EFT records incorrect MAC when Ciphers AES128-GMC and AES256-gmc are used

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- EFT, v8.0 - 8.0.3.x

SYMPTOM

EFT records incorrect MAC when Ciphers AES128-GMC and AES256-gmc are used

CAUSE

The ciphers aes256-gcm@openssh.com and aes128-gcm@openssh.com contain the integrity check inside itself. With OpenSSH, there no need to use any other "explicit" MAC algorithm.

MORE INFORMATION

The logs are expected to be made clear in a subsequent EFT release.

GlobalSCAPE Knowledge Base
https://kb.globalscape.com/Knowledgebase/11535/EFT-records-incorrect-MAC-wh...