globalscape by HelpSystems

DATA SHEET

EFT™ OPENPGP MODULE FAQ

KEY RESULTS

- Globalscape® EFT™ employs industry-standard OpenPGP (based on the open source implementation of Pretty Good Privacy) technology to safeguard data at rest.
- In contrast to symmetric encryption technologies that rely on a single password or shared secret for encryption and decryption, OpenPGP uses a public/private key pair and a password.
- EFT adheres to the OpenPGP standard and is RFC 2440 compliant.

The EFT™ OpenPGP Event Rule Action can encrypt, sign, decrypt, and verify files, even on files larger than 2GB. Below are answers to questions often asked about the EFT™ OpenPGP module.

How are PGP keys stored? Are they on file system or in a database?

They are stored on the file system.

How are PGP keys (especially private keys) protected?

They are stored in a PGP key ring file outside the areas available to connected users. Private keys protected by a passphrase are encrypted based on your chosen cipher.

If PGP keys are encrypted, what cypher is used and where is the encryption key stored?

Private keys protected by a passphrase are encrypted based on your chosen cipher. 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.

If disk-level (or file-system-level) encryption is used for any purpose, what would prevent an admin from accessing data?

This is entirely dependent on the technology used and the methodology with which it is implemented and is outside the scope of EFT.

In a scenario where an encrypted file is received from a third party and needs to be decrypted and placed into the target environment by EFT, how is data protected after it is decrypted but before it is written to the destination?

There are many different possibilities depending on the location and type of storage chosen. For broad compatibility, EFT is primarily storage and data agnostic. The best practice is to ensure EFT is running on a well-protected and securely managed part of the internal network. Beyond that, if there is a further concern about the sensitivity of user data, then using some form of protected storage is recommended.

For example, if a workflow has been specifically designed such that the user data that will be decrypted for some period, and that unencrypted data is deemed to be too sensitive to allow it to remain even briefly in its unencrypted state on unencrypted storage even in a well-protected and securely managed part of the internal network, then it is recommended that the storage in which this workflow takes place be protected by any satisfactory technology and methodology. If Microsoft's EFS qualifies, then allowing EFT to enable EFS on some or all directories would be the quickest and easiest solution.

In a scenario where the file needs to be OpenPGP encrypted by EFT, when does encryption happen? How is the file picked up from the source?

Encryption happens at whichever step in a workflow the administrator has defined.

An administrator may choose to leverage the OpenPGP action directly against the original storage source, including UNC paths to shared folders on the network. Otherwise people or systems may upload a file to EFT via an enabled protocol, or EFT may copy, move, or download a file from a compatible system.

MORE INFORMATION

For more information about the OpenPGP module, refer to the topics below in the EFT online documentation:

http://help.globalscape.com/help/index.html.

- Viewing and Changing Key Pair Path Settings
- Creating Key Pairs for OpenPGP
- Streaming Repository Encryption
- OpenPGP and EFT
- Copy/Move File to Host Action
- Download Action
- How are Passwords Stored in EFT?