anywhere

Access QNAP NAS, encrypt or decrypt files on Android, iOS devices with Qfile. (Coming soon)



QENC Decrypter - Decrypt on PC Locally

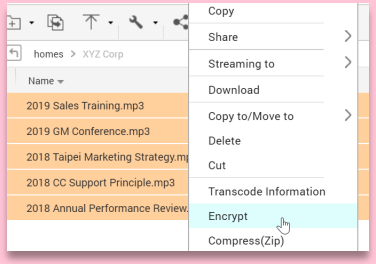
- QENC Decrypter (Coming soon)
- Support Windows/ macOS

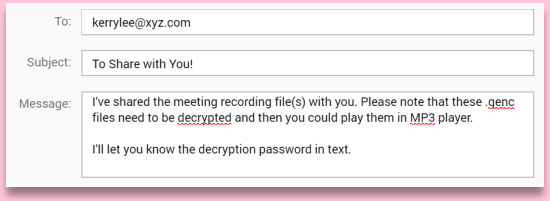


Share encrypted files, easily and securely

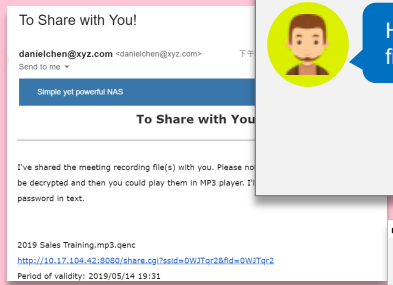
Encrypt before share, send password in another way. Make sure only specific people can open the file.

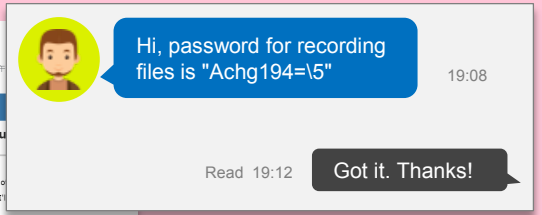
File Owner

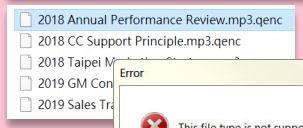


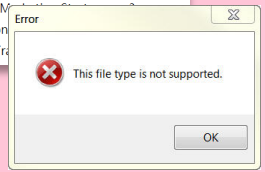


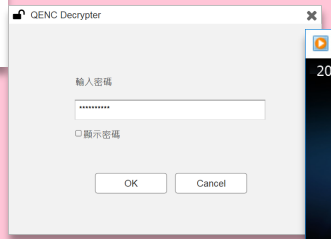
Recipient

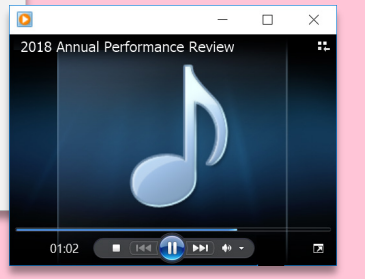












Demo

Encryption on File Station and Qfiling

Reminder: Protect password

Even with strict information security technology and hard-to-crack encryption algorithms, you still need to **use them correctly** to truly protect your confidentiality.

1. Do not record password where others can reach.
2. Only send password via trustable communication app. Carefully choose recipients to provide password.
3. REMEMBER your password! Even QNAP cannot decrypt files for you without the password you set.

QNAP

QNAP

Securely share your sensitive files, with

QENC file level encryption.