

SecureStream 256 Pro – User Manual

Version 1.0 (Stable Release)

SecureStream 256 Pro is an application for secure file encryption and decryption utilizing AES-256-GCM for confidentiality and integrity, Argon2id (KDF), HKDF for key derivation, and HMAC/KCV for key validation.

The program supports processing of large files with chunking, metadata obfuscation, and secure handling of I/O and file permissions.

Quick Start

- 1 Launch the application and select the folder containing the files.
- 2 Choose the authentication method: password or key file (.key, 32B).
- 3 Optionally configure extension filters, backup, and metadata obfuscation.
- 4 Adjust Argon2id parameters and chunk size if necessary.
- 5 Click Encrypt or Decrypt and monitor the progress..

Password vs. Key File (.key)

Password – convenient, flexible; its strength depends on password quality.

Recommended: minimum 12–16 characters with a diverse character set.

Key file (.key, 32 bytes) – provides the highest level of security, independent of password strength; requires secure storage of key copies, preferably offline..

Metadata Obfuscation

The Hide Metadata option removes the file name and extension from the header.

The original name and extension are encrypted within the stream and revealed only after decryption.

This enhances privacy at the cost of more difficult extension-based filtering during encryption.

Backup

Enabling Backup creates copies as follows: during encryption — a copy of the plaintext file in the backup subfolder; during decryption — a copy of the .enc file.

The backup folder is automatically excluded from further processing.

Privacy and Network — No Telemetry (100% Offline)

SecureStream 256 Pro operates in a fully offline mode.

The program does not initiate outbound connections and does not collect telemetry data; all logs remain strictly local.

Chunk Size – How to Choose the Settings

Chunking defines the size of the data portion processed in a single step.

A larger chunk typically improves throughput on fast storage (SSD/NVMe) and with large files, but increases temporary memory usage and may reduce system responsiveness on lower-end machines.

By default, 8 MiB is set as a reasonable compromise.

Chunk(MiB)	Use Case	Advantages	Notes
1–2	Old HDD, low RAM, small files, heavily loaded systems.	Low RAM usage, good responsiveness.	Lowest throughput; more I/O operations.
4	Universal for mixed file sets.	Balanced I/O and RAM.	Slower than 8–16 MiB on SSD.
8 (default)	SSD/SATA and most scenarios.	Good performance/RAM compromise.	Sufficient for files up to several tens of GB.
16	Faster SSD/NVMe, larger video files, archives.	Higher throughput.	Slightly higher RAM usage.
32–64	NVMe, very large files, local disk.	Maximization of throughput.	May reduce responsiveness on weaker CPU/RAM.
128–256	Servers, ultra-fast arrays/NVMe.	Highest throughput.	High RAM usage; rarely needed on desktops.

KDF Parameters (Argon2id)

Argon2id defines the computational cost of deriving a key from a password.

Higher values increase resistance against dictionary/GPU attacks,

but also prolong processing time. In SecureStream 256 Pro,

the default settings are $t=3$, $m=131072$ KiB (128 MiB), $p=4$.

Allowed ranges: t 1–10, m 32768–1048576 KiB (32 MiB–1 GiB), p 1–16.

Parametr	Description	Default	Range	Impact/Notes
t (timecost)	Number of iterations increases computation time.	3	1-10	Higher = slower, more secure.
m (memory KiB)	RAM used by KDF.F	131072	32768–1048576	Higher = slower, harder to attack in parallel.
p (parallelism)	Parallel KDF threads.	4	1-16	Match the number of cores; too high „p” may not improve speed.

Recommended Argon2id Settings

Scenario	Settings (t/m/p)	Comment
Laptop/Desktop (typical)	3 / 131072 / 4	Good security without noticeable slowdown.
High security.	4–6 / 262144–524288 / 4–8	Increased memory and time cost; check available RAM.
Lower-end hardware.	2 / 65536 / 2–4	Faster at the cost of reduced resistance.
Server/WS	3–6 / 262144–1048576 / 8–16	Leverage multi-core capability and larger memory.

Messages and Troubleshooting

Message/Symptom	Action
Invalid password/key (KCV) for file:	Key does not match the header; check the password/key file; ensure it is the correct .key file.
Header corrupted – name/ext lengths exceed file size.	The .enc file is corrupted or has been modified; try using a copy from the backup.
High RAM usage.	Reduce m (e.g., to 65536–131072 KiB) or chunk size; close other applications.

Parameters and Options – Summary

Options	Description	Default Value / Range
Authentication Mode	Password or 32-byte key file (.key)	Password (if no .key)
Hide Metadata	Does not store name/extension in the header; data stored inside the stream.	Disabled
Backup	Creates copies: plaintext during encryption, .enc during decryption.	Disabled
Extension Filters	Process only specified types (e.g., .pdf .jpg)	Manually enabled
Chunk (MiB)	Data chunk size in I/O	8 MiB (1–256 MiB)
Argon2id t/m/p	Time cost, memory (KiB), parallelism	3 / 131072 / 4 (t:1–10 m:32768–1048576 p:1–16)

Security Recommendations for Users

Passwords and keys – choose strong passwords (minimum 12–16 characters, diverse character types) and store them in a password manager.

Key files – do not store .key files in the same directory as the encrypted data. Keep them on a separate, secure medium.

Backups – regularly create backups of encrypted files and keys. Store the backup in a different, secure location.

Work environment – use the program only on devices with an up-to-date system and security software (antivirus, firewall).

Confidentiality – do not share passwords or keys with third parties. Remember that their compromise means a loss of data security.

Legal Notice

The SecureStream 256 Pro software has been developed with the utmost care and tested in accordance with the technical specifications described in this document.

The author makes every effort to ensure proper operation and security of the solution, but cannot guarantee complete error-free performance in every usage scenario.

The user is responsible for the manner in which the program is used, in particular for applying it in accordance with its intended purpose and the security principles described in the documentation.

The application operates 100% offline and does not collect telemetry.

The portable version is intended for personal use only (non-distributable); details are provided in the EULA.