# Configuring SFTP cipher/mac algorithms for EFT outbound connections in the registry

**THE INFORMATION IN THIS ARTICLE APPLIES TO:**

- EFT Enterprise v6.3 and later
- **EFT v4.x to v7.4.x** stores advanced properties in the registry.
- **EFT v8.x** stores Advanced Properties in a JSON file.

EFT v8.0 and later store Advanced Properties in a JSON file. When you upgrade from EFT v7.4.x to EFT v8, the non-default settings that you have defined in the registry will be added to the Advanced Properties file during upgrade. (Default settings become part of the EFT configuration files.) For a more on how to use advanced properties, and a spreadsheet of the advanced properties, please refer to the "Advanced Properties" topic in the help for your version of EFT.

**DISCUSSION**

EFT currently does not provide the ability to configure the SFTP cipher/mac algorithms for ***outbound*** connections in the administration interface. The Site-level SFTP configuration for the ***inbound*** protocols in the interface does not affect the outbound settings. The ability to configure algorithms for outbound connections is available via registry settings or, in V8 and later, the AdvancedProperties.json file to enable/disable the various ciphers and macs.

The SFTP registry keys are automatically created by the ClientFTP.dll. The ClientFTP.dll writes to the registry when it finishes a transfer; therefore, you should edit the settings when there are no transfers occurring so that it loads your custom settings, and then it will save your custom settings back to the registry when it finishes the transfer. (Once ClientFTP.dll writes your custom settings to the registry, it will continue to use those settings.) You may have to run an initial outbound transfer after a clean install before the keys are created, or you can create them manually. (Again, do this when there is no outbound activity to avoid overwriting your changes.)

**Prior to v8,** the advanced properties resided under: HKLM\SOFTWARE\Wow6432Node\GlobalSCAPE\TED 6\Settings\SecuritySFTP2\.

**In EFT v8 and later**, add the name:value pair to the AdvancedProperties.JSON file in EFT's \ProgramData\ directory as described in the "Advanced Properties" topic in the online help for your version of EFT.

```
{
"SFTP2_AES128": "false"
}
```

In the advancedproperties.json file, instead of 0 or 1, you must use false or true.

| Name | Type | Default | Description |
|---|---|---|---|
| SFTP2_AES128 | bool | 1/true | Setting to 1 enables the AES128 cipher algorithm. |
| SFTP2_AES128CTR | bool | 1/true | Setting to 1 enables the AES128CTR cipher algorithm. |
| SFTP2_AES128_GCM_AT_OPENSSH_COM (v8.0.4 and later) | bool | 1/true | Setting to true enables the aes128-gcm@openssh.com cipher algorithm. |
| SFTP2_AES192 (v8.0.4 and later) | bool | 1/true | Setting to true enables the aes192-cbc cipher algorithm. |
| SFTP2_AES192CTR (v8.0.4 and later) | bool | 1/true | Setting to true enables the aes192-ctr cipher algorithm. |
| SFTP2_AES256 | bool | 1/true | Setting to 1 enables the AES256 cipher algorithm. |
| SFTP2_AES256CTR | bool | 1/true | Setting to 1 enables the AES256CTR cipher algorithm. |
| SFTP2_AES256_GCM_AT_OPENSSH_COM (v8.0.4 and later) | bool | 1/true | Setting to 1 enables the aes256-gcm@openssh.com cipher algorithm. |
| SFTP2_ARCFOUR | bool | 0/false | Setting to 1 enables the |

| | | | |
|---|---|---|---|
| | | | ARCFOUR cipher algorithm. |
| SFTP2_AuthByKey | bool | 0/false | Enable ClientFTP SFTP authentication by key. |
| SFTP2_AuthByPassword | bool | 1/true | Enable ClientFTP SFTP authentication by password. |
| SFTP2_Blowfish | bool | 0/false | Setting to 1 enables the Blowfish cipher algorithm. |
| SFTP2_CAST128 | bool | 0/false | Setting to 1 enables the CAST128 cipher algorithm. |
| SFTP2_CHACHA20_POLY1305_AT_OPENSSH_COM (v8.0.4 and later) | bool | 1/true | Setting to 1 enables the chacha20-poly1305@openssh.com cipher algorithm. |
| SFTP2_HMAC_SHA1_ETM_AT_OPENSSH_COM (v8.0.4 and later) | bool | 1/true | Setting to 1 enables the hmac-sha1-etm@openssh.com algorithm. |
| SFTP2_HMAC_SHA2_256_ETM_AT_OPENSSH_COM (v8.0.4 and later) | bool | 1/true | Setting to 1 enables the hmac-sha2-256-etm@openssh.com algorithm. |
| SFTP2_HMAC_SHA2_512_ETM_AT_OPENSSH_COM (v8.0.4 and later) | bool | 1/true | Setting to 1 enables the hmac-sha2-512-etm@openssh.com algorithm. |
| SFTP2_Log | bool | 0/false | Set to 0 disables ClientFTP SFTP logging. |
| SFTP2_Log_Level | uint32_t | 9 | ClientFTP SFTP log level. 2147483647 maximum |
| SFTP2_MD5 | bool | 1/true | Setting to 0 disables the MD5 MAC algorithm. |

| | | | |
|---|---|---|---|
| SFTP2_MD5_96 | bool | 1/true | Setting to 0 disables the MD5_96 MAC algorithm. |
| SFTP2_RIJNDAEL_CBC_AT_LYSATOR_LIU_SE<br>(v8.0.4 and later) | bool | 1/true | Setting t0 1 enables the rijndael-cbc@lysator.liu.se cipher algorithm. |
| SFTP2_SHA1 | bool | 1/true | Setting to 1 enables the SHA1 MAC algorithm. |
| SFTP2_SHA1_96 | bool | 1/true | Setting to 0 disables the SHA1_96 MAC algorithm. |
| SFTP2_SHA2_256 | bool | 1/true | Setting to 1 enables the SHA2_256 MAC algorithm. |
| SFTP2_SHA2_512 | bool | 1/true | Setting to 1 enables the SHA2_512 MAC algorithm. |
| SFTP2_TripleDES | bool | 1/true | Setting to 1 enables the TripleDES cipher algorithm. |
| SFTP2_Twofish | bool | 1/true | Setting to 1 enables the Twofish cipher algorithm. |
| SFTP2_TWOFISH128 | bool | 1/true | Setting to 1 enables the TWOFISH128 cipher algorithm. |
| SFTP2_TWOFISH256 | bool | 1/true | Setting to 1 enables the TWOFISH256 cipher algorithm. |
| SFTP2_UMAC_64_AT_OPENSSH_COM<br>v8.0.4 and later) | bool | 1/true | Setting to 1 enables the umac-64@openssh.com algorithm. |
| SFTP2_UMAC_64_ETM_AT_OPENSSH_COM<br>(v8.0.4 and later) | bool | 1/true | Setting to 1 enables the umac-64-etm@openssh.com algorithm. |

| | | | |
|---|---|---|---|
| SFTP2_UseCompression | bool | 1/true | Enable ClientFTP SFTP compression. |
| SFTP2PrivateKey | string | none | ClientFTP SFTP private key. 4096 characters maximum |
| SFTP2PublicKey | string | none | ClientFTP SFTP public key. 4096 characters maximum |

.telerik-reTable-2 { border-collapse: collapse; border: solid 0px; font-family: Tahoma; } .telerik-reTable-2 tr.telerik-reTableHeaderRow-2 { border-width: 1.0pt 1.0pt 1.0pt 1.0pt; margin-top: 2pt; margin-right: 2pt; margin-bottom: 2pt; margin-left: 2pt; line-height: 115%; font-size: 9.0pt; font-family: "Calibri" , "sans-serif"; width: 119.7pt; border: solid white 1.0pt; border-bottom: solid white 1.0pt; background: #4F81BD; padding: 0in 2pt 0in 2pt; color: #FFFFFF; } .telerik-reTable-2 td.telerik-reTableHeaderFirstCol-2 { border-width: 1.0pt 1.0pt 1.0pt 1.0pt; border: solid white 1.0pt; border-bottom: solid white 1.0pt; padding: 0in 2pt 0in 2pt; } .telerik-reTable-2 td.telerik-reTableHeaderLastCol-2 { border-width: 1.0pt 1.0pt 3.0pt 1.0pt; border: solid white 1.0pt; border-bottom: solid white 3.0pt; padding: 0in 5.4pt 0in 5.4pt; } .telerik-reTable-2 td.telerik-reTableHeaderOddCol-2 { border-width: 1.0pt 1.0pt 1.0pt 1.0pt; border: solid white 1.0pt; border-bottom: solid white 1.0pt; padding: 0in 2pt 0in 2pt; } .telerik-reTable-2 td.telerik-reTableHeaderEvenCol-2 { border-width: 1.0pt 1.0pt 1.0pt 1.0pt; border: solid white 1.0pt; border-bottom: solid white 2.0pt; padding: 0in 2pt 0in 2pt; } .telerik-reTable-2 tr.telerik-reTableOddRow-2 { color: #666666; background-color: #F2F3F4; vertical-align: top; } .telerik-reTable-2 tr.telerik-reTableEvenRow-2 { color: #666666; background-color: #E7EBF7; vertical-align: top; } .telerik-reTable-2 td.telerik-reTableFirstCol-2 { margin-top: 0in; margin-right: 0in; margin-bottom: 1.0pt; margin-left: 0in; line-height: 115%; font-size: 9.0pt; font-family: "Calibri" , "sans-serif"; width: 119.7pt; border-top: none; border-left: solid white 1.0pt; border-bottom: none; border-right: solid white 1.0pt; background: #4F81BD; padding: 0in 2pt 0in 2pt; color: #FFFFFF; } .telerik-reTable-2 td.telerik-reTableLastCol-2 { padding: 0in 2pt 0in 2pt; } .telerik-reTable-2 td.telerik-reTableOddCol-2 { padding: 0in 2pt 0in 2pt; } .telerik-reTable-2 td.telerik-reTableEvenCol-2 { padding: 0in 2pt 0in 2pt; } .telerik-reTable-2 tr.telerik-reTableFooterRow-2 { color: #666666; background-color: #FFFFFF; vertical-align: top; padding: 0in 5.4pt 0in 5.4pt; } .telerik-reTable-2 td.telerik-reTableFooterFirstCol-2 { margin-top: 0in; margin-right: 0in; margin-bottom: 2.0pt; margin-left: 0in; line-height: 100%; font-size: 9.0pt; font-family: "Calibri" , "sans-serif"; width: 100% border-top: none; border-left: solid white 1.0pt; border-bottom: none; border-right: solid white 1.0pt; background: #4F81BD; padding: 0in 2pt 0in 2pt;

color: #FFFFFF; } .telerik-reTable-2 td.telerik-reTableFooterLastCol-2 { padding: 0in 2pt 0in 2pt; } .telerik-reTable-2 td.telerik-reTableFooterOddCol-2 { padding: 0in 2pt 0in 2pt; } .telerik-reTable-2 td.telerik-reTableFooterEvenCol-2 { padding: 0in 2pt 0in 2pt; } **The following snippet from the ClientFTP log file shows the output when only SFTP2_TWOFISH128 and SFTP2_MD5_96 are enabled:**

```
STATUS:> Host key match found in certificate database -- accepted.

STATUS:> First key exchange completed

Negotiated algorithms:

kex alg: diffie-hellman-group14-sha1

host key alg: ssh-rsa

c2s encr alg: twofish128-cbc

s2c encr alg: twofish128-cbc

c2s mac alg: hmac-md5-96

s2c mac alg: hmac-md5-96
```

GlobalSCAPE Knowledge Base
https://kb.globalscape.com/Knowledgebase/11092/Configuring-SFTP-ciphermac-a...