

Transfer Anywhere - Release 1.7.0

(January, 2006)

This new major release of Transfer Anywhere contains many new product enhancements, including support for SFTP and FTPS server connections, AES encryption for password-protected ZIP files, FTP file renaming and command scripting, detailed FTP logging, encryption for backup media and several other enhancements. Some fixes are also included in this new release 1.7.0.

ENHANCEMENTS

1. Provided support for SFTP (FTP over SSH) server connections. SSH (Secure Shell) is a protocol for securing login and communications between the client and server. It provides strong encryption, server authentication and integrity protection for FTP transmissions. The SSH protocol utilizes public and private keys to establish trust between the client and server. Transfer Anywhere complies with the SSH 2.0 protocol standard.

Using the Transfer Anywhere Administrator, you can predefine the SFTP server connections (e.g. host name, user, default path, private key, etc.). When creating a transfer within the wizard, a SFTP server connection can then be selected through a point-and-click dropdown menu.

The following ciphers are supported for SFTP:

- Triple DES, key length of 192 bit
- Blowfish, key length up to 448 bit
- AES, key length up to 256 bit

The following MAC algorithms are used in the SFTP protocol:

- MAC-SHA1, key length 160 bit, digest length 160 bit
- HMAC-SHA1-96, key length 160 bit, digest length 96 bit
- HMAC-MD5, key length 128 bit, digest length 128 bit
- HMAC-MD5-96, key length 128 bit, digest length 96 bit

The following key exchange algorithms are used in SFTP:

- Diffie-Hellman, MODP Groups 1, 2, 5 (1536-bit), 14 (2048-bit), 15 (3072-bit), 16 (4096-bit), 17 (6144-bit) and 18 (8192-bit).

2. Provided support for FTPS (FTP over SSL) server connections. SSL (Secure Socket Layer) is also a protocol for securing login and communications through the use of encryption, server authentication and integrity protection. This protocol utilizes certificates to establish trust between the client and server.

Using the Transfer Anywhere Administrator, you can predefine FTPS server connections (e.g. host name, user, password, default path, etc.). If you only want to connect to a FTPS server if matches a Trusted Certificate, then you can specify the name of the Key Store which contains the Trusted Server Certificates. If your trading partner's FTPS server requires a Client certificate, then you can also specify the location of the Key Store that contains your Client Certificates.

When creating a transfer within the wizard, a FTPS server connection can then be selected through a point-and-click dropdown menu.

3. If retrieving a file from a local file system or a FTP server, and if this file is transferred to a local file system or a FTP server, then the retrieved file can be targeted (renamed) to a different name on the destination. For instance, the retrieved file name of "ABCdata.xls" can be targeted to the file name of "XYZdata.xls" on the destination server. The target file name can be specified on the "Distribution" tab of the Transfer Wizard or can be specified on the iSeries RUNTFR (Run Transfer) command using the *TGTFIL keyword.
4. If retrieving files from a FTP server or the local file system, the user can specify one or more variables for filtering the files selected. Several variables are included, such as \$DATE\$ for the current date and \$TIME\$ for the current time.

For instance, the user could choose to retrieve files that have the filter name of "\$DATE\$orders.xls", which will retrieve any files that have a name starting with the current date, followed by the characters of "orders.xls" (i.e. 2005-11-05orders.xls). The file filter name can be specified on the "Retrieve" tab within the Transfer Wizard.

5. When distributing files to a FTP server or the local file system, the user can specify a prefix or suffix to append to the file names. The user can either enter a constant value or choose a variable for the prefix or suffix, such as the variable \$DATE\$ for the current date or \$TIME\$ for the current time.

For instance, the file name of "customers.xls" could be prefixed with the \$DATE\$ variable to become "2005-11-28customers.xls". The prefix and suffix can be specified on the "Distribution" tab within the Transfer Wizard.

6. The customer can specify a script of commands to run on a FTP server. For example, the FTP command of QUOTE RCMD could be specified to call a program on the server or the command of MKDIR could be specified to create a new directory. The customer can indicate if the FTP commands should run immediately after logging onto the FTP server or just before logging off the FTP server. These FTP commands can be specified within the Transfer Wizard on both the "Retrieve" and "Distribution" tabs.
7. Detailed logs can now be generated for FTP transmissions, which will provide customers with more information to debug failed transmissions. These logs will store all FTP commands issued within a transfer, along with any messages. The detailed FTP logging can be turned on using the iSeries WRKPRP (Work Properties) command. By default, the log files are stored in the IFS directory of \linoma\amblinoma\logs.
8. When generating a ZIP file with a password specified, the user can now protect the file with AES encryption. The provided protection levels are Standard protection, AES 128 bit encryption, AES 192 bit encryption and AES 256 bit encryption. The level of encryption can be specified on the "Compression" tab of the Transfer Wizard or on the iSeries ZIP command.
9. The iSeries UNZIP command was enhanced to allow unzipping a password-protected zip file which is secured with AES encryption.
10. The OpenPGP decryption and encryption processes were enhanced to support files over 4 GB in size.
11. Allow the customer to choose the preferred symmetric encryption algorithm to use for OpenPGP. Valid symmetric encryption algorithms are AES-256, AES-192, AES-128, Blowfish, CAST5, DES, IDEA, Triple DES (DESede) and Twofish. The preferred algorithm can be specified using the iSeries WRKPRP (Work Properties) command.

12. Allow the customer to choose the default hash algorithm to use for OpenPGP. Valid hash algorithms are MD2, MD5, RIPEMD-160, SHA-1, SHA-256, SHA-384 and SHA-512. The preferred algorithm can be specified using the iSeries WRKPRP (Work Properties) command.
13. Provided support for zipping and unzipping iSeries Save files which are over 4 GB in size.
14. Provided a new iSeries command named SAVLIBENC, which can be used to encrypt and save (back up) libraries to tape or other media. This new encryption feature allows customers to better secure their backup media for compliance with governmental regulations such as HIPPA and Sarbanes-Oxley.

SAVLIBENC will transform the selected iSeries libraries into encrypted stream files and then will save these encrypted files onto the designated media device (i.e. tape).

The customer can choose between ZIP/AES and OpenPGP encryption methods on the command. The SAVLIBENC command can be run from an OS/400 command line, placed in a CL program or run from a job scheduler for automation.

15. Provided a new iSeries command named RSTLIBENC, which will restore and decrypt libraries that were saved with the SAVLIBENC command. The libraries will be restored into the whole form as which they were saved, restoring the library descriptions, authorities, objects and data. The RSTLIBENC command can be run from an OS/400 command line, placed in a CL program or run from a job scheduler for automation.
16. Provided a new iSeries command named SAVOBJENC, which can be used to encrypt and save (back up) objects to tape or other media. This command will transform the selected iSeries objects into an encrypted stream file and then will save the encrypted file onto a designated media device (i.e. tape).

The customer can choose between ZIP/AES and OpenPGP encryption methods on the command. The SAVOBJENC command can be run from an OS/400 command line, placed in a CL program or run from a job scheduler for automation.

17. Created a new iSeries command named RSTOBJENC, which will restore and decrypt objects that were saved with the SAVOBJENC command. The objects will be restored in the whole form as which they were saved, restoring the object descriptions, authorities and data. The RSTOBJENC command can be run from an OS/400 command line, placed in CL program or run from a job scheduler for automation.
18. Created a new iSeries command named RTVPOPMSG, which can be used to retrieve emails from a specified POP3 server. For a specified user id, this command can monitor all incoming email or just the email sent from a specific email address. Any retrieved email file attachments can be automatically saved into a designated IFS directory for processing. The RTVPOPMSG command can be run from an OS/400 command line, placed in CL program or run from a job scheduler for automation.
19. Created a new iSeries command named SNDEMLMSG, which can be used for sending email messages. This command provides parameters for specifying the SMTP host, from/to/cc/bcc email addresses, subject, message and attachments. The SNDEMLMSG command can be run from an OS/400 command line, placed in CL program or run from a job scheduler for automation.
20. When defining a transfer that converts database records into a fixed-width or delimited text files, the user indicate if a record delimiter should be used or not. This can be specified on the "Convert" tab within the Transfer Wizard.

21. When logging onto the Transfer Anywhere server with the Administrator, the entered IP and Port# of the server will be saved. The next time the user launches the Administrator, the last IP and Port# used for logon will be shown.
22. The Transfer Anywhere Server Engine can now run on JDK 1.4, in addition to JDK 1.3.
23. If using the iSeries RUNTFR command to run a transfer which retrieves files from a local file system, produce an informational message if no source files were found to transfer. The message will be produced in the job log.
24. Within the Transfer wizard, show the name of the transfer that is currently being viewed/edited in the title bar.
25. Do not allow encrypting or signing a file with an OpenPGP key that is expired (has an expiration date less than the current date).
26. When verifying a file signature with the iSeries VFYSIG or DECRYPT commands, do not require the user to specify the alias of the public key. Instead, automatically search the keyring for the correct public key to use for verifying the signature.
27. On the iSeries ENCRYPT command, default the ARMOR parameter to *NO to reduce processing time and file size.
28. Made significant performance improvements in OpenPGP decryption and signature verifications.
29. On the iSeries ENCRYPT, DECRYPT, VFYSIG and SGNFIL commands, allow the user to use the same destination directory as the source directory with the *SAMEDIR special value.
30. Provided an upgrade process for migrating iSeries installations from versions 1.6.x of Transfer Anywhere to this new version of 1.7.0.

FIXES

1. Within the iSeries ZIP command, allow the user to specify a higher number of file names to zip. This was accomplished by expanding the SOURCE parameter from 100 characters to 3,000 characters.
2. Allow unzipping a Save File to the QSYS.LIB folder using the UNZIP command.
3. If armoring a file using the ENCRYPT command, the file is now closed to release locks on it.
4. If the column mappings are not configured properly in a database-to-database copy, then allow the user to edit the transfer, correct the mappings and resave the transfer.
5. Fixed the CPYTFR (Copy Transfer) command to allow overriding the IP or host name of the source installation.
6. Temporary key ring files are cleaned up from the IFS /tmp directory after performing encryption/decryption operations.

7. After running a transfer that had any keyword overrides on the RUNTFR command, then automatically clean up any temporary folders and files created under the TATemp folder.
8. If a customer upgrades from OS/400 V5R1 to V5R2, the cryptographic JAR files may be removed from the IBM user directory. If the cryptographic JAR files are missing from the IBM user directory, then the encryption/decryption processes will re-copy them from the Transfer Anywhere installation directory.
9. For a FTP-to-Email transfer, produce the appropriate error message when a FTP connection fails.
10. The customer can now edit a transfer in the Transfer Wizard which was defined as Database->HTML->Local or Database->XML->Local transfer.
11. Fixed the zip process so any files in the TATemp folder are not included in the destination zip file.
12. Do not auto-retry a FTP connection if the user id or password is invalid.
13. Do not show console screen when running iSeries commands (e.g. ZIP, UNZIP, ENCRYPT, etc.).

Crypto Studio - Release 2.0

1. Renamed *PGP Studio* to *Crypto Studio*.
2. Added new function to allow generating SSH compliant keys which can be used in SFTP server transmissions.
3. When creating an OpenPGP key pair, the customer can now specify an expiration date for the key.
4. Do not allow encrypting or signing a file if the key is expired.
5. The OpenPGP decryption and encryption processes were enhanced to support files over 4 GB in size.