



**Enterprise Message Transmission System
SFTP User Guide**

Table of Contents

1	<i>Overview</i>	3
•	<i>Purpose</i>	3
•	<i>Requirements</i>	3
2	<i>Trading Partner Receiving Files via SFTP Push (Direct Connection)</i>	4
•	<i>System Access</i>	4
•	<i>SSH Key Sharing</i>	4
•	<i>Host information</i>	4
•	<i>Supported Ciphers</i>	4
•	<i>Preferred MAC (Message Authentication Code)</i>	4
•	<i>Outbound EDI / Non-EDI Files (SFTP Push)</i>	5
3	<i>Trading Partner Downloading Files via SFTP Pull (Mailbox)</i>	6
•	<i>System Access</i>	6
•	<i>SSH Key Sharing</i>	6
•	<i>Mailbox Structure</i>	7
•	<i>Sample SFTP Session</i>	7
•	<i>Downloading EDI/Non-EDI Files (SFTP Mailbox)</i>	8
4	<i>Trading Partner Uploading Files via SFTP (Direct Connect or Mailbox)</i>	9
•	<i>System Access</i>	9
•	<i>Mailbox Structure</i>	9
•	<i>Sample SFTP Session</i>	10
•	<i>Uploading EDI/Non-EDI Files</i>	11
5	<i>Performing A Loopback Test</i>	12
•	<i>Example</i>	12
•	<i>Expected Results</i>	12
6	<i>Retry Handling - Undeliverable Files (Trading Partner – Push Only)</i>	13
	<i>Appendix A – Inbound File Name Requirements</i>	14
	<i>Appendix B – Default Outbound Filename Standards</i>	15
	<i>Appendix C – EDI Transaction to Inbound Directory Cross Reference</i>	17
	<i>Appendix D – Client Software Settings</i>	18
•	<i>OpenSSH version 8.8 or higher</i>	18

• Cleo Software _____	19
• WinSCP _____	20
<i>Appendix E – Generating SSH Keys</i> _____	22
<i>Appendix – Documentation Version Control</i> _____	24

1 Overview

- **Purpose**

This document will provide information for a Trading Partner (TP) to send and receive files to and from the Enterprise Message Transmission System (EMTS) using SFTP over the Internet.

- **Requirements**

The requirements assume that the Trading Partner has the necessary software to create and send files over the Internet. To send and retrieve files you will need following:

- Access to the Internet.
- Standards-based SFTP Client or Commercial software specifically developed to support EMTS.
- Password authentication is not allowed.
- Host based authentication is not allowed.
- Support Version 2 SSH and Version 3 SFTP protocol; SSH-1 is not supported.
- The preferred cipher is AES256-cbc.
- The preferred MAC is hmac-sha1.
- Limit Invalid login attempts to 6 (users are locked out if they exceed the limit)
 - **If your account becomes locked, you must disable your processing for 5 minutes so that the system can unlock your account.**
- Limit concurrent logins for each user to 5
- For SFTP Mailbox Users, consider the following when setting your polling interval.
 - **Under no circumstances should your polling interval be more than every 3 minutes**
 - Depending on the type of Supplier you are sending/receiving, you must follow these rules:

Supplier Type	Polling Interval
Production Supplier (CHASE) / Transportation (STARS or OBT)	3 minutes
Non-production supplier	10 minutes
EFID (Electronic Fiscal Documents acknowledgments)	20 minutes
Proprietary – > than 20 files per day	10 minutes
Proprietary – < than 20 files per day	30 minutes

2 Trading Partner Receiving Files via SFTP Push (Direct Connection)

- **System Access**

If your system is connected to a firewall, you are required to allow EMTS access through the firewall. Because all firewall software configurations are different, the Trading Partner must contact their firewall support staff to determine the proper configuration. The SFTP server on EMTS will use port 22 to receive connections.

- **SSH Key Sharing**

You are required to add the EMTS Public key (provided to you by EMTS on-boarding support) to the account you created to allow EMTS access your SFTP Server. Generally, the public keys are added to an “authorized key file” associated to the account you have created for access. Depending on your software, this can take many forms. We suggest you contact your IT support with any questions on setting up the SFTP Account/Authorized Key File.

Steps to share Keys:

1. EMTS sends public key to Trading Partner.
2. Trading Partner stores public key.
3. Trading Partner generates public/private key pairs.
4. Trading Partner sends public key to EMTS.
5. EMTS stores Trading Partner public Key.
6. Trading Partner initiates a session with EMTS to accept the host key.
7. EMTS initiates a session with TP to accept the host key.

- **Host information**

For EMTS to send data via SFTP, EMTS requires the following details from the Trading Partner’s system to push files.

- DNS Hostname or IP address
- Port Number – Preferably Standard SFTP/SSH port 22
- User ID
 - You are required to add the EMTS Public Key to this User ID. Your software will dictate how this must be accomplished.
- SSH Host Key – Can be manually acquired when setting up the connection.
- Directory – **EMTS requires that the Trading Partner provides a single directory to store files.**

- **Supported Ciphers**

- blowfish-cbc
- aes256-cbc
- aes192-cbc
- aes128-cbc
- aes128-ctr
- aes192-ctr
- aes256-ctr

Note: The preferred cipher is AES256-cbc

- **Preferred MAC (Message Authentication Code)**

- hmac-sha1
- hmac-md5
- hmac-sha2-256
- hmac-sha1-96 (V5.2.5_15 or later)
- hmac-md5-96 (V5.2.5_15 or later)

Note: The preferred MAC is hmac-sha1

- **Outbound EDI / Non-EDI Files (SFTP Push)**

See **Appendix B** for Outbound Filename formats.

Application/File Type	Trading Partner must provide
CHASE-ASN/ASC (EDI 824) Responses	<Trading Partner Specific> See note 1.
STARS (EDI 824) Responses	
Outbound batch EDI	
OBT (VICS/VISTA) EDI	
Modular Supplier (MS) EDI	
EFID/CFD XML Invoices	
All other Outbound Non-EDI / Proprietary files	<Trading Partner Specific> See note 2.

1. For EDI files, EMTS requires one directory/location per EMTS Account.
2. A Trading Partner may separate Non-EDI/Proprietary from EDI files, however EMTS requires consolidating all of these into one directory/location.

3 Trading Partner Downloading Files via SFTP Pull (Mailbox)

- **System Access**

In general, the Trading Partner will connect using a standard SFTP client or commercially developed software that support EMTS and “pull” files from an EMTS mailbox. The Trading Partner needs to programmatically connect and extract files from the mailbox.

Considerations:

- Support Version 2 SSH and Version 3 SFTP protocol.
- The preferred cipher is AES256-cbc.
- The preferred MAC is hmac-sha1.
- Limit Invalid login attempts to 6 (users are locked out if they exceed the limit).
- Limit concurrent logins for each user to 5.
- **NOTE: Limit your polling intervals to one connection every 3 minutes. Any interval that is less than 1 every 3 minutes may require EMTS support to lock your ID preventing from sending or receiving data.**

- **SSH Key Sharing**

You are required to generate an SSH key pair (Public/Private). There are many tools available for SSH key generation, such as PuttyGen (free utility). Appendix E provides an example of generating an RSA key pair. Once you have generated the SSH Key Pair, you will provide the Public Key to EMTS on-boarding support. They will add the Public Key to your EMTS account and at that time you may validate connectivity by initiating a session. This process is dependent on your software package.

Steps to share Keys:

1. Trading Partner generates public/private key pairs.
2. Trading Partner sends public key to EMTS.
3. EMTS stores Trading Partner public Key.
4. Trading Partner initiates a session with EMTS to accept the host key.

Note: If you are originating traffic from multiple hosts using the same user id, you are required to:

1. Duplicate the RSA/DSA keys to each of your hosts.
or
2. Generate and send EMTS Support each of the RSA/DSA public keys.

- **Mailbox Structure**

EMTS uses a Directory structure for file processing. The Trading Partner will see the following directory structure when logging in:

```
/archive (not currently used)
/Inbox
/Outbox
```

- All inbound files (Trading Partner -> EMTS) will be uploaded in a specific directory located under the **/Inbox** directory.
- All Supplier Related files (EMTS -> Trading Partner) are located in a specific directory located under the **/Outbox** directory.
- See **Section 4.5** for a list of directories where your files must be uploaded.
- See **Appendix A** for information regarding Trading Partner generated file naming requirements.
- See **Appendix B** for information regarding EMTS generated file naming standards.

- **Sample SFTP Session**

Text in bold is user supplied commands.

```
sftp EMTSUSER@ems-test.intra.chrysler.com
Connecting to ems-test.intra.chrysler.com...
You are accessing FCA (Fiat Chrysler Automobiles) systems - EMTS SFTP Server S2.

Access to FCA's computer systems is controlled.

FCA authorizes use for its business purposes only.

Unauthorized access is prohibited due to risk of irreparable harm to FCA.

FCA management may monitor use to ensure compliance with its policies.

FCA may terminate access privileges, take disciplinary action and/or institute civil or criminal
proceedings to enforce this policy.

If any part of this policy is unacceptable to you, please disconnect now!!!
sftp> cd /Outbox/EDI
sftp> mget *
Fetching /Outbox/EDI/DCXASR.file1 to DCXASR.file1
/Outbox/EDI/DCXASR.file1                                100% 692      0.7KB/s   00:00
Fetching /Outbox/EDI/DCXASR.file2 to DCXASR.file2
/Outbox/EDI/DCXASR.file2                                100% 943      0.9KB/s   00:00
Fetching /Outbox/EDI/DCXASR.file3 to DCXASR.file3
/Outbox/EDI/DCXASR.file3                                100% 3989    3.9KB/s   00:00
sftp> bye
```

- **Downloading EDI/Non-EDI Files (SFTP Mailbox)**

Use the mailboxes below to download files from EMTS: (See **Appendix B** for *Outbound Filename formats*)

Application/File Type	Directory Structure
CHASE-ASN/ASC (EDI 824) Responses	/Outbox/EDI
STARS (EDI 824) Responses	/Outbox/EDI
Outbound batch EDI	/Outbox/EDI
OBT (ASN, Plant Hold, Carrier Activity)	/Outbox/OBT/EDIVD
OBT (VISTA)	/Outbox/OBT/EDIVT
OBT (VICS)	/Outbox/OBT/EDIVI
Modular Supplier (MS) EDI	/Outbox/MS/MSEDIX12
EFID/CFD XML Invoices	/Outbox/NONEDI/EFIDACKC
All other Outbound Non-EDI / Proprietary files	/Outbox/NONEDI/<MESSAGETYPE> See note 1

1. EMTS support will provide you with the MESSAGETYPE parameters at the time of onboarding your account.

4 Trading Partner Uploading Files via SFTP (Direct Connect or Mailbox)

- **System Access**

In general, the Trading Partner will connect using a standard SFTP client or Commercially developed software that supports EMTS and “put” the file to the EMTS system.

EMTS provides one SFTP ID for each Trading Partner. Only in very specific and approved configurations will a Trading Partner be allowed to have additional SFTP IDs. When the Trading Partner is uploading files to EMTS, the files are routed using two methods; Content and Directory/File.

Content Based Routing

All EDI is routed by specific values contained in the file, for instance the ISA record in the ASN 856. The following Directories perform Content Based Routing:

```
/Inbox/EDI  
/Inbox/EDI/CHASE  
/Inbox/EDI/STARS
```

Directory/File Based Routing

The remaining types of data, such as Outbound Transportation (OBT), Modular Suppliers, and Proprietary files are routed based on a specific directory or file name format. See **Section 4.4** and **Appendix A** for additional details.

- **Mailbox Structure**

EMTS uses a Directory structure for file processing. The Trading Partner will see the following directory structure when logging in:

```
/archive (not currently used)  
/Inbox  
/Outbox
```

- All inbound files (Trading Partner -> EMTS) will be uploaded in a specific directory located under the **/Inbox** directory. See **Section 4.4** for a list of directories where your files must be uploaded.
- See **Appendix A** for information regarding Trading Partner generated file naming requirements.
- See **Appendix B** for information regarding EMTS generated file naming standards.

- **Sample SFTP Session**

Text in bold are user supplied commands/responses.

```
sftp EMTSUSER@emts-test.intra.chrysler.com
Connecting to emts-test.intra.chrysler.com...
You are accessing FCA (Fiat Chrysler Automobiles) systems - EMTS SFTP Server S2.

Access to FCA's computer systems is controlled.

FCA authorizes use for its business purposes only.

Unauthorized access is prohibited due to risk of irreparable harm to FCA.

FCA management may monitor use to ensure compliance with its policies.

FCA may terminate access privileges, take disciplinary action and/or institute civil or criminal
proceedings to enforce this policy.

If any part of this policy is unacceptable to you, please disconnect now!!!
sftp> cd /Inbox/EDI
sftp> put EDI.txt
Uploading EDI.txt to /Inbox/EDI/EDI.txt
EDI.txt                               100% 2018      2.0KB/s   00:00
sftp> dir
<Once the file has completely uploaded, the system will take ownership and process the file, the
file is no longer visible.>
sftp> bye
```

- **Uploading EDI/Non-EDI Files**

See **Appendix A** for Inbound Filename Requirements.

Application/File Type	Directory Structure (mailbox)
CHASE-ASN/ASC (EDI 856)	/Inbox/EDI/CHASE (see note 1 & 2)
STARS (EDI 214)	/Inbox/EDI/STARS
Inbound batch EDI	/Inbox/EDI
OBT (VICS/VISTA) EDI	/Inbox/OBT/EDI
OBT 2V/3R In/Out Gate (VISTAG)	/Inbox/OBT/2V3R
Modular Supplier (MS) EDI	/Inbox/MS/MSEDIX12 (see note 3)
EFID/CFD XML Invoices	/Inbox/NONEDI/EFID9086/EFIDINVS
All other inbound Non-EDI / Proprietary files	/Inbox/NONEDI/<CONSUMERID>/<MESSAGETYPE> (see note 4)

1. For Freight Consolidators sending in ASCs element ISA08 should be 04000FC. This instructs the CHASE system to process the 856 as an ASC rather than as an ASN.
2. EMTS will not process ASN/ASC transactions larger than 400k. If ASN/ASC's are larger than, they will need to be separated into multiple submissions smaller than 400k. The following error message will be returned: "FILE NOT PROCESSED. MAX FILE SIZE 400K LIMIT EXCEEDED".
3. There are no specific requirements outside of the EMTS Standard Inbound File Name Requirements (See Appendix A). EMTS will route the files based on the ISA information. ISA should have MS1 and MS2 sender and receiver ID.

Example: *ISA*00* *00* *ZZ*MS259962 *ZZ*MS158145 *211007*1035*U*

4. EMTS support will provide you with the CONSUMERID and MESSAGETYPE parameters at the time of onboarding your account.
5. See Appendix C for the EDI Transaction to Inbound Directory cross reference.

5 Performing A Loopback Test

This initial test will be completed by the Trading Partner to test network configuration and access.

For Mailbox (PULL) – The Trading Partner will upload a file to /Inbox/LOOPTEST and the system will route the file to /Outbox/LOOPTEST.

For Direct Connection (PUSH) – The Trading Partner will upload a file to /Inbox/LOOPTEST and the system will route the file to the destination directory on the Trading Partners SFTP Server.

- **Example**

Trading Partner initiates an SFTP session to EMTS:

```
cd /Inbox/LOOPTEST
```

Transfers a file:

```
put <filename>
```

At this time, within ~1 minute the file is processed and delivered to the requested destination.

- **Expected Results**

A successful loopback test will result in one of the following:

- If the Trading Partner is configured as SFTP pull (mailbox), an automated process will place the file back in the source mailbox: **/Outbox/LOOPTEST**
- If the Trading Partner is configured as SFTP push, the same file will be delivered back to the Trading Partner's server in the directory specified by the Trading Partner.

6 Retry Handling - Undeliverable Files (Trading Partner – Push Only)

EMTS will attempt to send (push) any file to a Trading Partner using SFTP as soon as EMTS receives the file from the source application.

SFTP push assumes that the Trading Partner's SFTP server will be up and running on a 7 x 24 x 365 basis. Recognizing that this cannot always be the case, EMTS has implemented a simple retry strategy where as EMTS will attempt to connect three (3) times at an interval of 15 seconds for a total of 60 seconds.

Appendix A – Inbound File Name Requirements

The following rules should be adhered to when creating file names:

- All filenames must be unique.
- Valid file names should consist of upper and lower case alphabetic characters, numbers, underscores and periods.
- **Embedded spaces** or **dashes/hyphens** are not allowed.
- Special characters (/ \ & @ , | etc) are not allowed.
- File name length should be no more than 100 characters.

Appendix B – Default Outbound Filename Standards

Default Filename format for Proprietary/Non-EDI Files

Note: For the exact naming of proprietary files, EMTS Support will provide filename format during the on-boarding process.

Format 1: <SourceFileName>_<YYYYMMDDHHmmSSsss>

Where:

SourceFileName – Filename that the source system uses when depositing the file to EMTS.

YYYYMMDDHHmmSSsss – System Generated timestamp

Example: *testfile.txt* will be sent as ***testfile.txt_20170901142111920***

Format 2: P_<ApplicationJobName>_EMTSDATA_<EMTSMessageType>_< YYYYMMDDHHmmSSsss>

Where:

ApplicationJobName – An internal name used in tracking message delivery (Internal Use Only)

EMTSDATA – Eye Catcher

EMTSMessageType – This describes the content of the data

YYYYMMDDHHmmSSsss – System Generated timestamp

Example: P_ASFU550Z_EMTSDATA_AIOBCPYTOLS_20191014140043760

Default Filename format for EDI Files

Format: EDI_<Translation Map>_<SupplierCode>_<Doctype>_<YYYYMMDDHHmmSSsss>_<Process ID#>

Where:

EDI – File prefix to denote EDI file type (Constant).

Translation Map - Internal Information (Internal Use Only)

SupplierCode – FCA US Assigned Supplier Code

Doctype – EBMX Doctype - Optional

YYYYMMDDHHmmSSsss – System Generated timestamp

Process ID# - EMTS Business Process number, used for troubleshooting.

Example 1: EDI_850DIA_12345_DCXAAC_20170918100311311_67893024

Example 2: EDI_862KAN_47277_DCXKNV3_201802131524142414_76234561

Example 3: EDI_824PHX_62891Z_201802131524142414_83756375

Format: EDI_997-<Transaction>_<YYYYMMDDHHmmSSsss>_<Process ID#>

Where:

EDI – File prefix to denote EDI file type (Constant).

Transaction – 856, 858, 210, etc.

YYYYMMDDHHmmSSsss – System Generated timestamp

Process ID# - EMTS Business Process number, used for troubleshooting.

Example 1: EDI_997-210_12345_20200918100311311_56712398

Example 2: EDI_997-856_98765A_20200918100311311_81361385

Default Filename format for Outbound Transportation (OBT) Files

Format: OBT_<nnnnnnn>_<ST Transaction>_<ICS Receiver>

Where:

nnnnnnn – sequence number

ST Transaction – ANSI X12 Document Type

ICS Receiver – FCA US Assigned Carrier Code

Example 1: OBT_4700776_610_12345

Example 2: OBT_4700777_660_12345

Filename format for outbound Modular Supplier (MS) EDI filenames:

<MS1>_<MS2>_MSEDIX12_<datetimestamp or filename>

Example: MS199999_MS212345A_MSEDIX12_2019073010530000

Appendix C – EDI Transaction to Inbound Directory Cross Reference

Transaction	Directory
214	/Inbox/EDI/STARS
856	/Inbox/EDI/CHASE
210	/Inbox/EDI/
410	/Inbox/EDI/
417	/Inbox/EDI/
810	/Inbox/EDI/
820	/Inbox/EDI/
822	/Inbox/EDI/
824	/Inbox/EDI/
830	/Inbox/EDI/
846	/Inbox/EDI/
850	/Inbox/EDI/
855	/Inbox/EDI/
858	/Inbox/EDI/
860	/Inbox/EDI/
861	/Inbox/EDI/
862	/Inbox/EDI/
863	/Inbox/EDI/
864	/Inbox/EDI/
870	/Inbox/EDI/
928	/Inbox/EDI/
996	/Inbox/EDI/
997	Do not Send
127	/Inbox/OBT/EDI
510	/Inbox/OBT/EDI
520	/Inbox/OBT/EDI
530	/Inbox/OBT/EDI
540	/Inbox/OBT/EDI
550	/Inbox/OBT/EDI
838	/Inbox/OBT/EDI
853	/Inbox/OBT/EDI
980	/Inbox/OBT/EDI
RA2VE	/Inbox/OBT/2V3R
RA2VR	/Inbox/OBT/2V3R

Appendix D – Client Software Settings

- **OpenSSH version 8.8 or higher**

When using OpenSSH version 8.8 or higher we have found some users are having issues connecting to EMTS using the OpenSSH SFTP Client and receiving “Permission Denied” or prompted to enter a password. If you experience this type of error/issue, please add the following option to your SFTP command.

```
-o PubKeyAcceptedAlgorithms=+ssh-rsa
```

Example:

```
sftp -o PubKeyAcceptedAlgorithms=+ssh-rsa TEST@ems-test.intra.chrysler.com
```

How to determine which OpenSSH Version you are using; multiple examples.

```
[server 1 ~]$ ssh -V  
OpenSSH_8.0p1, OpenSSL 1.1.1g FIPS 21 Apr 2020
```

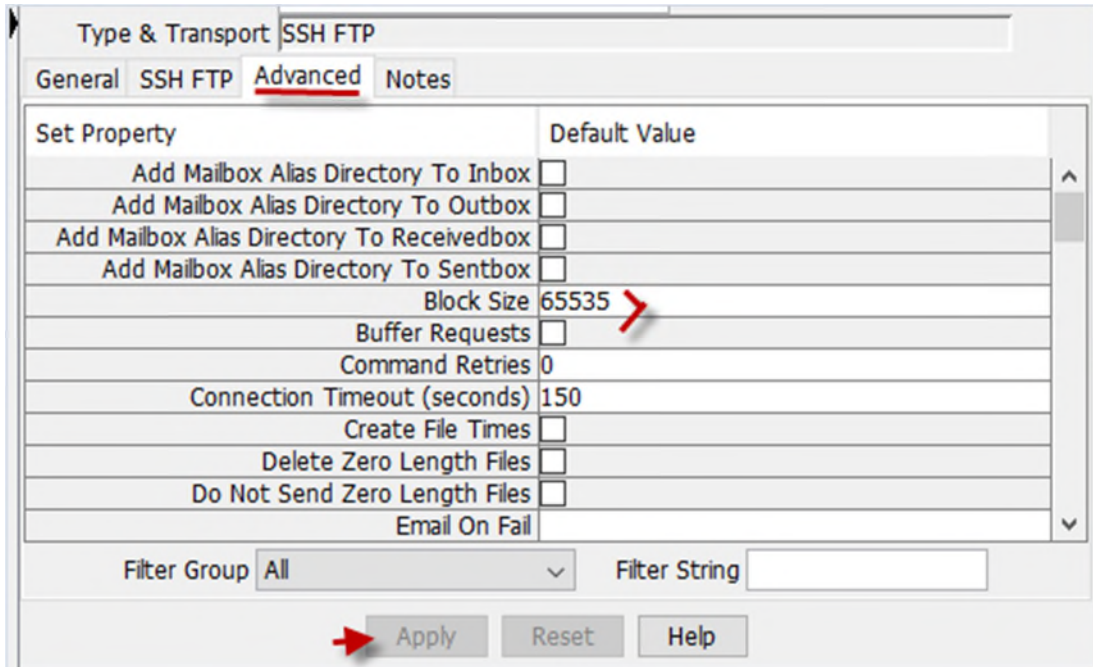
```
raspberrypi:~$ ssh -V  
OpenSSH_8.9p1 Ubuntu-3ubuntu0.6, OpenSSL 3.0.2 15 Mar 2022
```

- **Cleo Software**

Java.io.IOException: The Message [/Outbox/LOOPTEST/<filename>] is not extractable! Error code: 4

To correct this error, go to the Advanced tab in the Type & Transport settings and clear the check box

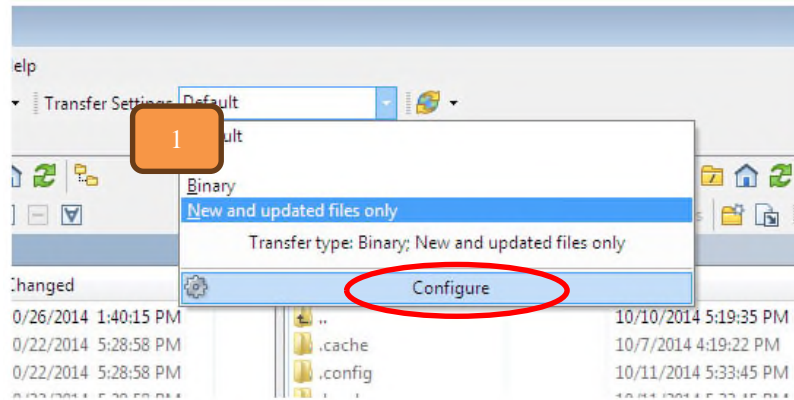
Buffer Requests



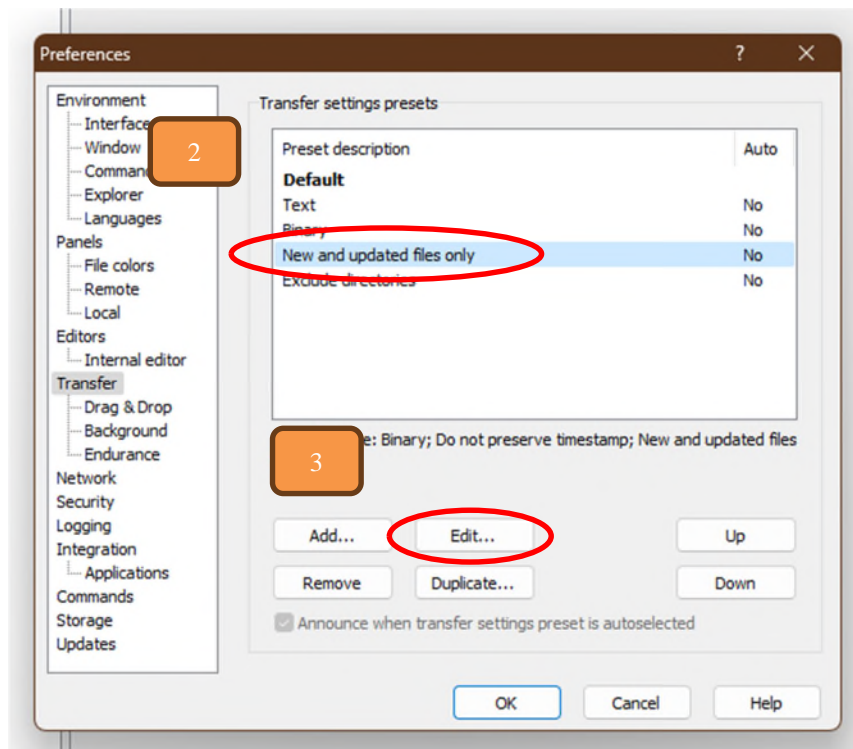
- **WinSCP**

By default, WinSCP will try to update the timestamp to that of the local files, this causes the "Permission Denied" Error. To correct this, disable the **Preserve Timestamp** option on the Transfer Settings.

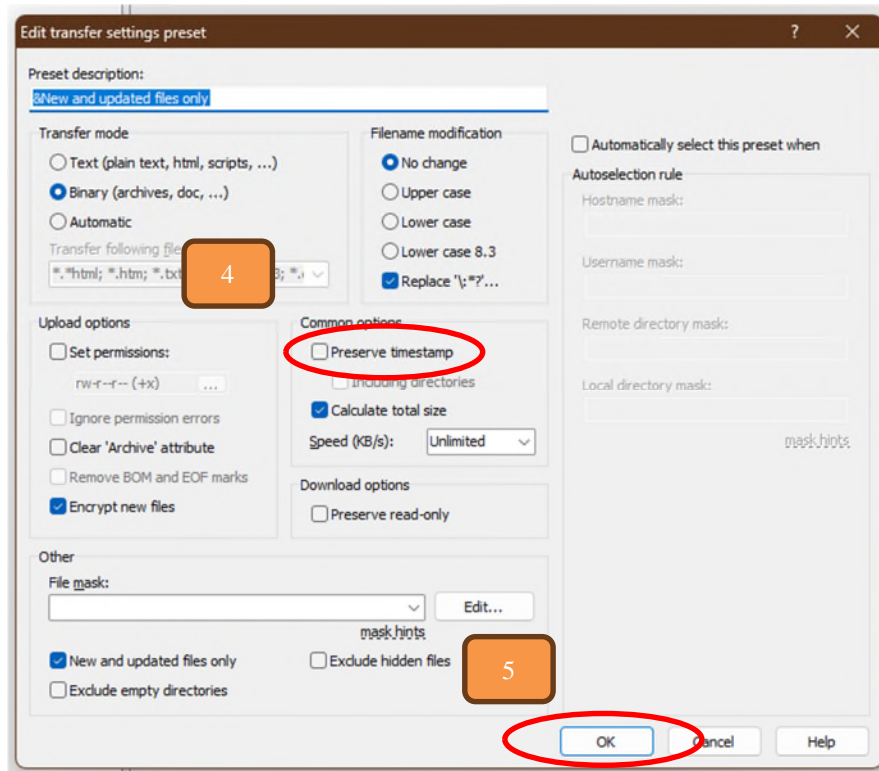
1. Open the Transfer Settings dialog and select **"Configure"**



2. Select **"New and updated files only"**
3. Click **"Edit..."**



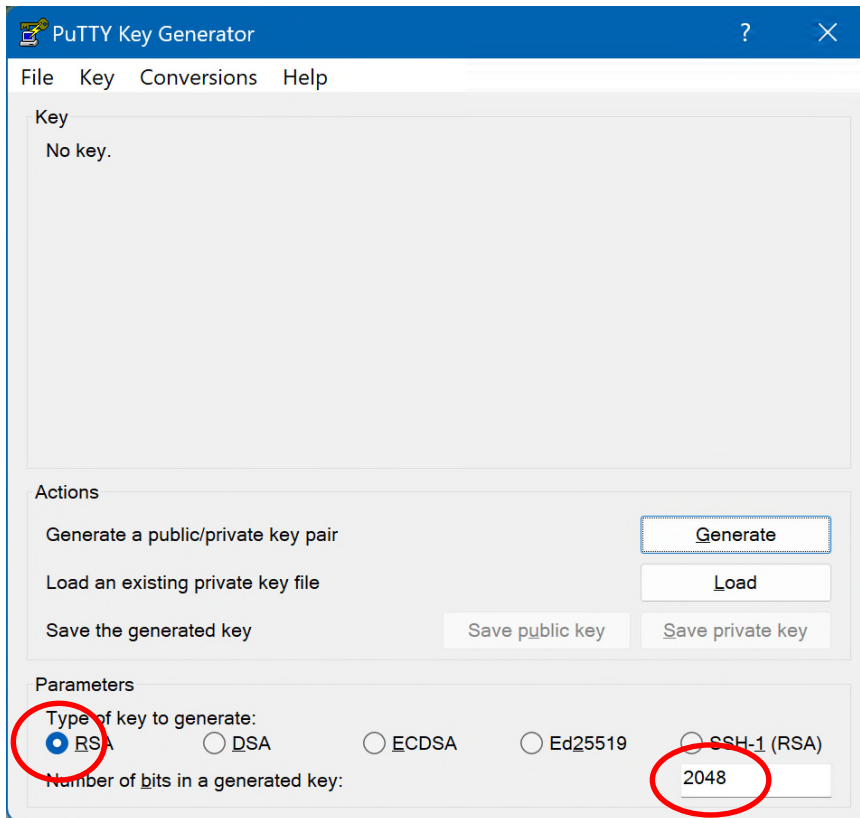
4. Deselect “Preserve Timestamp”



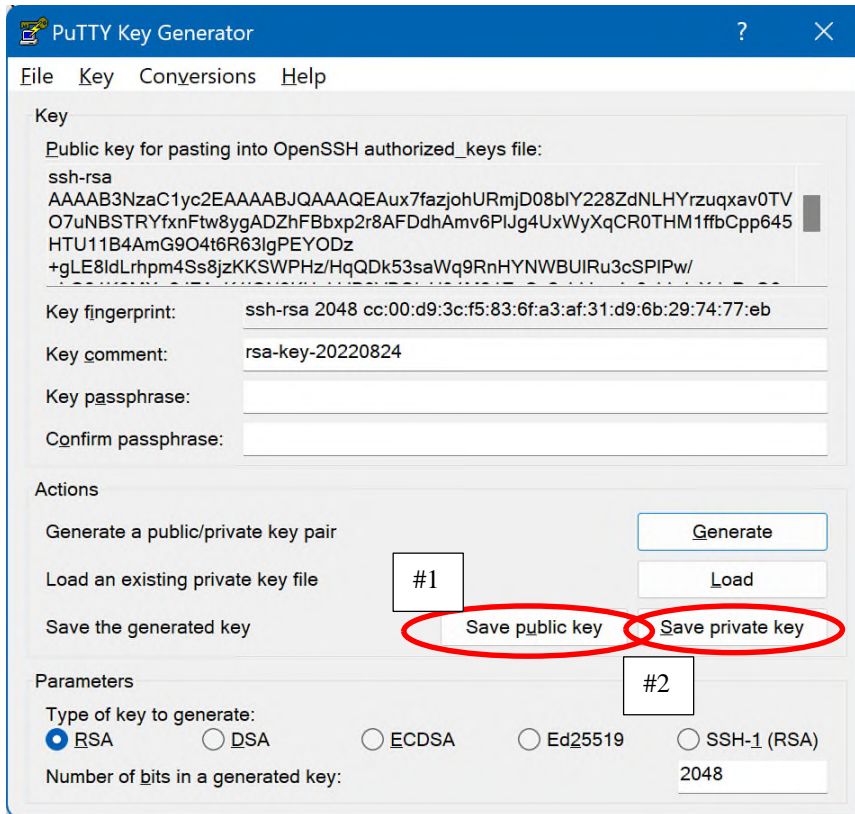
5. Click OK

Appendix E – Generating SSH Keys

This example demonstrates using PuttyGen (Freeware) to generate a Public/Private RSA Key Pair. This can be downloaded from multiple location on the Internet.



Click Generate and follow the directions.



Save each of the keys.

- Save public key - #1
 - Send this key to EMTS on-boarding Support (we have found it best when sending via email to rename the file with a .txt extension)
- Save private key - #2
 - Use this key in your SFTP client/Application.

Appendix – Documentation Version Control

Current Date	Author	Change from Previous Version
03/29/2023	EMTS	Updated Logo to Stellantis, removed references to FCA
07/05/2022	EMTS	Updated EDI outbound filename format and added details for 997.
05/20/2022	EMTS	Added EDI Transaction to Inbound Directory Cross Reference.
11/23/2020	EMTS	Added Client Software Information
02/07/2020	EMTS	Additional information and reorganized sections
10/15/2019	EMTS	Added Default filename information
8/5/2019	EMTS	2 nd version - EMTS SFTP user guide
8/8/2017	EMTS	1 st version - EMTS SFTP user guide