SFTP HMAC Settings and Advanced Properties

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- EFT v8.x and later

DISCUSSION

A keyed-Hash Message Authentication Code (HMAC) is used to verify data integrity and message authenticity, to confirm data has not been altered between the client and the server. EFT supports the following HMAC algorithms, which are each selected/enabled by default:

- hmac-sha2-512
- hmac-sha2-256
- hmac-sha1
- hmac-md5
- hmac-sha1-96
- hmac-md5-96

EFT provides advanced properties that affect hmac ciphers for OUTBOUND client connections:

- hmac-sha2-512 - is considered secure and enabled by default; it can be disabled for outbound client connections via Advanced Property SFTP2_SHA2_512 to false
- hmac-sha2-256 - is considered secure and enabled by default; it can be disabled for outbound client connections via Advanced Property SFTP2_SHA2_256 to false
- hmac-sha1 - is considered secure and enabled by default; it can be disabled for outbound client connection via Advanced Property SFTP2_SHA1 to false
- hmac-md5 - can be ENABLED for outbound client connections via Advanced Property SFTP2_MD5 to true
- hmac-sha1-96 - can be ENABLED for outbound client connections via SFTP2_SHA1_96 to true
- hmac-md5-96 - can be ENABLED for outbound client connections via Advanced Property SFTP2_MD5_96 to true

The ciphers hmac-md5, hmac-sha1-96, or hmac-md5-96 are *disabled* by default. An EFT file transfer will fail if it is using hmac-md5, hmac-sha1-96, or hmac-md5-96 and the advanced property for that cipher is not enabled.

SFTP HMAC Settings and Advanced Properties

Even if you disable the cipher via an advanced property, it may still be selected in the UI for *inbound* connections.

If a particular cipher is selected in the interface, both inbound and outbound connections will use that cipher, UNLESS you enable an Advanced Property that changes the behavior for OUTBOUND (EFT acting as client) connections. For the most part, the advanced property is used to turn OFF a specific cipher for outbound that is allowed for inbound; however, in some instances, due perhaps to the security risk involved, the advanced property must enable that algorithm, even if it is already enabled for inbound connections via the interface. This additional step forces administrators to take extra steps for security, and also prevents accidental enabling of a cipher for outbound connections when it was only intended for inbound connections.

Note: For logging purposes, setting the following advanced properties to **true** will improve the log performance:

EnableXferLog (enable transfer logs) and CloseFinishedItemLog (false = enabled/default. By default successful logs are removed.)

GlobalSCAPE Knowledge Base
https://kb.globalscape.com/Knowledgebase/11521/SFTP-HMAC-Settings-and-Advan...