TLS Resumption Compatibility, "Failed to establish data socket"

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- EFT, v7.0 and later

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.

SYMPTOM

When connecting to a TLS resumption-enabled server from EFT, it is common that you will encounter an SSL error shortly after attempting to establish the data socket with the remote server. The below error is typically what you'll see in the logs in the event that the connection fails due to these reasons.

Note: TLS resumption is commonly used by Filezilla Server and is enabled by default.

```
COMMAND:>    PASV

          227 Entering Passive Mode (13,67,183,127,113,82)

COMMAND:>    REST 0

          350 Rest supported. Restarting at 0

COMMAND:>    STOR Log145416.txt.pgp

STATUS:>     Host name 13.67.183.127 resolved: ip = 13.67.183.127.

STATUS:>     Connecting FTP data socket 13.67.183.127:29010 (ip = 13.67.183.127)...

          150 Opening data channel for file upload to server of "/Log145416.txt.pgp"
```

TLS Resumption Compatibility, "Failed to establish data socket"

```
STATUS:>     Connected. Exchanging encryption keys...

ERROR:>     SSL: Error in negotiating SSL connection. The server could be rejecting your
certificate.

ERROR:>     Failed to establish data socket.
```

WORKAROUND

After my investigation of potential ways to remediate this behavior, I found that there was a registry key to enable TLS Resumption compatibility called "ReuseSSLData." After stopping the service, enabling this advanced property (registry key), and restarting the service; this should resolve your issue.

Enable Compatibility with TLS Resumption on FZ Server:

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.

```
{
"ReuseSSLData": true
}
```

In versions prior to v8, add the DWORD value to the registry:

Name: ReuseSSLData

Key: HKLM\SOFTWARE\Wow6432Node\Globalscape\TED 6\Settings\SecuritySSL

Type: DWORD

Set ReuseSSLData value to "1" to enable "TLS resumption"-compatibility mode in EFT (requires service restart).

MORE INFORMATION

What is TLS Resumption?

https://hpbn.co/transport-layer-security-tls/

https://tools.ietf.org/html/rfc5077

https://vincent.bernat.im/en/blog/2011-ssl-session-reuse-rfc5077.html

GlobalSCAPE Knowledge Base
https://kb.globalscape.com/Knowledgebase/11327/TLS-Resumption-Compatibility...