How are passwords stored in EFT?

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- EFT Server, v8.0 and later

QUESTION

How are passwords stored in EFT?

ANSWER

EFT user and administrator passwords are stored as one-way, 32-bytes PBKDF2-HMAC-SHA1 hash, with random 18-bytes salt, 1996 iterations.

Passwords stored in memory are encrypted with two-fish.

In SQLite:

- Site-level and below: either encrypted with AES or IDs of the password physically stored in AKV
- Server-level: TwoFish

The EFT configuration files were moved to SQLite storage in EFT v8.0.0.37. Prior to v8, passwords managed by EFT for user and administrator authentication were stored using a base64-encoded SHA256* one-way hash. Passwords used for unattended operations such as outbound client transfers, database access, private key decryption, etc. must be reversible; thus, depending on the situation, these passwords are either obfuscated or encrypted (Twofish or similar) using a server-managed symmetric key. Passwords stored (temporarily) in memory are not encrypted.

GlobalSCAPE Knowledge Base
https://kb.globalscape.com/Knowledgebase/10400/How-are-passwords-stored-in-...