Allowed MACs for HMAC-SHA2-512 and HMAC-SHA2-256 are disabled upon ugrade

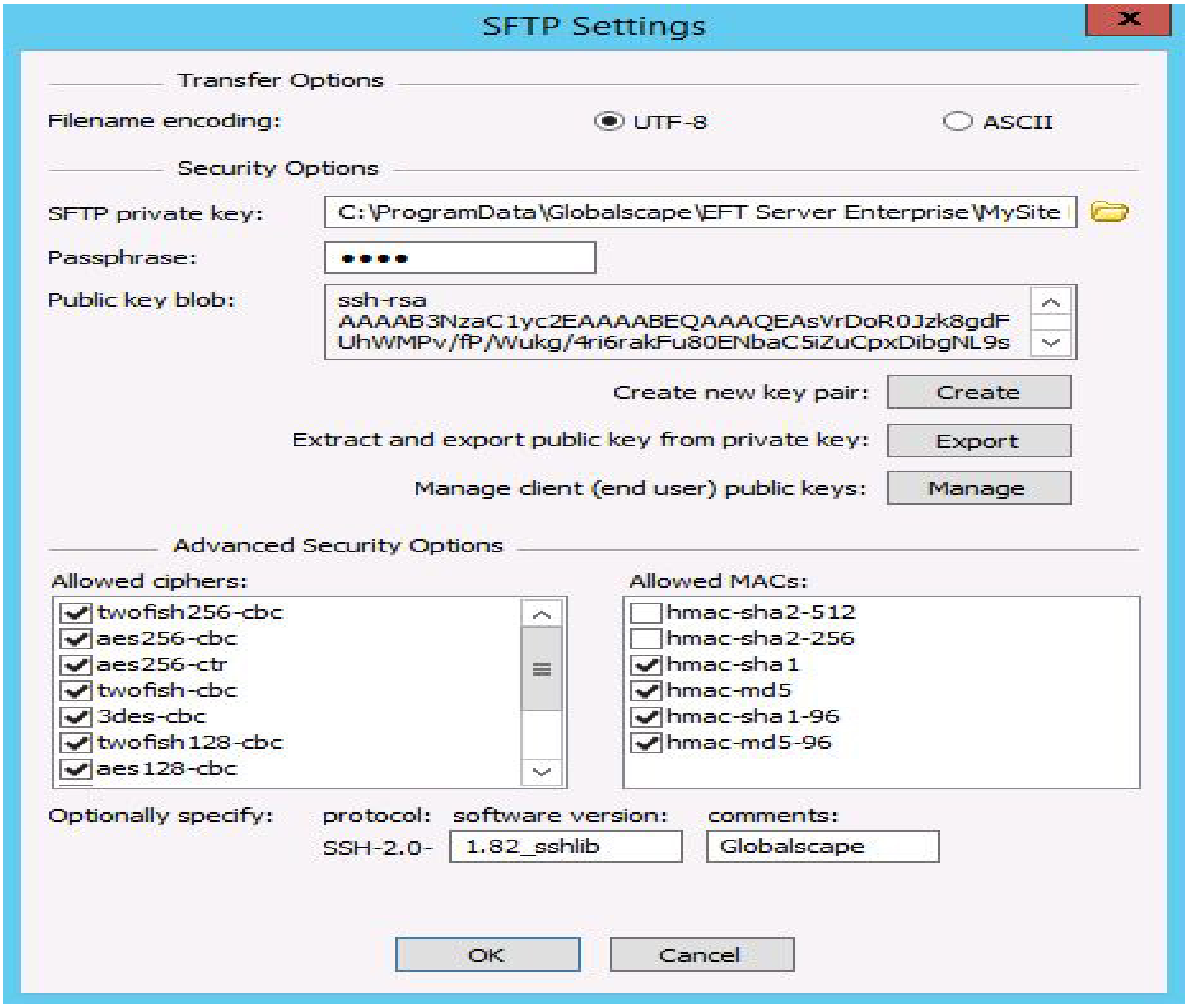
THE INFORMATION IN THIS ARTICLE APPLIES TO:

- EFT v7.2.1 and later

DISCUSSION

When EFT version 7.2.0 build is upgraded to version 7.2.1, the allowed MACs for HMAC-SHA2-512 and HMAC-SHA2-256 are disabled, while other allowed MACs are still enabled. You must enable these new ciphers if you want to use them. During new installs, these MACs are enabled by default.

Globalscape chose not to modify any existing SSH configuration during upgrade, allowing the customer to decide whether to enable them.



SFTP Settings

Transfer Options

Filename encoding: ● UTF-8 ○ ASCII

Security Options

SFTP private key: C:\ProgramData\Globalscape\EFT Server Enterprise\MySite

Passphrase: ••••

Public key blob: ssh-rsa AAAAB3NzaC1yc2EAAAABEQAAAQEAsVrDoR0Jzk8gdF UhWMPv/fP/Wukg/4ri6rakFu80ENbaC5iZuCpxDibgNL9s

Create new key pair: Create

Extract and export public key from private key: Export

Manage client (end user) public keys: Manage

Advanced Security Options

Allowed ciphers:

- ☑ twofish256-cbc
- ☑ aes256-cbc
- ☑ aes256-ctr
- ☑ twofish-cbc
- ☑ 3des-cbc
- ☑ twofish128-cbc
- ☑ aes128-cbc

Allowed MACs:

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

Optionally specify: protocol: SSH-2.0- software version: 1.82_sshlib comments: Globalscape

Allowed MACs for HMAC-SHA2-512 and HMAC-SHA2-256 are disabled upon ugrade

GlobalSCAPE Knowledge Base

https://kb.globalscape.com/Knowledgebase/11262/Allowed-MACs-for-HMACSHA2512...