AS2 Signature and Encryption Algorithms for Inbound Transactions

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- EFT v7.4.11 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.

DISCUSSION

EFT v7.4.11 was updated to use the /n 2016 EDI Integrator component, which includes the option to specify allowed signature/ encryption algorithms for inbound transactions. The MDN (Message Disposition Notification) is signed using the specified algorithm. Which algorithms to use can be configured in the registry, as described below.

Available signature algorithms for inbound transactions include:

- 0 As Requested
- 1 As Requested Or SHA1
- 2 SHA1
- 3 MD5
- 4 None
- 5 SHA-256
- 6 SHA-384
- 7 SHA-512
- 8 SHA-224
- 9 As Requested Or SHA-256 (default)

Available encryption algorithms include:

- 3DES
- DES
- AESCBC128
- AESCBC192

- AESCBC256

All available algorithms except "DES" are selected by default.

To specify one or more algorithms

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.

```
{
"AS2EncryptionAlgorithm": "AESCBC256",
"AS2SignatureAlgorightm": "SHA-256"
}
```

In versions prior to v8.0:

Create the following registry settings:

HKEY_LOCAL_MACHINE\Software\WOW6432Node\GlobalSCAPE Inc.\EFT Server 7.4\

Type: STRING

Value names:

- AS2EncryptionAlgorithm
- AS2SignatureAlgorithm

Restart Required: yes

Backup/Restore: yes

In the COM API, these options are configurable via the COM API properties "Signature

Algorithm" and "Encryption Algorithm".

GlobalSCAPE Knowledge Base
https://kb.globalscape.com/Knowledgebase/11432/AS2-Signature-and-Encryption...