Enabling FIPS-Compliant Mode for the OpenPGP Module

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- EFT version 7 and later

DISCUSSION

Some organizations require that file transfers are restricted to FIPS-compliant algorithms. The library used by our OpenPGP module is not restricted to only FIPS-compliant cryptography. However, you can add a registry setting to EFT to restricts the OpenPGP module to use only FIPS-compliant cryptography that is available in the library.

The registry setting described below, when present and the DWORD value is set to non-zero, will configure the OpenPGP library to use FIPS-compliant cryptography only.

To enable FIPS-compliant mode for the OpenPGP module

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\GlobalSCAPE Inc.\EFT Server 4.0\Config\]

DWORD: `OpenPGPFIPSCompliantAlgorithmsOnly`

- 0 = not FIPS only
- 1 = FIPS-compliant cryptography only
- Default when not specified = 0 (not FIPS-only cryptography)

The table below lists the algorithms available for each mode.

FIPS compliant mode	**Non-FIPS mode**
=Symmetric Encryption Algorithms=	**=Symmetric Encryption Algorithms=**
3DES (192-bit key)	3DES (192-bit key)
AES256 (256-bit key)	CAST5 (128-bit key)
AES192 (192-bit key)	AES256 (256-bit key)
AES128 (128-bit key)	AES192 (192-bit key)

	AES128 (128-bit key) BLOWFISH (128-bit key, 16 rounds) TWOFISH (256-bit key) IDEA (128-bit key)
=Hash Algorithms= SHA1 SHA256 SHA384 SHA512 SHA224	**=Hash Algorithms=** SHA1 MD5 SHA256 SHA384 SHA512 SHA224 RIPEMD160
=Asymmetric Algorithms= RSA (512-bit ~ 4096-bit key) DSA (512-bit ~ 4096-bit key, Sign-Only)	**=Asymmetric Algorithms=** RSA (512-bit ~ 4096-bit key) DSA (512-bit ~ 4096-bit key, Sign-Only) Elgamal (512-bit ~ 4096-bit key, Encrypt-Only)
=Compression Algorithms= zip (RFC1951) zlib (RFC1950) bzip2 (BZ2) none	**=Compression Algorithms=** zip (RFC1951) zlib (RFC1950) bzip2 (BZ2) none

.telerik-reTable-3 { border-collapse: collapse; border: solid 0px; font-family: Tahoma; }
.telerik-reTable-3 tr.telerik-reTableHeaderRow-3 { margin: 10px; padding: 10px; color: #3a4663; text-align: left; font-size: 10pt; font-style: normal; font-family: Verdana; text-transform: capitalize; font-weight: normal; border-spacing: 10px; vertical-align: top;

background-color: #C4D1E3; } .telerik-reTable-3 td.telerik-reTableHeaderFirstCol-3 { padding: 0in 5.4pt 0in 5.4pt; color: #3a4663; line-height: 14pt; } .telerik-reTable-3 td.telerik-reTableHeaderLastCol-3 { padding: 0in 5.4pt 0in 5.4pt; color: #3a4663; line-height: 14pt; } .telerik-reTable-3 td.telerik-reTableHeaderOddCol-3 { padding: 0in 5.4pt 0in 5.4pt; color: #3a4663; line-height: 14pt; } .telerik-reTable-3 td.telerik-reTableHeaderEvenCol-3 { padding: 0in 5.4pt 0in 5.4pt; color: #3a4663; line-height: 14pt; } .telerik-reTable-3 tr.telerik-reTableOddRow-3 { color: #666666; vertical-align: top; font-size: 10pt; } .telerik-reTable-3 tr.telerik-reTableEvenRow-3 { color: #666666; vertical-align: top; font-size: 10pt; } .telerik-reTable-3 td.telerik-reTableFirstCol-3 { padding: 0in 5.4pt 0in 5.4pt; background-color: #E7EBF7; } .telerik-reTable-3 td.telerik-reTableLastCol-3 { padding: 0in 5.4pt 0in 5.4pt; background-color: #E7EBF7; } .telerik-reTable-3 td.telerik-reTableOddCol-3 { padding: 0in 5.4pt 0in 5.4pt; background-color: #F7F3F7; } .telerik-reTable-3 td.telerik-reTableEvenCol-3 { padding: 0in 5.4pt 0in 5.4pt; background-color: #E7EBF7; } .telerik-reTable-3 tr.telerik-reTableFooterRow-3 { background-color: #C4D1E3; color: #3a4663; font-weight: normal; font-size: 10pt; font-family: Verdana; line-height: 11pt; } .telerik-reTable-3 td.telerik-reTableFooterFirstCol-3 { padding: 0in 5.4pt 0in 5.4pt; text-align: left; } .telerik-reTable-3 td.telerik-reTableFooterLastCol-3 { padding: 0in 5.4pt 0in 5.4pt; text-align: left; } .telerik-reTable-3 td.telerik-reTableFooterOddCol-3 { padding: 0in 5.4pt 0in 5.4pt; text-align: left; } .telerik-reTable-3 td.telerik-reTableFooterEvenCol-3 { padding: 0in 5.4pt 0in 5.4pt; text-align: left; }

GlobalSCAPE Knowledge Base
https://kb.globalscape.com/Knowledgebase/11172/Enabling-FIPSCompliant-Mode-...