

Chapter 11

Administration in i-effect

The following functions are part of i-effect's comprehensive module administration:

- o Work with Program Modules
- o Work with Logbook
- o Reorganize i-effect
- o Remove no longer required files
- o Start i-effect Sub Systems
- o End i-effect Sub Systems

This chapter is divided into four thematic focal points and service functions:

1. Licensing + Default Module Values
2. Logbook Functions
3. Monitor Functions
4. i-effect Administration Tasks

Licensing and Default Module Values

Menu Item 80: Work with Program Modules (WRKEFFMOD)

Select this menu item to license modules and to change default settings of installed modules.

i-effect can be configured and adapted to client specific needs by calling up these menu items at any time. To some extent, modifications of the parameters will be realized immediately after entering the values; others will come into effect after restarting the sub systems (*AS2, *EMAIL, *CRYPT, *FAX, *HTTP and *OFTP).

Select menu item 80 in the i-effect main menu to work with program modules.

The following display will appear:

```

Sitzung A - [24 x 80]
-----
Work with i-effect modules                               System:  DEVELOP

Product, release . : 2MEBEFF, V1R4M0
Serial-#, partition: 650956A, 01 (develop)
Position to . . . .

Select option and press enter.
1=Add license key information  2=Change  5=Display details
8=Additional parameters

Op  Module      Description                               State of
tion name      Description                               installation
-   -
-   *BASE       Base module                               *LICENSE
-   *SP00L      Spoolconversion (PDF, HTML...)           *LICENSE
-   *SP00L+    Spoolconversion plus (PCL,...)          *LICENSE
-   *ZIP       ZIP archives                             *LICENSE
-   *CRYPT      Signature/Encryption                    *LICENSE
-   *SIGG      Qualified electronic signature          *LICENSE
-   *EMAIL     eMail send/receive                     *LICENSE
-   *FAX       eFAX send                               *LICENSE
-   *EDIFACT   UN/EDIFACT conversion                  *LICENSE
                                         None...

F3=Exit  F5=Refresh  F11=More  F12=Cancel
© menten GmbH, 1989-2008.
  
```

The dialog program shows the following parameters:

- “Product”, the in-system description of the i-effect license program.
- The i-effect release number.
- Under “Position to”, the list of modules can be repositioned by entering a character string. Repositioning is begun with the first module larger than or equal to the value entered into this field.
- The table shows the most important details of the licensed module, e.g. module name.

Options

To edit the entries, the following options can be used. Enter the option number into the choice box at the beginning of the line of the corresponding entry.

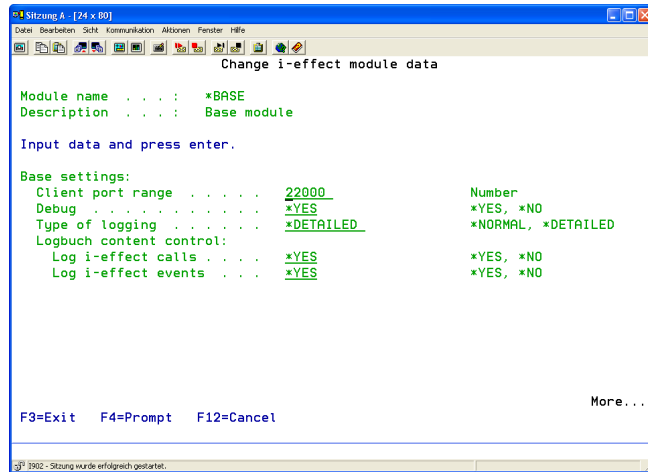
- Add License Key Information (option 1)** To enter the license number for modules that will be licensed, use option 1. The license number is automatically communicated to you after the manufacturer has received the license order.
- Change (option 2)** To change license program information for licensed modules, use option 2 in the corresponding choice box.
- Display (option 5)** To display all details concerning the current licensing of the relevant module, use option 5 in the corresponding choice box. A new dialog program will appear. Current prohibitions, the license key, and possibly the expiration date of the demo version can be viewed.
- Additional Parameters (option 8)** To edit adjustable parameters for licensed modules, use option 8.

Additional Parameters (Option 8)

Some i-effect modules have adjustable parameter values. These can be called up and edited by using option 8.

Additional Parameters of the *BASE Module

Select the *BASE module by entering option number 8 into the corresponding choice box. In the dialog program "Change i-effect Module Data", parameters can now be modified.



The following options for the *BASE module can be set:

Client Port Range

Enter the port range for clients that have remote access to certain functionalities of i-effect.

Positive Integral Default Value: 22000

Debug ?

The debug switch controls whether additional information is recorded in the job log within an i-effect application and whether temporary files are kept for analysis.

Possible values:

- *NO Additional information is not recorded. Temporary files will be deleted at the end of the job.
- *YES Additional information is recorded. Temporary files will not be deleted at the end of the job.

Type of Logging

This parameter determines the amount of messages logged into the job log. It is recommended to set this parameter to *DETAILED in order to allow a detailed problem analysis. Important information for the support will be recorded.

Possible values:

- *NORMAL Normal logging.
- *DETAILED Detailed logging.

Logbook Control

This parameter includes two elements:

- Record i-effect calls
- Record i-effect events

This parameter is used to define the amount of messages logged into the logbook. Using the value *NO in both parameters completely disables all logging.

Internal Protocols: Other Work Files

This directory is fixed during installation and cannot be changed. It contains internal loggings and debugging information.

Default: /i-effect/<RELEASE>/internal

Basic IFS

This directory is fixed during installation and cannot be changed. It contains the basic i-effect program directory in the IFS files system.

Default: /i-effect/<RELEASE>

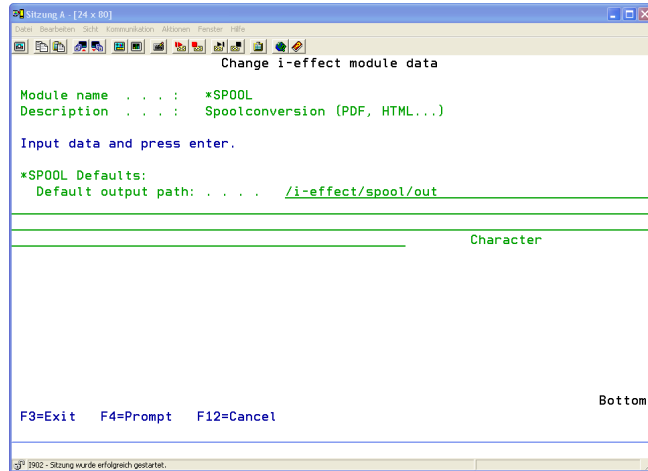
Sending Preparation Path: Working Directory

This directory contains files prepared for sending. It is a working directory for i-effect that can store temporary work files.

Default: /i-effect/<RELEASE>/internal/send_prepared

Additional Parameters of the *SPOOL Module

Select the *SPOOL module by entering option number 8 into the corresponding choice box. In the dialog program "Change i-effect Module Data", parameters can now be modified.



The following parameters can be defined for the *SPOOL module:

*SPOOL Defaults:

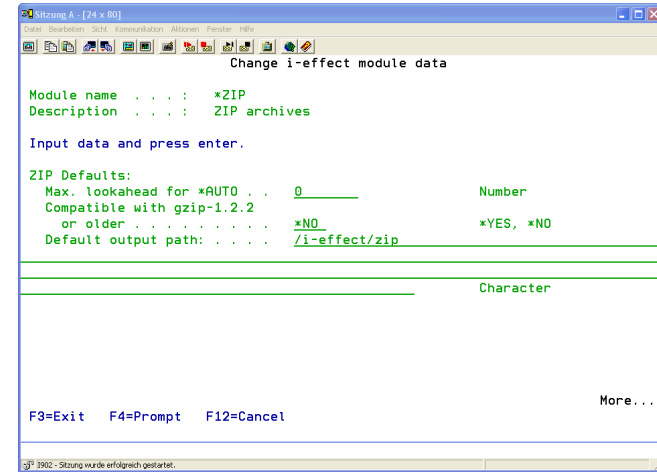
Default Output Path

This parameter defines the path where files generated with this module will be stored this path automatically if the variable %DEFAULTPATH% is used in the OUTPFILE parameter of the CVTSPLXXX command.

Default: /i-effect/<RELEASE>/spool/out

Additional Parameters of the *ZIP Module

Select the *ZIP module by entering option number 8 into the corresponding choice box. In the dialog program "Change i-effect Module Data", parameters can now be modified.



The following parameters can be defined for the *ZIP module:

*ZIP Defaults:

Max. Lookahead for *AUTO

The maximum lookahead defines how many bytes are to be read from the decompressed data stream when determining the record length of a file (OUTRECL(*AUTO)). The larger the number of bytes, the longer it takes to automatically determine the record length.

Default value:

0 The default value is 0 (read the entire data stream).
If large files with definite record structure are processed, it is recommended to limit the value in order to improve runtime.

Compatible with gzip 1.2.2

Determine if gzip files are generated in a format compatible with older versions of gzip. Version 1.2.2 does not support file comment fields, which are supported by version 1.2.4. and higher.

Possible values:

- *NO Create gzip files in the current format of version 1.2.4 and use file comment field
- *YES Create gzip files in an older format. This is required to open i-effect files with older gzip or WinZip versions, or other unpacking applications.

Default Output Path

This parameter defines the path where files generated with this module will be stored this path automatically if the variable %DEFAULTPATH% is used in the OUTPFILE parameter of the CVTSPLXXX command.

Default: /i-effect/<RELEASE>/spool/out

ZIP Standards for Compression before Sending:**Create ZIP Archive?**

Determine if a ZIP archive will be created to archive outbound data.

Possible values:

- *NO No ZIP archive is created for archiving.
- *YES A ZIP archive is created for archiving.

Compression Rate

With this parameter the relation between optimal compression speed and maximum compression is managed. This relation is balanced in the default setting. Using value 1, the program achieves the highest speed but maximum compression will not be achieved. Using value 9, maximum compression is achieved but the program runs at a slower rate.

Default value:

- 3 Values between 0 – 9 are valid. 0 = no compression; 9 = maximum compression.

Use Original Name?

The original name of the input file can be output into the compressed output file. Therefore, i-effect uses the name of the input file member. This name can be used for decompression in order to restore the file with exactly this name. (In this version the name can indeed be used for compression, but when decompressing the name is merely stored for information purposes in the file member text of the generated file member.)

Possible values:

- *NO The original name of the input file member is not stored.
- *YES The original name of the input file member is stored in the compressed output file.

Enter CRLF ?

In order to enable the recipient to recognize the record structure of the original file, control characters for carriage return and line feed (CRLF) can optionally be inserted at the end of each record.

Possible values:

- *NO Data remain unchanged for input and compression
- *YES The control characters EBCDIC X'0D25' or ASCII X'0D0A' are inserted at the end of each record.

Delete Subsequent Blanks ?

When processing a file for compression, i-effect may delete all subsequent blanks at the end of each dataset. In connection with the parameter CRLFINSERT, this may be used to have the last character of a dataset followed by a record control character, which is not a blank.

Possible values:

- *NO Blanks at the end of a dataset will NOT be deleted.
- *YES All blanks at the end of a dataset will be deleted.

From CCSID ?

The code page number of the source system.

Possible values:

- *JOB i-effect uses the job's CCSID. .
- Zahl The CCSID's number.

To CCSID ?

The code page number of the target system.

- *JOB i-effect uses the job's CCSID. .
- Zahl The CCSID's number.

Naming the Archive Entry

Enter the name of the archive entry.

**DEFAULT*

Format for Filenames

Enter the default format for filenames. When storing the file in the archive, the file is built as follows.

<i>*FILE</i>	The name of the archive file is identical to the name of the input file
<i>*MEMBER</i>	The name of the archive file is identical to the name of the input file member.
<i>*NAMEFMT0</i>	The name of the archive file corresponds to the following format: library/file.filemember
<i>*NAMEFMT1</i>	The name of the archive corresponds to the following format: QSYS.LIB/library.LIB/file.FILE/file member.MBR

ZIP Standards for Decompression after Reception:**From CCSID ?**

The code page number of the source system.

<i>*JOB</i>	i-effect uses the job's CCSID.
<i>Number</i>	The CCSID's number.

To CCSID ?

The code page number of the target system.

<i>*JOB</i>	i-effect uses the job's CCSID.
<i>Number</i>	The CCSID's number.

Record Length Output File

This parameter defines the record length of the output file.

<i>*AUTO</i>	Using this setting, the input file's record length is automatically used for compression. If inserting additional control characters is activated in parameter "CRLFINSERT"; this will be considered when determining the record length. The decompressed data will be analyzed during decompression if *AUTO is selected. If record control characters (CRLF) are found, the output file will be stored with the record length that is necessary to store all datasets. (The length of the longest record will be used for the file.)
<i>Number</i>	Record length

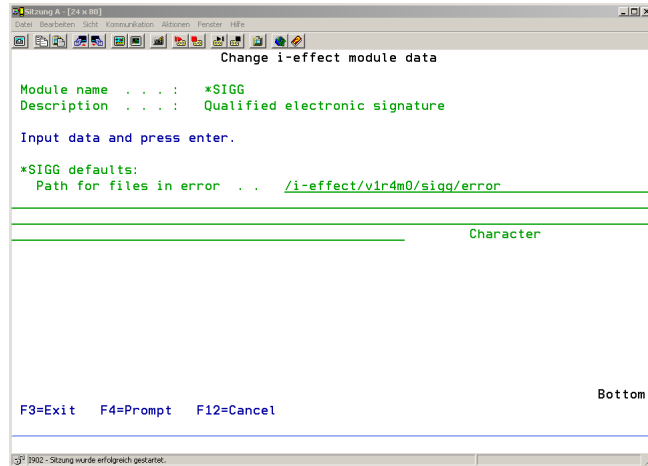
Output Library

Enter the name of the library for output files.

<i>*STD</i>	Default value.
-------------	----------------

Additional Parameters of the *SIGG Module

Select the *SIGG module by entering option number 8 into the corresponding choice box. In the dialog program "Change i-effect Module Data," parameters can now be modified.



The following options for the *SIGG module can be set:

*SIGG Defaults:

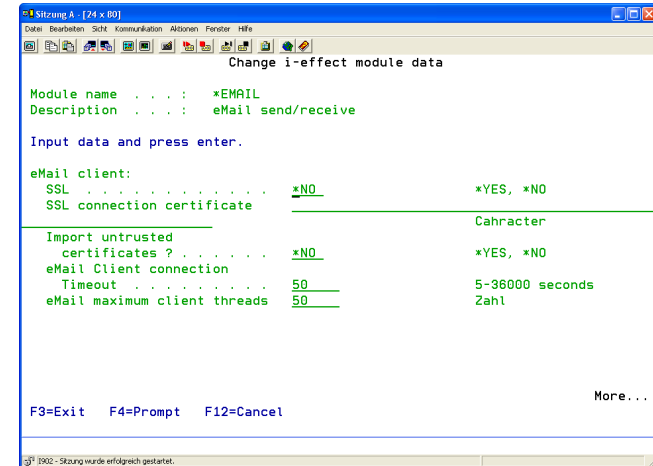
Path for Damaged Files

This parameter defines the default path where files are stored for which a qualified digital signature could not be generated automatically, e.g. if the input file was an erroneous EDIFACT file.

Default Path: /i-effect/>RELEASE>/sigg/error

Additional Parameters of the *EMAIL Module

Select the *EMAIL module by entering option number 8 into the corresponding choice box. In the dialog program "Change i-effect Module Data," parameters can now be modified.



The following options for the *EMAIL module can be set:

SSL

Determine if SSL (Secure Socket Layer) will be used to establish a connection to the email server.

*YES YES, SSL is used.

*NO NO, a standard connection is to be established.

SSL Connection Certificate

If *YES is set in the parameter "SSL," the name of the certificate in the keystore, which will be used for authentication of the email server, can be entered here. In SSL connections, the email server identifies to the client by transmitting its X509 certificate to the client when the connection is established. The client decides whether the certificate is known and valid, and therefore, whether the email server can be trusted. The certificate defined here is compared to the certificate sent by the email server. Of course, the email server's certificate must be imported into the i-effect keystore before establishing a connection.

Use Client Authentication ?

This parameter no longer applies.

Import Untrustworthy Certificates ?

Enter the value *YES into this parameter to automatically import email server certificates. The email server identifies to the client by transmitting its X509 certificate itself when the connection is established. If the certificate does not exist in the i-effect keystore, it will be imported automatically.

If the value *NO is entered into this parameter and the certificate of the remote server does not exist in the i-effect keystore, the connection will automatically be closed

- *YES YES, server certificates are automatically imported.
- *NO NO, server certificates are not imported.

Use TLS ?

This parameter is dropped.

Email Client Connection Timeout

Define the time in seconds that the client waits for connection establishment. If the time has expired, a timeout notification will be sent.

Possible values: 5-36000

Maximum Email Client Threads

Enter the maximum number of simultaneous email-client-connections.

SMTP Host/IP

Define the SMTP email server that will be used to send emails. It may be either a DNS name or a TCP/IP address in the form of xxx.xxx.xxx.xxx.

All email servers working according to SMTP protocols, e.g. Lotus Notes or Microsoft Exchange, can be used.

SMTP Port

Define the TCP/IP port that will be used for SMTP communication. The default port for SMTP is 25.

SMTP User ID

Enter the user ID of the user authorized to access the SMTP server.

SMTP Password

Enter the password of the user being authorized to access the SMTP server.

SMTP Sender

Enter the sender of outbound emails sent via SMTP.

SMTP Reply-to

Enter an address to which a reply to the email should be sent.

Possible special value:

- *SENDER The Reply-to email address is identical to the sender's address.

SMTP Error-to

Enter an address to which an error notification should be sent

Possible special value:

- *SENDER The Error-to email address is identical to the sender's address.

SMTP Text Format

This parameter defines which format is to be used for the message text.

The following values are possible:

- *PLAIN Simple Text
 The entered text, or text imported from an external file, will be sent as email with content type „text/plain“.
- *HTML HTML Text
 The entered text, or text imported from an external file, will be sent as email with content type „text/html“. The text will be put into a standard HTML structure and needs not to be available as HTML file.
 If the external file is a HTML file (file extension .htm or .html), the content will not be put into a standard HTML structure but will be sent as it is. Therefore, it is possible to send arbitrary HTML contents as email.
- *BOTH Text and HTML
 The entered text, or text imported from an external file, shall be sent as email with content type „ multipart/alternative “ („text/plain“ and „text/html“). The text will be put into a standard HTML structure. The email client on the remote side decides which of the two parts will be displayed (depending on the preferences of the particular email-client-program).

SMTP Encryption

This parameter defines the character set that is to be used for the message text. Data will be converted into the code page defined in this setting before sending.

The following values are possible:

*UNICODE	Universal character set
*ISO-8859-1	ISO-8859-1 (Latin1) covers most of the Western European languages, e.g. French (fr), Spanish (es), Catalan (ca), Basque (eu), Portuguese (pt), Italian (it), Albanian (sq), Rhaeto-Romanic (rm), Dutch (nl), German (de), Danish (da), Swedish (sv), Norwegian (no), Finnish (fi), Faeroese (fo), Icelandic (is), Irish (ga), Scottish (gd) and English (en), partly Afrikaans (af) and Swahili (sw). Therefore, it covers the entire American continent, Australia, parts of Asia and a big part of Africa.
*ISO-8859-2	SO-8859-2 (Latin2) covers the languages of Central and Eastern Europe: Czech (cs), Hungarian (hu), Polish (pl), Romanian (ro), Croatian (hr), Slovak (sk), Slovenian (sl), Sorbian.
*ISO-8859-3	SO-8859-3 (Latin3) is to be used for Esperanto (eo) and Maltese (mt), and covered Turkish before the introduction of Latin5 in 1988.
*ISO-8859-4	ISO-8859-4 (Latin4) contains letters for Estonian (et), the Baltic languages, Latvian (lv) and Lithuanian (lt), Greenlandic (kl) and Sami languages.
*ISO-8859-5	These Cyrillic letters cover Bulgarian (bg), Belorussian (be), Macedonian (mk), Russian (ru), Serbian (sr) and before 1990 Ukrainian (uk).
*ISO-8859-6	This is the Arabic alphabet, but regrettably just the simple one for Arabian (ar) without the four Persian (fa) and eight Pakistani (Urdu, ur) extra letters.
*ISO-8859-7	This is the (modern monotonic) Greek (el) alphabet.
*ISO-8859-8	This is the Hebrew script, used for Hebrew (iw) and Yiddish (ji).
*ISO-8859-9	ISO-8859-9 (Latin 5) replaces the rarely used Icelandic specific characters with Turkish letters.
*ISO-2022-JP	The Japanese Katakana DBCS character set.
*ISO-2022-KR	The Korean DBCS character set.
*ISO-2022-CN	The Chinese DBCS character set.

Archive Outbound Emails

This parameter determines if outbound emails are to be stored in the archive directory. The email will be stored entirely including possible attachments.

The following values are possible:

*YES	YES, emails are archived after sending.
*NO	NO, emails are archived after sending.

SMTP Archive Directory

The default IFS path where sent emails are stored.

SMTP Priority

This parameter defines the priority by which the email is sent.

The following values are possible:

*NORMAL	Normal Priority. The email is marked with normal priority.
*LOW	Low Priority. The email is marked with low priority.
*HIGH	High Priority. The email is marked with high priority.

MDN Request

This parameter determines if a receipt confirmation (MDN) is requested for sent emails. If the receiving system supports this function, an email (MDN) to confirm the reception of the original email will be generated automatically.

The following values are possible:

*YES	Request MDN. Receipt confirmation is requested.
*NO	MDN is not requested. Receipt confirmation is not requested.

SMTP Proxy Host

If a proxy server is used for sending emails, enter its IP address or DNS name here.

SMTP Proxy Port

If a proxy server is used for sending emails, enter its TCP/IP port here.

SMTP Proxy User ID

Enter, if required, the user ID of the user being authorized to access the proxy server.

SMTP Proxy Password

Enter, if required, the password of the user being authorized to access the proxy server.

SMTP Signature Alias

Enter the alias of the key pair (private key) in the keystore, which is used for signature.

SMTP Signature Algorithm

This parameter determines if the outbound email has to be signed electronically. If an email is signed electronically, it allows the receiver to check it for authenticity and integrity as well as its origin by using his public key.

Possible values:

*NONE	No Signature. The email is not signed.
*MD5	MD5 Signature The signature is generated using the MD5 algorithm (Message Digest Algorithm 5). It is a widespread cryptographic hash function, generating a 128bit hash value.
*SHA1	SHA1 Signature The signature is generated using the SHA-1 algorithm (secure hash algorithm). This algorithm, designating a group of standardized cryptographic hash functions, generates a 160bit hash value.

SMTP Encryption Alias

Enter the alias of the public key (certificate) in the keystore, which is used for encryption.

SMTP Encryption Algorithm

This parameter determines if the outbound email must be encrypted before sending. If an email is encrypted using the partner's public key, it can only be decrypted by the partner with his private key.

Possible values:

*NONE	No encryption. The email is not encrypted.
*TRIPLEDES	3DES Encryption The email is encrypted by the 3DES (Data Encryption Standard) It is a widespread symmetric encryption algorithm. Its key length of 3DES (= 168 bits) is three times as long as with DES (= 56 bits).

POP Host/IP

This parameter defines the email server that is to be used to receive emails. Enter either a DNS name or a TCP/IP address in the form of xxx.xxx.xxx.xxx.

Every server working according to the POP3 or IMAP protocol can be used, e.g. Lotus Notes or Microsoft Exchange. An account, which is read out with the command RCVE-MAIL, must be created on the server.

POP Port

The TCP/IP port number, under which the mail server can be accessed. The standard value for a SMTP server is 25, for POP3 it is 110 and for IMAP mostly 143.

POP User ID

Usually, authentication is necessary to login to the POP3/IMAP server. The user ID defined here is used for this purpose.

POP Password

Enter the password related to the user ID.

POP Protocol

This parameter determines the protocol that will be used to receive emails.

The following values are possible:

*POP3	The POP3 protocol is used.
*IMAP	The IMAP protocol is used.

Archive Inbound Emails

Determines if inbound emails will be archived. The email will be stored entirely including possible attachments.

The following values are possible:

- *YES YES, received emails are archived.
- *NO NO, received emails are not archived.

Archive Directory

Enter the directory where received emails are to be stored.

Attachment Directory

Enter the IFS directory where attachments of incoming emails are stored.

Inline Text Directory

Enter the directory where the textual content of incoming emails is stored.

POP Proxy Host

If a proxy server is used for receiving emails, enter its IP address or DNS name here.

POP Proxy Port

If a proxy server is used for receiving emails, enter its TCP/IP port here.

POP Proxy User ID

Enter, if required, the user ID of the user authorized to access the proxy server.

POP Proxy Password

Enter, if required, the password of the user authorized to access the proxy server.

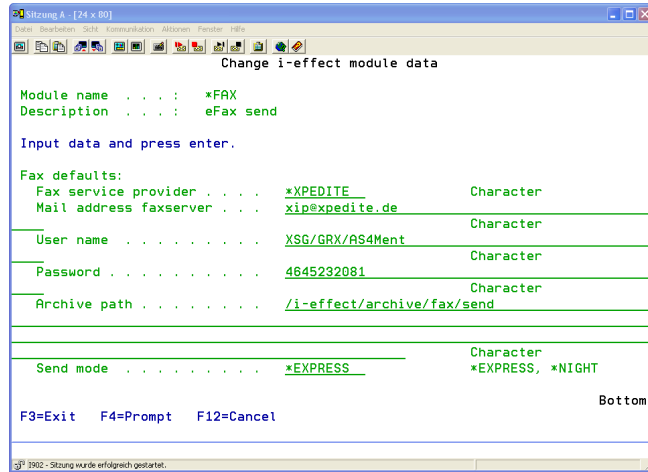
Type of Call

This parameter defines whether the calling server waits for a feedback or is immediately available for further action.

- *SYNCH Synchronous means the system will wait for an answer from the remote side, with for example RCV/SNDEMAIL, all files will be sent, before further actions can be taken.
- *ASYNCH The iSeries server is immediately available for further actions, because processing of the remote-controlled call runs in the background.

Additional Parameters of the *FAX Module

Select the *FAX module by entering option number 8 into the corresponding choice box. In the dialog program "Change i-effect Module Data", parameters can now be modified.



The following options for the *FAX module can be set:

Fax Parameters

Fax Service Provider

Enter the fax service provider's name. The fax is sent via telephone lines to the designated addressees.

Email Address Fax Server

Enter the email address of the fax server that is used to receive the fax jobs in the form of an email.

Currently, the following fax servers can be used:

<http://datacomm.premiereglobal.com/de/de/>

User ID

Enter a user ID to login to the fax-email-server.

Password

Enter a password to login to the fax-email-server.

Archive Path

Define the directory where outbound faxes are to be stored.

Default path: /i-effect/<RELEASE>/archive/fax/send

Send Mode

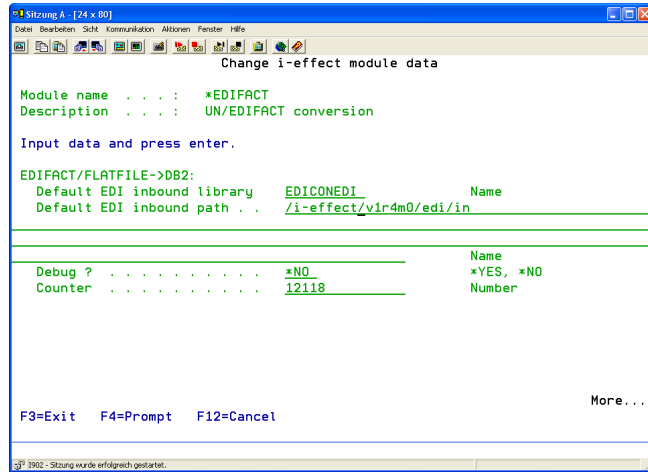
This parameter determines the mode of sending. The fax can either be sent immediately to the recipient or the cost-effective night rate is used.

The following values are possible:

- *NIGHT* Using this mode, the fax is sent directly but with low priority. Job execution is temporally delayed, at night, and therefore costs less.
- *EXPRESS* Using this mode, the fax is sent immediately after transmission to the fax server. It is sent with high priority at a higher rate.

Additional Parameters of the *EDIFACT Module

Select the *EDIFACT module by entering option number 8 into the corresponding choice box. In the dialog program "Change i-effect Module Data", parameters can now be modified.



The following options for the *EDIFACT module can be set:

EDIFACT general settings:

One File per Document ?

This parameter determines if a new output file is generated for each record processed from a primary file.

- | | |
|------|--|
| *YES | A new output file is created for every primary data set. |
| *NO | A new output file is created only if the description of the primary file, defined as primary key, changes. |

EDIFACT/FLATFILE->DB2:

Default EDI Inbound Library

This parameter determines the name of the library being used as default inbound library to process conversions EDIFACT/FLATFILE->DB2. This default library will be provided automatically when selecting the form of conversion from the DB2 file system, when the conversion command is used.

<i>Name</i>	Name of the Default EDI Inbound Library
-------------	---

Default EDI Inbound Path

This parameter determines the name of the path used as the default inbound path to process conversions EDIFACT/FLATFILE->DB2. This default path will be provided automatically when selecting the form of conversion from the IFS file system, when the conversion command is used.

Default path: /i-effect/<RELEASE>/edi/in

Debug ?

This parameter determines if conversion is to be processed with or without debugging. If this parameter is set to *YES, errors occurring during conversion do not lead to cancellation of the conversion process. All problems that occur during conversion are logged into the logbook for further analysis.

- | | |
|------|--|
| *YES | YES, conversion is processed with debugging. |
| *NO | NO, conversion is processed without debugging. |

Counter

This global counter can be used in a conversion mapping table, e.g. to generate a clear serial counter number for every generated output file.

<i>Number</i>	Counter value
---------------	---------------

DB2 -> EDIFACT/FLATFILE:

Default EDI Outbound Library

This parameter determines the name of the library being used as default outbound library to process conversions EDIFACT/FLATFILE->DB2. This default library will be provided automatically when selecting the form of conversion from the DB2 file system, when the conversion command is used.

<i>Name</i>	Name of the Default EDI Outbound Library
-------------	--

Next Number

In the DB2 file system, only 10-digit names can be used to store output files of a conversion. The name is generated automatically, composed of a prefix (1 character) and a serial number (9 digits) created here. This number will be automatically increased by 1 for every generated outbound file.

Number Value of the next number.

File Prefix

In the DB2 file system, only 10-digit names can be used to store output files of a conversion. The name is generated automatically, composed of a prefix (1 character) to be defined here and serial number (9 digits) created in the parameter "Next Number".

Character Value of the file prefix.

Default EDI Outbound Path

This parameter determines the name of the path being used as default outbound path to process conversions EDIFACT/FLATFILE->DB2. This default path will be provided automatically when selecting the form of conversion from the IFS file system, when the conversion command is used.

Default path: /i-effect/<RELEASE>/edi/out

Debug ?

This parameter determines if conversion is to be processed with or without debugging. If this parameter is set to *YES, errors occurring during conversion do not lead to cancellation of the conversion process. All problems that occur during conversion are logged into the logbook for further analysis.

*YES YES, conversion is processed with debugging.

*NO NO, conversion is processed without debugging.

EDI Archiving:**Archive Inbound Files ?**

This parameter determines if inbound files are to be stored in an archive directory after being processed. (A copy of the generated file will be made.)

*YES YES, every processed inbound file is archived.

*NO NO, none of the processed inbound files is archived.

Default EDI Inbound Archive Path

This parameter determines the name of the path where inbound files are to be archived if archiving is activated. Directories will be created automatically in this path if they do not exist.

Default Path: /i-effect/<RELEASE>/archive/edi/in

Archive Outbound Files ?

This parameter determines if outbound files are to be stored in an archive directory after being processed. (A copy of the generated file will be made.)

*YES YES, every processed outbound file is archived.

*NO NO, none of the processed outbound files is archived.

Default EDI Outbound Archive Path

This parameter determines the name of the path where outbound files are to be archived if archiving is activated. Directories will be created automatically in this path if they do not exist.

Default Path:/i-effect/<RELEASE>/archive/edi/out

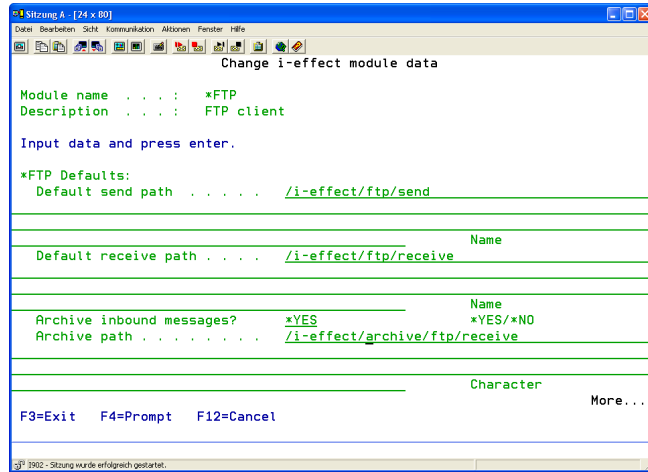
EDI Error:**Path for Erroneous Files**

This parameter determines the name of the path where erroneous files are to be moved to, if desired.

Default path: /i-effect/<RELEASE>/edi/error

Additional Parameters of the *FTP Module

Select the *FTP module by entering option number 8 into the corresponding choice box. In the dialog program "Change i-effect Module Data", parameters can now be modified.



The following options for the *FTP module can be set:

*FTP Details:

Default Send Path

Enter the default path for outbound FTP files.
Default Path: /i-effect/<RELEASE>/ftp/send

Default Receive Path

Enter the default path for inbound FTP files.
Default Path: /i-effect/<RELEASE>/ftp/receive

Archive Inbound Messages?

Determine if inbound FTP files will be archived.

- *YES YES, inbound FTP files are archived.
- *NO NO, inbound FTP files are not archived.

Archive Path

Enter the archive path where inbound FTP files are to be archived.
Default Path: /i-effect/<RELEASE>/archive/ftp/receive

Archive Outbound Messages?

Determine if outbound FTP files will be archived.

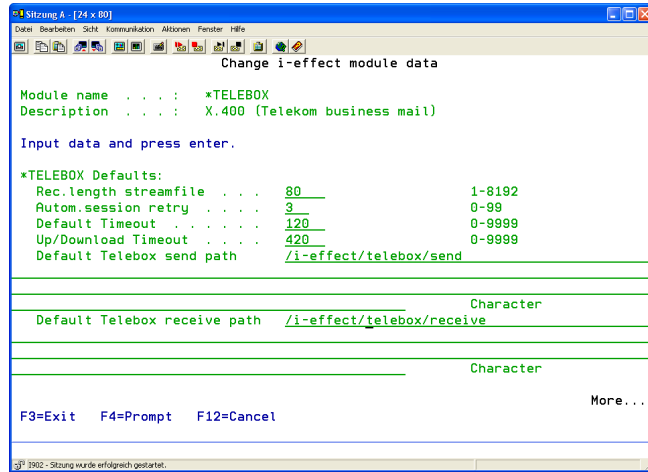
- *YES YES, outbound FTP files are archived.
- *NO NO, outbound FTP files are not archived.

Archive Path

Enter the archive path where outbound FTP files will to be archived.
Default Path:/i-effect/<RELEASE>/archive/ftp/send

Additional Parameters of the *TELEBOX Module

Select the *TELEBOX module by entering option number 8 into the corresponding choice box. In the dialog program „Change i-effect Module Data“, parameters can now be modified.



The following options for the *TELEBOX module can be set:

*TELEBOX Details:

Record Length Stream File

Enter the record length of a dataset in data stream data.

Za Number Valid values: 1-8192
hl

Retries

Define the maximum number of attempts to establish *TELEBOX communication.

Number Valid values: 0-99

Default Timeout

Define a timeout value until *TELEBOX communication is canceled in the case of error.

Number Valid values: 0-9999

Up/Download Timeout

Define a timeout value until *TELEBOX communication is canceled in the case of upload or download failure.

Number Valid values: 0-9999

Default Telebox Send Path

Enter the default path from where *TELEBOX data is sent.

Default path: /i-effect/<RELEASE>/telebox/send

Default Telebox Receive Path

Enter the default path where *TELEBOX data is received.

Default path: /i-effect/<RELEASE>/telebox/receive

*TELEBOX Archive Settings:

Archive Inbound Messages ?

Determine if inbound *TELEBOX messages will be archived.

**YES* YES, *TELEBOX inbound messages will be archived.
**NO* NO, *TELEBOX inbound messages will not be archived.

Archive Path (Inbound)

Enter the path where inbound *TELEBOX data will be archived.

Default path: /i-effect/<RELEASE>/archive/telebox/receive

Archive Outbound Messages ?

Determine if outbound *TELEBOX messages shall be archived

**YES* YES, *TELEBOX outbound messages will be archived.
**NO* NO, *TELEBOX outbound messages will not be archived.

Archive Path (Outbound)

Enter the path where outbound TELEBOX data will be archived.

Default path: /i-effect/<RELEASE>/archive/telebox/send

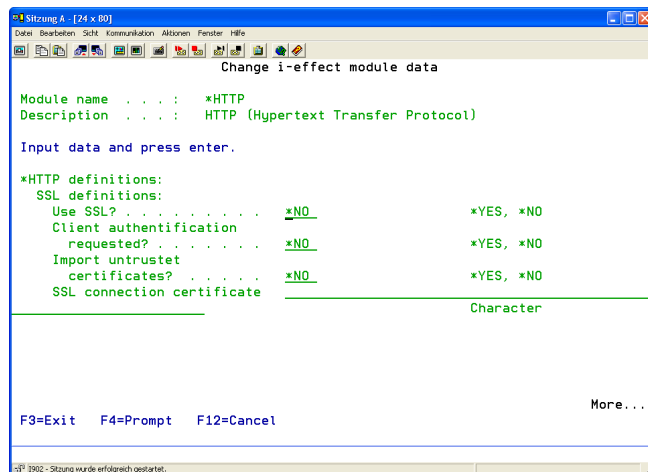
TELEBOX Error:*Path for Erroneous Files**

This parameter determines the name of the path where erroneous *TELEBOX data is moved.

Default path: /i-effect/<RELEASE>/archive/telebox/error

Additional Parameters of the *HTTP Module

Select the *HTTP module by entering option number 8 into the corresponding choice box. In the dialog program "Change i-effect Module Data", parameters can now be modified.



The following options for the *HTTP module can be set:

SSL Details:**SSL**

This parameter controls the protocol to be used. Determine whether HTTP communication is to be established via SSL/HTTPS (Secure Socket Layer) or standard HTTP.

- *YES YES, the connection is established via SSL/HTTPS
- *NO NO, the connection is established via standard HTTP.

Use Client Authentication?

If *YES is set in the "SSL" parameter, this parameter determines if the client sending data must authenticate with its X.509 certificate to the HTTP server.

If *YES is set here and *NO is set in the preceding parameter "Import Untrustworthy Certificates ?", the partner's certificate must exist in the keystore before establishing a connection. By this, the partner's certificate, automatically sent via an established HTTPS connection, can be verified by the HTTP server. The HTTP server only accepts the incoming connection after successful verification of the client's certificate (check with certificate in the keystore). Otherwise, the connection will be closed due to the lack of proof that it is the partner trying to connect.

If *NO is set in this parameter, certificate verification is not requested when establishing a connection.

- *YES Yes, client authentication is used.
- *NO No, client authentication is not used.

Please note: This form of SSL authentication is supported by only a few clients and is generally not common on the Internet.

Import Untrustworthy Certificates?

If *YES is set in the "SSL" parameter, it is possible to allow the HTTP server to automatically import client certificates that do not exist in the keystore. Therefore, select option *YES in this parameter. This might be a security risk inasmuch as every client is considered trustworthy due to automatic import of the client's certificate into the keystore.

If option *NO is set and the certificate does not exist in the keystore when a connection is established, the connection will automatically be closed. It is correct to abort the connection because the client's identity cannot be verified due to the missing certificate in the keystore.

Automatic import of certificates into the keystore is only possible if the parameter „Use Client Authentication ?” is set *YES.

- | | |
|------|---|
| *YES | Yes, untrustworthy client certificates are automatically imported. |
| *NO | No, untrustworthy client certificates are not automatically imported. |

SSL Connection Certificate

Enter the name of the key pair containing the public key (certificate) in the keystore, which is to be used for connection authentication.

Characters Alias of the certificate in the keystore.

Connection:

Connection Timeout

Define the timeout in seconds for connection establishment.

Read Timeout

Define the timeout in seconds for reading data on an open data connection.

Internal Timeout

This parameter defines the timeout value in seconds until an internal timeout is reported.

Maximum Send Retries

Define the maximum number of attempts to retry to send a file after connection failure or interruption.

Retry Pause

Define the pause in seconds before the next attempt to connect.

Email Address Originator

Originator email address that is inserted into the header as sender address.

Email Address Webmaster

Email address of the responsible Webmaster.

Proxy:

HTTP Proxy Host

If a proxy server is used for HTTP communication, enter its IP address or DNS name here.

HTTP Proxy Port

If a proxy server is used for HTTP communication, enter its TCP/IP port here.

HTTP Proxy User ID

If a proxy server is used for HTTP communication, enter, if required, the user ID of the authorized user.

HTTP Proxy Password

If a proxy server is used for HTTP communication, enter, if required, the password of the authorized user.

Archive:

Archive Inbound Messages ?

Determines if inbound HTTP data is to be archived.

The following values are possible

- | | |
|------|------------------------------------|
| *YES | YES, received data is archived. |
| *NO | NO, received data is not archived. |

Archive Outbound Messages ?

Determine if outbound HTTP data shall be archived.

The following values are possible

- | | |
|------|---|
| *YES | YES, inbound data shall be archived. |
| *NO | NO, inbound data shall not be archived. |

Archive Directory**Archive Path (Inbound)**

Enter the directory where inbound HTTP data shall be archived.

Default path: /i-effect/<RELEASE>/http/in

Archive Path (Outbound)

Enter the directory where outbound HTTP data shall be archived.

Default path: /i-effect/<RELEASE>/http/out

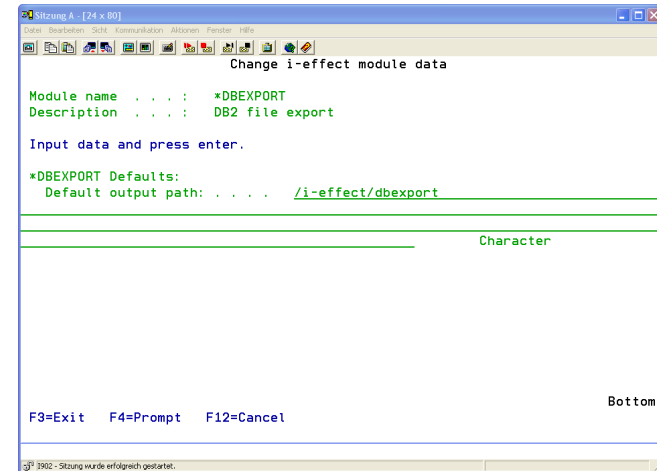
Path for Erroneous Files

This parameter determines the name of the path where erroneous HTTP data is moved.

Default path: /i-effect/<RELEASE>/http/error

Additional Parameter of the *DBEXPORT Module

Select the *DBEXPORT module by entering option number 8 into the corresponding choice box. In the dialog program "Change i-effect Module Data", parameters can now be modified.



The following options for the * DBEXPORT module can be set:

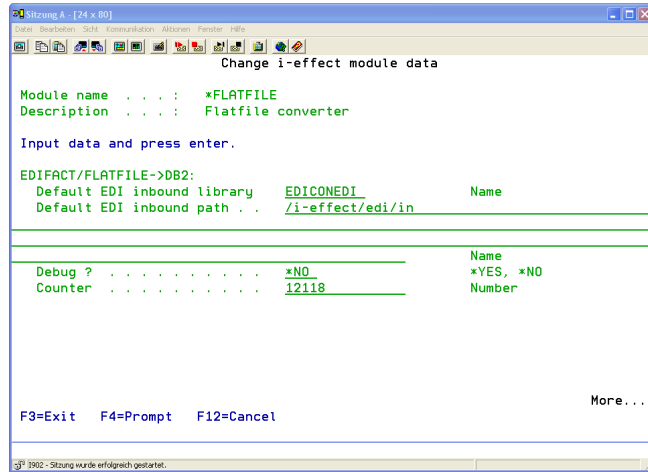
DBEXPORT Default Settings:*Default Output Path**

Files generated with this module will be stored in this path automatically if the variable %DEFAULTPATH% is used in the TOSTMF parameter of the CVTDDBF command.

Default path: /i-effect/<RELEASE>/dbexport

Additional Parameters of the *FLATFILE Module

Select the *FLATFILE module by entering option number 8 into the corresponding choice box. In the dialog program "Change i-effect Module Data", parameters can now be modified.



The following options for the *FLATFILE module can be set

EDIFACT/FLATFILE->DB2:

Default EDI Inbound Library

See: "Additional Parameters of the *EDIFACT Module"

Default EDI Inbound Path

See: "Additional Parameters of the *EDIFACT Module"

Debug ?

See: "Additional Parameters of the *EDIFACT Module"

Counter

See: "Additional Parameters of the *EDIFACT Module"

DB2 -> EDIFACT/FLATFILE:

Default EDI Outbound Library

See: "Additional Parameters of the *EDIFACT Module"

Next Number

See: "Additional Parameters of the *EDIFACT Module"

File Prefix

See: "Additional Parameters of the *EDIFACT Module"

Default EDI Outbound Path

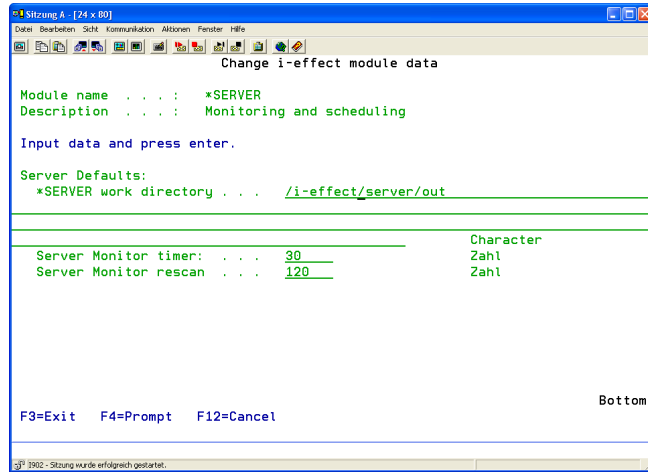
See: "Additional Parameters of the *EDIFACT Module"

Debug ?

See: "Additional Parameters of the *EDIFACT Module"

Additional Parameters of the *SERVER Module

Select the *SERVER module by entering option number 8 into the corresponding choice box. In the dialog program "Change i-effect Module Data", parameters can now be modified.



The following options for the *SERVER module can be set:

SERVER Defaults:

*SERVER Working Directory

This directory temporarily stores files that were generated in a server process and serve as source files for further server processes.

Default Path: /i-effect/<RELEASE>/server/out

Server Monitor Timer

Time between scans of IFS directories and DB2 libraries, both monitored by *MONITOR of the i-effect *SERVER module.

Server Monitor Rescan

Time passing until the same file is called again for processing when scanning IFS directories and DB2 libraries, both monitored by *MONITOR of the i-effect *SERVER module.

Backup Monitor Processing List

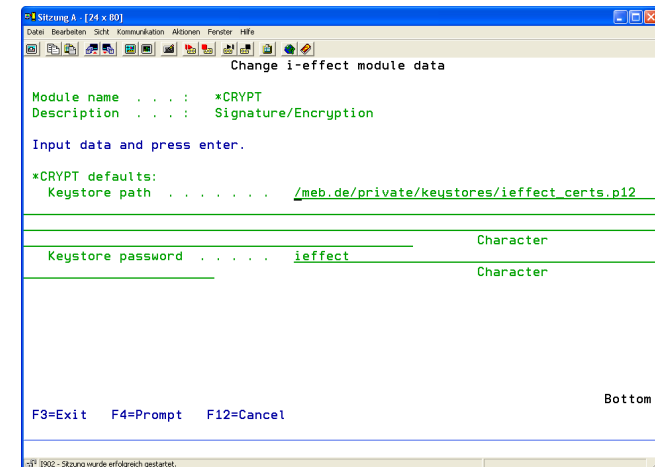
It can be specified here, if a list of files/file names currently being monitored will be backed up when EFFSERVER subsystems are shut down. This list will be used during the next start up to restore the file/processing list for every monitor. Double or multiple processing due to system restart can be avoided with this option.

*YES	Processing/ File lists will be backed up at shut-down.
*NO	Processing/ File lists will not be backed up at shutdown.

Please note: The file is reprocessed until it is either replaced or deleted from the monitored library/directory. This parameter only specifies the duration of the interval during which processed files existing in the library/directory are not processed.

Additional Parameters of the *CRYPT Module

Select the *CRYPT module by entering option number 8 into the corresponding choice box. In the dialog program "Change i-effect Module Data", parameters can now be modified.



The following options for the *CRYPT module can be set:

Keystore Path

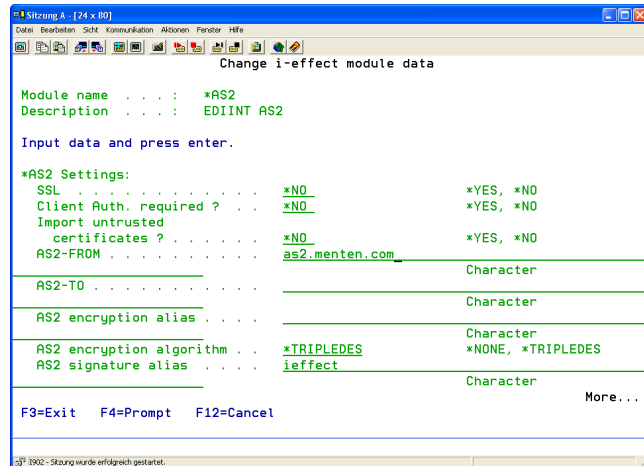
Path leading to the keystore. A keystore is a file in the PKCS_12 format where all required private and public keys/certificates are filed.

Keystore Password

The password to access the keystore. For security reasons, access to the keystore is only possible with the password. The default password of the provided keystore is „ieffect“

Additional Parameters of the *AS2 Module

Select the *AS2 module by entering option number 8 into the corresponding choice box. In the dialog program „Change i-effect Module Data“, parameters can now be modified.



The following options for the *AS2 module can be set:

SSL

This parameter determines the protocol to be used. Determine whether AS2 communication is to be established via SSL/HTTPS (Secure Socket Layer) or standard HTTP.

*YES	YES, the connection is established via SSL/HTTPS
*NO	NO, the connection is established via standard HTTP.

Use Client Authentication

If *YES is set in the “SSL” parameter, this parameter determines if the client sending an AS2 message must authenticate with its X.509 certificate to the AS2 server.

If *YES is set here and *NO is set in the previous parameter “Import Untrustworthy Certificates?”, the partner’s certificate must exist in the keystore before establishing a connection. By this, the partner’s certificate, automatically sent via an established HTTPS connection, can be verified by the AS2 server. The AS2 server only accepts the incoming connection after successful verification of the client’s certificate (check with certificate in the keystore). Otherwise, the connection will be closed due to the lack of proof that it is the partner sending an AS2 message.

If *NO is set in this parameter, certificate verification is not requested when establishing a connection.

*YES	Yes, client authentication is used.
*NO	No, client authentication is not used.

Please note: This form of SSL authentication is supported by only a few clients and is generally not common on the Internet.

Import Untrustworthy Certificates

If *YES is set in the “SSL” parameter, it is possible to allow the AS2 server to automatically import client certificates that do not exist in the keystore. Therefore, select *YES in this parameter. This might be a security risk inasmuch as every client is considered trustworthy due to automatic import of the client’s certificate into the keystore.

If *NO is set and the certificate does not exist in the keystore when a connection is established, the connection will automatically be closed. It is correct to abort the connection because the client’s identity cannot be verified due to the missing certificate in the keystore.

Automatic import of certificates into the keystore is only possible if the parameter “Use Client Authentication?” is set *YES.

- *YES Yes, untrustworthy client certificates are automatically imported.
- *NO No, untrustworthy client certificates are not automatically imported.

AS2-FROM

This is the distinct AS2 originator ID. It is inserted as sender into the outbound message. This ID enables the recipient to clearly identify the originator of the AS2 message.

AS2-TO

This parameter remains empty. It will be removed from one of the next versions.

AS2 Encryption Alias

This parameter remains empty. It will be removed from one of the next versions.

AS2 Encryption Algorithm

This parameter remains empty. It will be removed from one of the next versions.

AS2 Signature Alias

Enter the alias name of the key pair stored in the keystore. This key pair (more precisely: the private key) serves to digitally sign the AS2 message.

AS2 Signature Algorithm

Determine the default signature algorithm that is to be used to digitally sign the AS2 message.

- *MD5 The message is not signed.
- *SHA1 The message is signed with an MD5 signature algorithm (Message Digest 5).
- *NONE Default. The message is signed with an SHA1 signature algorithm (Secure Hash Algorithm 1).

AS2 Proxy Host

If a proxy server is used for AS2 communication, enter its IP address or DNS name here.

AS2 Proxy Port

If a proxy server is used for AS2 communication, enter its TCP/IP port here.

AS2 Proxy User ID

If a proxy server is used for AS2 communication, enter, if required, the user ID of the authorized user.

AS2 Proxy Password

If a proxy server is used for AS2 communication, enter, if required, the password of the authorized user.

Maximum Client Threads

Specify the maximum number of AS2 client (sending) processes that shall be processed contemporaneously.

AS2 Originator ID

The originator ID serves to define a clear message ID (in the form: <i-effect AS2 client-30092005092214+0200-0438@ieffect.com>) for outbound AS2 messages. It is recommended that you use your domain name because it is already clearly defined on the Internet. This ID will be transmitted in the header of the AS2 message.

AS2 Originator Email Address

An email address can be entered here. This address is transmitted in the headers of AS2 messages. Usually, the address of the EDI department or the AS2 contact person is used.

AS2 Originator Name

Enter either the official name of the organization, or company, or the name of the i-effect AS2 software will be used (default value). This field has just a descriptive character, its content is arbitrary. The parameter is not involved in receiving or sending processes. The name will be transmitted in the header of the AS2 message.

Maximum Send Retries

Specify the maximum number of attempts to retry to send an AS2 message. Send retry is started if the message was not sent due to an error (e.g. target system could not be reached).

Send Retry Pause

Determine the pause in seconds before the next attempt to connect is started.

Recommended value: 360 seconds.

Connection Timeout

The AS2 client waits until the set time has expired before connecting to a remote host (partner's server). If establishing a connection to the server fails after the indicated time (in seconds) has expired, the sending process will be canceled. After the set time in parameter "Send Retry Pause" has expired, the sending process will be repeated.

Recommended value: 120 seconds.

Read Timeout

After a connection to the partner's server has been established and data has been transmitted, the AS2 client waits until the set time has expired to receive an OK from the partner's server (HTTP status code 200). If the required OK is not received within the set time, the *AS2 module will send a timeout error notification. Regrettably, there is no general rule for the time to be set, only experience may help to define this value.

Recommended value: 120 seconds.

Internal Timeout

This parameter defines the AS2 client's internal processing timeout. The AS2 client waits the set time, for example in the case of processing bottlenecks, to try to process user defined tasks (prepare / send AS2 messages).

This parameter will be removed from one of the next versions. Please leave the value as it is.

Default Outbound Path

The default IFS path from which outbound data is selected.

Default Receive Path

The default IFS path where successfully transmitted data is stored. It can be overwritten when an AS2 server is defined.

Path for Received MDN

The default IFS path where received MDNs (Message delivery notifications) are stored. It can be overwritten when an AS2 server is defined.

Path for Sent MDN

The default IFS path where received MDNs (Message delivery notifications) are stored. It can be overwritten when an AS2 client is defined.

Path for Open MDN

The default IFS path where received data is temporarily stored until the requested MDN is transmitted. It can be overwritten when an AS2 client is defined.

Path for Received Headers

The default IFS path where headers of received AS2 messages are stored.

Path for Sent Headers

The default IFS path where headers of sent AS2 messages are stored.

Archive Inbound Messages?

This parameter determines if inbound data is to be stored in an archive directory immediately after being processed. (A copy of the generated file will be made.)

*YES YES, all received data is archived.

*NO NO, received data is not archived.

Archive Path

Default IFS path where received data is stored, if requested.

Archive Outbound Messages ?

This parameter determines if sent data is to be stored in an archive directory. (A copy of the generated file will be made.)

*YES YES, all sent data is archived.

*NO NO, sent data is not archived.

Archive Path

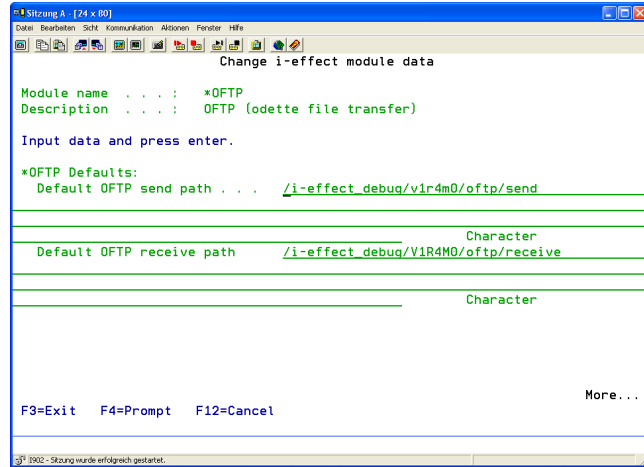
Default IFS path where sent data is stored, if requested.

Path for Erroneous Data

Default IFS path where erroneous inbound and outbound data is stored.

Additional Parameters of the *OFTP Module

Select the *OFTP module by entering option number 8 into the corresponding choice box. In the dialog program "Change i-effect Module Data," parameters can now be modified.



The following options for the *OFTP module can be set:

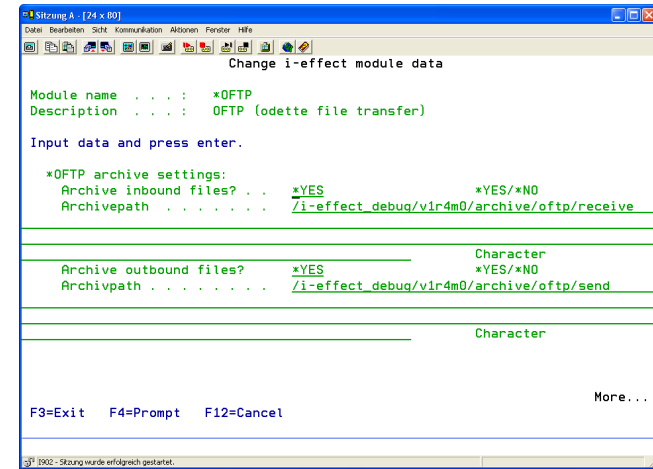
*OFTP Details

Default OFTP Outbound Path

Determine the directory where OFTP outbound files are stored. To increase performance of *OFTP, it should be an IFS path.

Default OFTP Inbound Path

Determine the directory where OFTP inbound files are stored. To increase performance of *OFTP, it should be an IFS path.



*OFTP Archive Settings

Archive Inbound Messages?

This parameter determines if inbound data will be archived automatically.

Possible values:

- *YES YES, inbound data is archived.
- *NO NO, inbound data is not archived.

Archive Path

Determine where inbound data will be archived. This might be an IFS or a DB2 path.

Archive Outbound Messages?

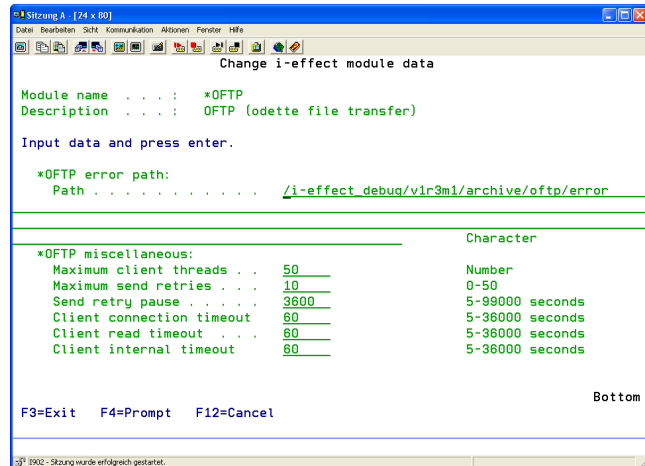
This parameter determines if outbound data will be archived automatically.

Possible values:

- *YES YES, outbound data is archived.
- *NO NO, outbound data is not archived.

Archive Path

Determine where outbound data is to be archived. This might be an IFS or a DB2 path.



```

Sitzung A: [24 x 80]
Datei Bearbeiten SCH Kommunikation Abkürzen Fenster Hilfe
Change i-effect module data
Module name . . . . : *OFTP
Description . . . . : OFTP (odette file transfer)
Input data and press enter.
*OFTP error path:
Path . . . . . /i-effect_debug/v1r3m1/archive/oftp/error

Character
*OFTP miscellaneous:
Maximum client threads . . 50          Number
Maximum send retries . . . 10          0-50
Send retry pause . . . . . 3600       5-99000 seconds
Client connection timeout . 60          5-36000 seconds
Client read timeout . . . . 60          5-36000 seconds
Client internal timeout . . 60          5-36000 seconds

Bottom
F3=Exit F4=Prompt F12=Cancel
2002 - Sitzung wurde erfolgreich gestartet.

```

OFTP Error*Path for Erroneous Data**

Determine the error directory where data can be stored in the case of extremely serious errors, if possible

OFTP Miscellaneous*Maximum Client Threads**

In order that the system is not overworked, this value determines the maximum number of client processes. If *OFTP overworks the system by using too many client instances, the value can be decreased.

Maximum Send Retries

This parameter determines the maximum number of send retries.

Send Retry Pause

Determines the pause in seconds before the next attempt to send is made.

Client Connection Timeout

This parameter determines the time in seconds that *OFTP waits for a reaction from remote side during connection establishment. After the indicated time has expired, the attempt to connect will be canceled.

Client Read Timeout

Timeout for reading data on an open data connection in seconds.

Client Internal Timeout

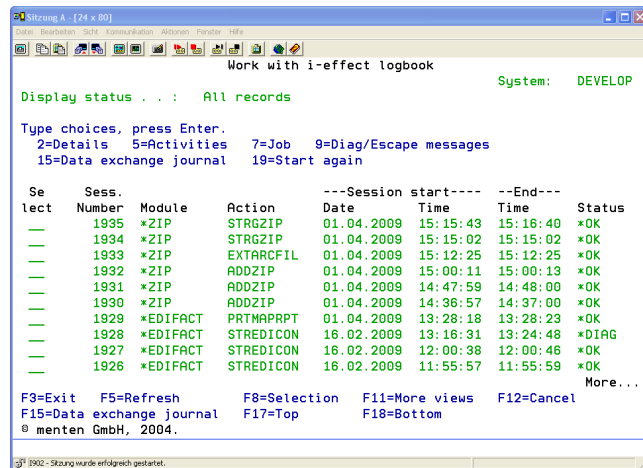
Internal timeout in seconds the OFTP client is given to respond to internal requests.

Logbook Functions

Menu Item 81: Work with Logbook (WRKEFFLOG)

To work with the logbook, select menu item 81 "Work with Logbook" or enter the command WRKEFFLOG in the i-effect main menu. While working in i-effect, pressing F13 opens the "Work with Logbook" dialog program.

The following display will appear:



```

Sitzung A: [24 x 80]
-----
Work with i-effect logbook
System:  DEVELOP

Display status . . . :  All records

Type choices, press Enter.
 2=Details  5=Activities  7=Job  9=Diag/Escape messages
15=Data exchange journal 19=Start again

Se lect  Sess.  Module  Action  ---Session start---  --End---  Status
-----  -----  -----  -----  -----  -----  -----
 1935  *ZIP  STRGZIP  01.04.2009  15:15:43  15:16:40  *OK
 1934  *ZIP  STRGZIP  01.04.2009  15:15:02  15:15:02  *OK
 1933  *ZIP  EXTARCFIL  01.04.2009  15:12:25  15:12:25  *OK
 1932  *ZIP  ADDZIP  01.04.2009  15:00:11  15:00:13  *OK
 1931  *ZIP  ADDZIP  01.04.2009  14:47:59  14:48:00  *OK
 1930  *ZIP  ADDZIP  01.04.2009  14:36:57  14:37:00  *OK
 1929  *EDIFACT  PRTHAPRPT  01.04.2009  13:28:18  13:28:23  *OK
 1928  *EDIFACT  STREDICON  16.02.2009  13:16:31  13:24:48  *DIAG
 1927  *EDIFACT  STREDICON  16.02.2009  12:00:38  12:00:46  *OK
 1926  *EDIFACT  STREDICON  16.02.2009  11:55:57  11:55:59  *OK
More...

F3=Exit  F5=Refresh  F8=Selection  F11=More views  F12=Cancel
F15=Data exchange journal  F17=Top  F18=Bottom
© menten GmbH, 2004.
1002 - Sitzung wurde erfolgreich gestartet.

```

The i-effect logbook serves as central area for documentation of all i-effect processes. All processes are arranged chronologically and supplemented with comprehensive detailed information. Contents may be filtered using the appropriate options.

Options

The dialog program displays a list of all logbook entries. The following details are listed for every i-effect session number:

- The i-effect module that was used for the designated session.
- Starting date and time of the session.
- Ending date and time of the session.
- Final status of the session.
- The i-effect action that was executed.

The following status values are possible:

- OK** The session was successfully closed without any error.
- ACTIVE** The session is currently active. The final status will be recorded when the session is ended. Use option F5 "Refresh" to refresh the statuses and display the final status of the session
- ESCAPE** During the session a fatal error occurred that led to the abort of the session. The exact cause for the error and advice how to proceed are to be found in "Setting Activities" (option 5) as well as in the session's job protocol (option 7).
- DIAGNOSIS** The session was normally closed but the i-effect control routine received one or more diagnostic messages, which are the reason for this final status. However, the causes were not serious enough for i-effect to have aborted the session. "Setting Activities" (option 5) as well as in the session's job protocol (option 7) contain further information about the diagnostic messages.
- WAIT** Special value for the *AS2 module marking that an asynchronous MDN is still expected.

The following overview describes the available options of the dialog program. Enter the option number in the choice box at the beginning of the line of the corresponding session.

Option 2 – Display i-effect Session Details

The following dialog program displays the details of the selected i-effect session.

Option 5 – Work with i-effect Actions

```

Sitzung A [24 x 80]
Datei Bearbeiten Such Kommunikation @Horen Fenster Hilfe
Work with i-effect actions
System: I5EFFECT

Session number . . . : 334      Filtered
Type choices, press Enter.
5=Message details

Se      lect  Time   Sev.   Activity
shortdescription
-      -      -      -      -
12:19:12 0     i-effect processing started.
12:19:13 0     Preparing signing of file "/sigg/pdf_in/*", type "*PDF",
12:19:13 0     PDF signature selected
12:19:13 0     Signature job added. Waiting for finalisation
12:19:15 0     Signature job successful completed by slot "1"
12:19:15 0     i-effect processing finished.

Bottom
F3=Exit      F5=Refresh   F8=Selection  F9=Diagnostic/cancel messages
F11=More views F12=Cancel  F17=Top       F18=Bottom
© menten GmbH, 2004.
  
```

This display lists all details of an i-effect session. All activities of an executed i-effect command are logged in the i-effect logbook. The table entries are in chronological order and display all messages recorded while the program is run.

Available Information:

1. Session number of the selected session.
2. Time when the action was executed.
3. Message priority. Possible 2-digit values: 00 to 99. The higher the value, the higher the priority.
4. Short description of the activity.

Use option 5 “Message Details” in the corresponding choice box to display further details or explanations for this message.

Option 7 – Display System i Job (DSPJOB)

Using this option, the IBM System i Job log (DSPJOB) for the selected job, in which the session was run, is called up. If this job still exists on the system, because it is still active or the job protocol is still in an output queue, all relevant information for the program run can be retrieved.

Option 9 – Diagnosis/Escapes Messages

Available information:

- i-effect session number.
- Point in time when the action was recorded. (The timestamp of the system clock is valid.)
- Message number.
- Short message text.
- Detailed description of the converter activity.

Option 15 – Data Exchange Protocol

Available information:

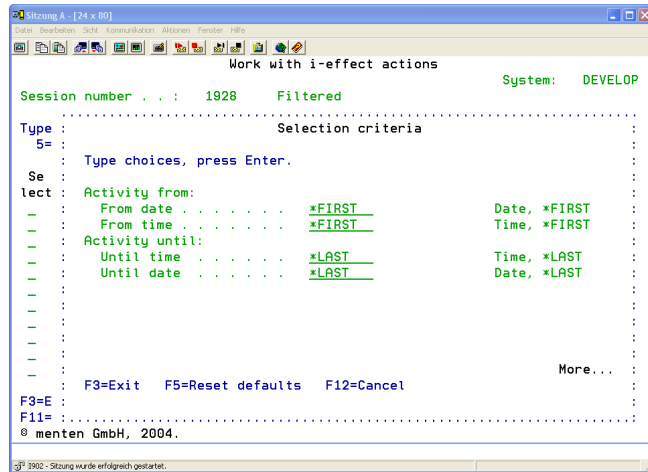
- Date and time when the action was recorded. (The timestamp of the system clock is valid.)
- Original file, archive file.
- AS2 header and AS2 MDN, if needed.
- Target address.

Option 19 – Start again

With this option, a job that is protocolled in the logbook can be executed again. It is possible to specify this job’s parameters in the dialog program.

Logbook Filter Function

Use option F8 to filter the displayed information by means of numerous selection criteria.



The following selection criteria are available:

Session

From Number

Enter a value in this field to filter the information in the list according to session number.

Possible special value:

**FIRST* Display from the beginning of the logbook (most current entry)

To Number

Enter a value in this field to filter the information in the list according to session number.

Possible special value:

**LAST* Display to the end of the logbook (last entry)

Session Start Begin

From Date

Enter a value in this field to filter the information in the list according to session starting date.

Possible special value:

**FIRST* Display from the date of the first action.

From Time

Enter a value in this field to filter the information in the list according to session starting time.

Possible special value:

**FIRST* Display from the starting time of the first action.

Session Start End

To Date

Enter a value in this field to filter the information in the list according to session starting date.

Possible special value:

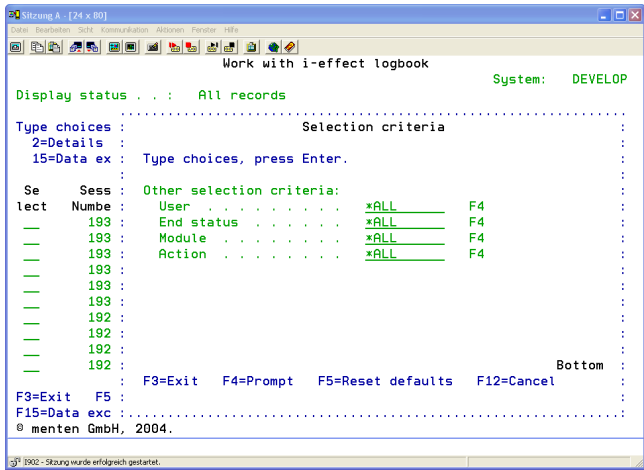
**LAST* Display to the date of the last action.

To Time

Enter a value in this field to filter the information in the list according to session starting time.

Possible special value:

**LAST* Display to the ending time of the last action.



Other

User

Enter a value in this field to filter the information in the list according to username. Press F4 to display a list of all available usernames.

Final Status

Enter a value in this field to filter the information in the list according to final status.

Possible values are:

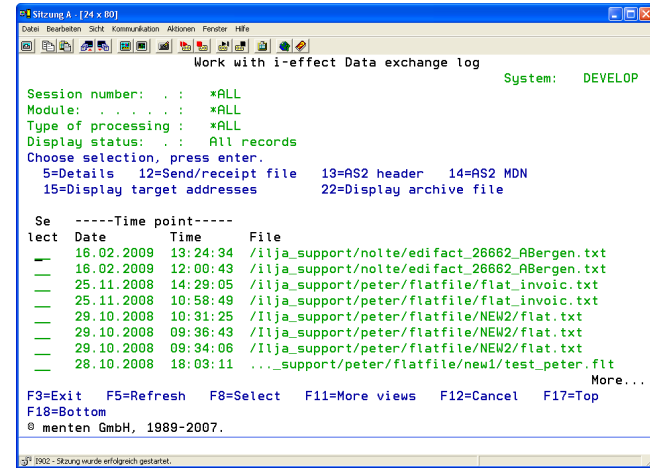
- *ALL The information in the list is not filtered according to final status.
- *OK Only sessions with the final status *OK will be listed.
- *ESCAPE Only sessions with the final status *ESCAPE will be listed.

Module

Enter a value in this field to filter the information in the list according to modules. Press F4 to display a list of all available modules.

Logbook Data Exchange Protocol

Press F15 to display all sent or received files.

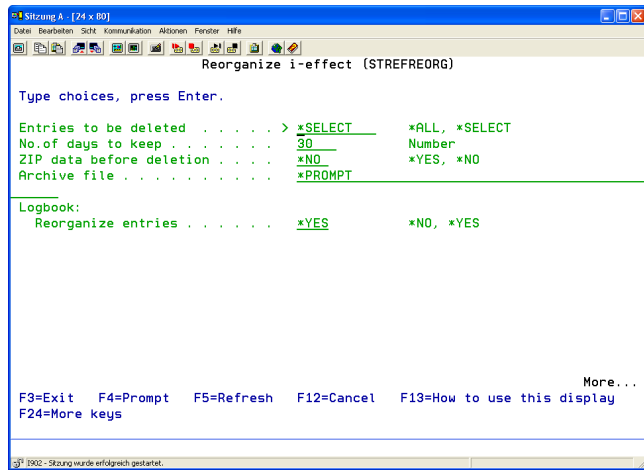


Menu Item 83: Reorganize i-effect (STREFREORG)

The command STREFREORG can organize all logbook files, archive directories, and internal protocols generated by i-effect. It is possible to either delete all files or select files to be deleted.

When selecting files, a period of days can be entered. Log data will not be reorganized until the starting point of the period. Furthermore, it is possible to save logbook files, archive directories and internal protocols in an i-effect archive before reorganization is started.

Please note: the RMVEFFLNK command. The RMVEFFLNK command organizes data in any IFS directory. For process automation, go to menu item 40 "Work with i-effect server" in the i-effect main menu.



Entries to be deleted

This parameter determines the entries to be deleted.

- *ALL** The content of all logbook files, all files in archive directories, and all internal protocols will be deleted.
- *SELECT** Entries in logbook files, IFS files in archive directories, and internal protocols older than the number of days specified in parameter "Day" will be deleted.

Days (not being deleted)

Entries in logbook files, IFS files in archive directories, and internal protocols NOT older than the number of days specified in this parameter will NOT be deleted. Other entries and files will be removed from the logbook.

Archive Logbook data

Determines if logbook files, archive directories, and internal protocols will be archived in an i-effect archive before reorganization. In order to keep DDS data, logbook files will be saved in a backup file before archiving.

Possible special values:

- *YES** YES, all i-effect data to be reorganized is saved.
- *NO** NO, i-effect data to be reorganized is not saved.

Archive File

The qualified name of the archive file, e.g. /tmp/test.zip.

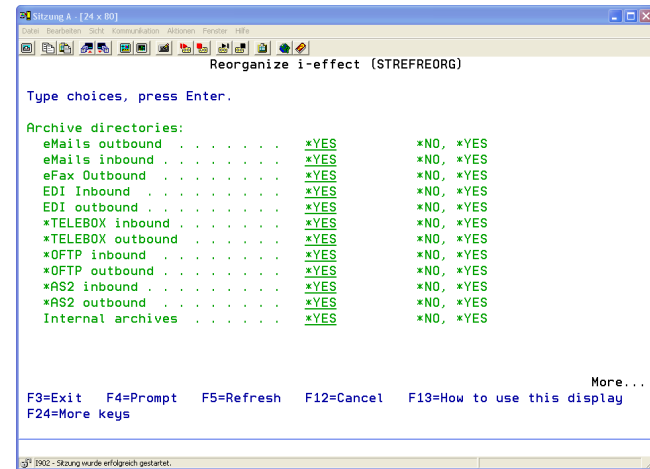
Possible special values:

- *PROMPT** With the i-effect command ADDARCFIL it will be requested to enter an archive file name.

Logbook

Choose whether logbook entries will be reorganized or not.

- *YES** YES, logbook entries are reorganized.
- *NO** NO, logbook entries are excluded from reorganization.



Archive Directories

Choose the directories to be reorganized.

- *YES** YES, files in this directory will be reorganized.
- *NO** NO, files in this directory will not be reorganized.

The following archive directories can be selected:

Emails outbound/inbound, eFax outbound, EDIFACT inbound/outbound, *FLATFILE inbound/outbound, *TELEBOX inbound/outbound, *OFTP inbound/outbound, *AS2 inbound/outbound, internal archives

Internal Protocols

Choose the internal protocols to be reorganized.

- *YES YES, files in this protocol will be reorganized.
- *NO NO, files in this protocol will not be reorganized.

The following internal protocols can be selected:

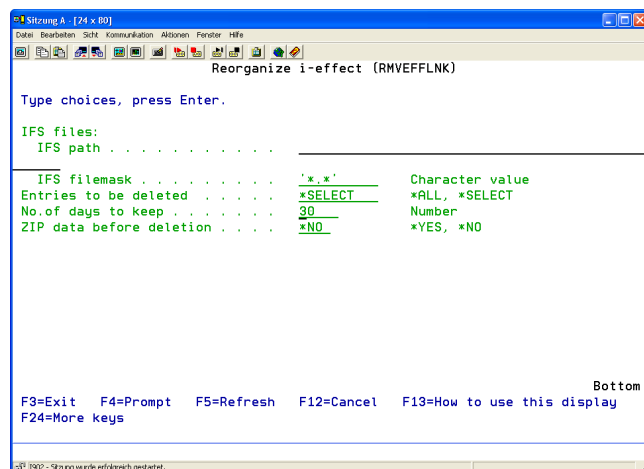
Email protocol file, server working directories, other work files.

Remove no longer required Files (RMVEFFLNK)

The command RMVEFFLNK can remove or archive any IFS files. It is possible to either delete all files or select files to be deleted.

If selecting files is desired, a period in days can be entered. Log data will not be reorganized until the starting point of the period.

Furthermore, it is possible to save file in a ZIP archive before deletion.

**IFS Path**

Enter the IFS path. Use the "&" character to enlarge the input field.

IFS Filemask

Enter the search pattern. Use the "&" character to enlarge the input field.

Entries to be deleted

This parameter determines the entries to be deleted.

- *ALL All files in the selected IFS directories will be deleted.
- *SELECT IFS files being older than the number of days specified in parameter "Day" will be deleted.

Days (not being deleted)

IFS files NOT older than the number of days specified in this parameter will NOT be deleted. Other entries and files will be removed from the logbook.

Save in ZIP Archive before removing

Determines if the selected files will be saved in a ZIP archive before deletion.

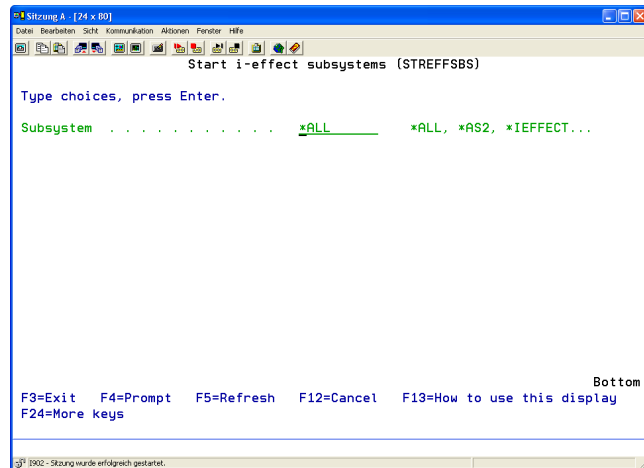
- *YES YES, selected files will be saved before deletion.
- *NO NO, selected files are not saved before deletion.

i-effect Sub Systems

Menu Item 85: Start i-effect Sub Systems (STREFFSBS)

Select menu item 85 in the i-effect main menu to start sub systems.

The following display will appear:



Use this dialog program to start all or individual i-effect sub systems. This will no longer be necessary after version V1R3M1, because the required sub systems will be started automatically.

Sub System

Enter the sub system that is to be started.

The following values – depending on the modules be licensed – are possible:

- *ALL All i-effect sub systems are started.
- *AS2 The i-effect AS2 sub system is started.
- *IEFFECT The i-effect IEFFECT sub system is started.
- *SERVER The i-effect SERVER sub system is started.

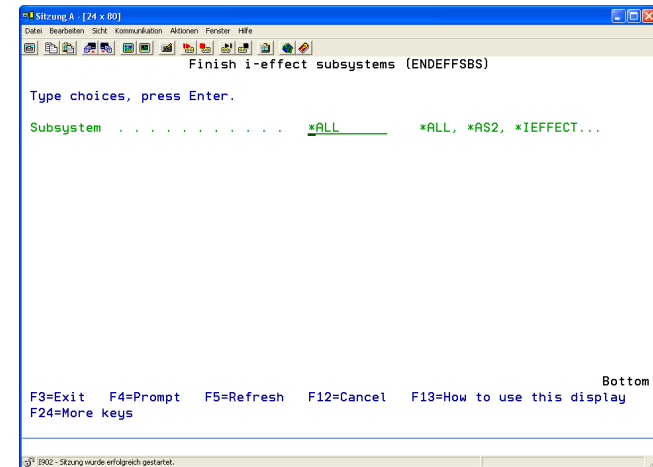
*TELEBOX The i-effect TELEBOX sub system is started.

*OFTP The i-effect OFTP sub system is started.

Menu Item 86: End i-effect Sub Systems (ENDEFFSBS)

Select menu item 86 in the i-effect main menu to end sub systems

The following display will appear:



Use this dialog program to end all or individual i-effect sub systems.

Sub System

Enter the sub system that is to be ended.

The following values – depending on the modules be licensed – are possible

- *ALL All i-effect sub systems are ended.
- *AS2 The i-effect AS2 sub system is ended.
- *IEFFECT The i-effect IEFFECT sub system is ended.

- **SERVER* The i-effect SERVER sub system is ended.
- **TELEBOX* The i-effect TELEBOX sub system is ended.
- **OFTP* The i-effect OFTP sub system is ended.