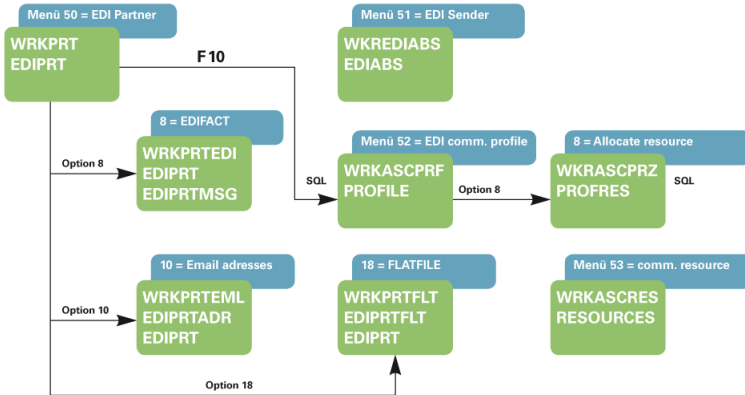


Chapter 10

Master Data in i-effect

i-effect V1R4M0 Master Data



At this point, master data being relevant for the functions of i-effect can be managed.

This chapter includes the following i-effect menu items:

- o Menu item 50 EDI partner master data (WRKPRT)
- o Menu item 51 EDI sender partner master data (WKREDIABS)
- o Menu item 52 EDI communication profiles (WRKASCPRF)
- o Menu item 53 EDI communication resources (WRKASCRES)

The section

- o user authentication for communication servers

contains information about creation of user accounts for login on i-effect servers. On the one hand, these accounts serve to identify the communication partner; on the other hand, they serve the security of externally accessed communication servers.

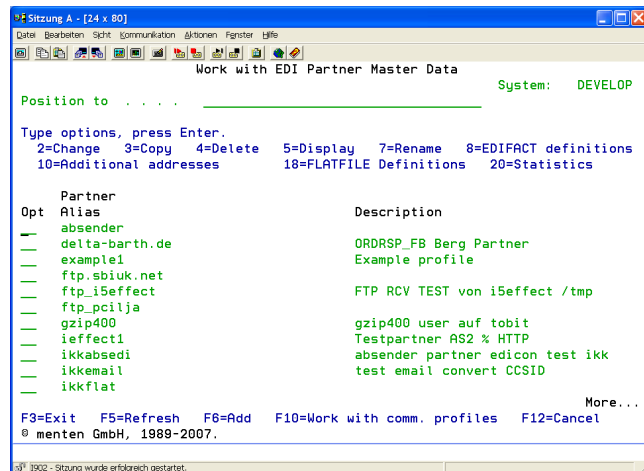
Master Data for Communication

Communication master data is a central area in i-effect to store data that is used for repeatedly occurring communication tasks.

Menu item 50: Work with EDI Partner Master Data

This program interface manages master data of communication partners with whom data is interchanged. The entries made here serve the transaction of data communication with business partners. Call up the program interface for partner master data administration by selecting menu item 50 in the i-effect main menu.

The following display will appear:



Dialog Program 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. The following overview describes the available options of the program interface, followed by a more detailed description.

Add (option F6)	Use option F6 (function key F6) to add a new partner. In the appearing program interface, choose an alias name for the partner. Then, further data required for communication with this partner can be entered.
Change (option 2)	To change an entry, use option 2 in the corresponding choice box. The partner's data concerning the installed modules will be displayed and can be modified according to new specifications.
Copy (option 3)	To copy an existing entry to a new alias name, use option 3 in the corresponding choice box.
Delete (option 4)	To delete an entry, use option 4 in the corresponding choice box.
Display (option 5)	To display an entry, use option 5 in the corresponding choice box.
Rename (option 7)	To rename an entry, use option 7 in the corresponding choice box.
EDIFACT definitions (option 8)	To edit an entry's details needed for EDIFACT communication, use option 8 in the corresponding choice box. To enter these details, a new dialog will open.
Additional addresses (option 10)	To add email, fax or SMS addresses to an entry, use option 10 in the corresponding choice box. To enter these addresses, a new dialog will open.
FLATFILE definitions (option 18)	To edit an entry's details needed for FLATFILE communication, use option 18 in the corresponding choice box. To enter these details, a new dialog will open.
Statistics (option 20)	To display EDIFACT and FLATFILE specific statistics for a partner, use option 20 in the corresponding choice box.

Details: F6=Add, 2=Change, 5=Display

Using options F6=Add, 2=Change or 5=Display, the following display will appear.

Screenshot of the 'Input/change partner data' screen. The 'Send' section is visible, showing the following data:

CCSID send	1252	*JOB, 0-65535
DB2 Insert CRLF	*NO	*YES, *NO
DB2 Remove blanks	*NO	*YES, *NO

Other visible fields include: Partner alias: menten, Primary communication profile: 190, Description: menten GmbH.

Partner Alias

The alias name of this address entry. The partner alias is a short reference for the partner definition. It can be used in commands to refer to partner master data details.

Primary Communication Profile

Enter the communication profile related to this entry here. This profile will only be used by the command SNDFILE. The EDIFACT data will be sent by SNDFILE using this defined primary communication profile. For further information concerning SNDFILE, see Chapter 6 Communication, "EDI Communication".

Description

A brief description of the partner can be created here. Using the partner's official name is recommended. In contrast to the alias, which serves as a key for the partner master data, this field has just a descriptive character, its content is arbitrary.

Send

CCSID

Enter the CCSID (Coded Character Set Identifier) for outbound files. If these files are not included in the CCSID, they will be converted automatically.

Insert DB2 CRLF

Determine if a CRLF control character should be inserted at the end of each dataset (end of line) for outbound DB2 database files.

Delete DB2 Subsequent Blanks

Determine if subsequent blanks at the end of each dataset in DB2 database files should be deleted before transmission.

Screenshot of the 'Input/change partner data' screen. The 'Receive' section is visible, showing the following data:

IFS CCSID	1252	*JOB, 0-65535
DB2 CCSID	1252	*JOB, 0-65535
DB2 Record length	*AUTO	1-32766, *AUTO
Receive path text	*DEFAULT	

Other visible fields include: Partner alias: menten, Receive path attachment: *DEFAULT.

Receive

IFS CCSID

Enter the CCSID (Coded Character Set Identifier) for received files. Received files will be saved in the IFS under this CCSID and will not be converted.

DB2 CCSID

Enter the CCSID (Coded Character Set Identifier) for received files that are to be saved in the DB2. These files' CCSID will be converted to the database's CCSID before they are saved.

Remarks on IFS and DB2 CCSID:

Character Set

The default is *JOB. A character conversion will not happen if *JOB is indicated. Data is received in the EBCDIC code page of the current job (on German IBM System i it is code page 273). Any code page ID supported by IBM System i can be entered into this field. The system will convert the received data into the indicated destination code page.

Typical CCSID values are:

273	(EBCDIC Germany)
273	(EBCDIC England/America)
1252	(ASCII Windows)
850	(ASCII DOS)

Possible special value:

*JOB The job's CCSID is used.

DB2 Record Length

The maximum record length for DB2 datasets can be defined here. Using the special value *AUTO, the length of the dataset will be defined automatically on the basis of the data, if possible.

Receive path text

Enter the path where inbound files of the type "Text" are to be saved by default.

Receive path attachments

Enter the path where inbound files of the type "Attachment" are to be saved by default.

In the default setting, data received as "text" or "attachment" will be filed in an IFS path. After installation of the product, this path will be /i-effect/telebox/receive. It can be overwritten and adapted to personal needs, e.g. partner individual reception directories.

To file data in a physical file in the DB2, enter the name of the reception library as follows:

/QSYS.LIB/<name of library>.LIB

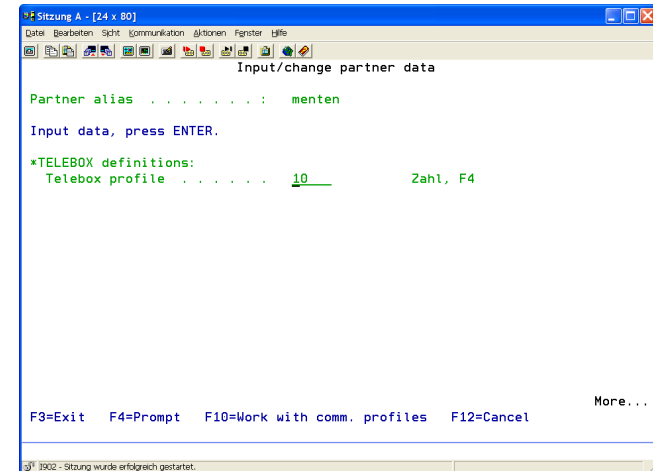
By indicating the following format, an individual prefix can be assigned to the physical file that is to be generated. In the following example, data will be filed in the library MYLIB. Every file must have the prefix VK.

/QSYS.LIB/MYLIB.LIB/VK.FILE*

For instance, if a file called SALES.TXT is received it gets the name VKSALES in the library MYLIB.

Note: When creating a name for the received file in a library, it will be shortened to 10 characters. If a file under this name already exists in the library, a clear serial number will be added to the shortened name, e.g. VKSALES turns into VKSALES1. If the file is filed in an IFS directory and the name already exists, i-effect generates an unambiguous name by annexing a serial numerical suffix, e.g. SALES.TXT turns into SALES_1.TXT.

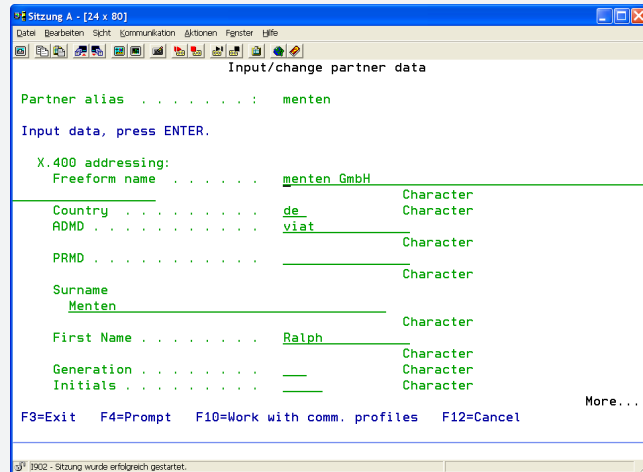
In addition to the preceding parameters, the Add/Change/Display display will only show the parameters of the installed modules. Hereafter, their specific parameters are described.



Partner Master Data for the *TELEBOX Module

Telebox Profile

In order to assign data to an i-effect profile (and therefore to a Telebox partner to connect with), enter the number of the i-effect profile describing this partner. Use function key F4 to display a list of profiles defined in the system.



```

Sitzung A - [24 x 80]
Datei Bearbeiten Sicht Kommunikation Aktionen Fenster Hilfe
-----
Input/change partner data

Partner alias . . . . . : menten

Input data, press ENTER.

X.400 addressing:
Freeform name . . . . . : menten GmbH
-----
Country . . . . . : de_ Character
ADMD . . . . . : viat Character
PRMD . . . . . : Character
Surname
Menten Character
First Name . . . . . : Ralph Character
Generation . . . . . : Character
Initials . . . . . : Character
-----
More...

F3=Exit F4=Prompt F10=Work with comm. profiles F12=Cancel
1902 - Sitzung wurde erfolgreich gestartet.

```

X.400 Addressing:

Freeform name:

Name of the addressee. Enter a descriptive name of the X.400 partner.

Country:

Country key. The usual X.400 abbreviation for this field is "C".

ADMD:

ADMD stands for Administration Management Domain. The usual X.400 abbreviation for this field is "A".

PRMD:

PRMD stands for Private Management Domain. The usual X.400 abbreviation for this field is "P".

Surname:

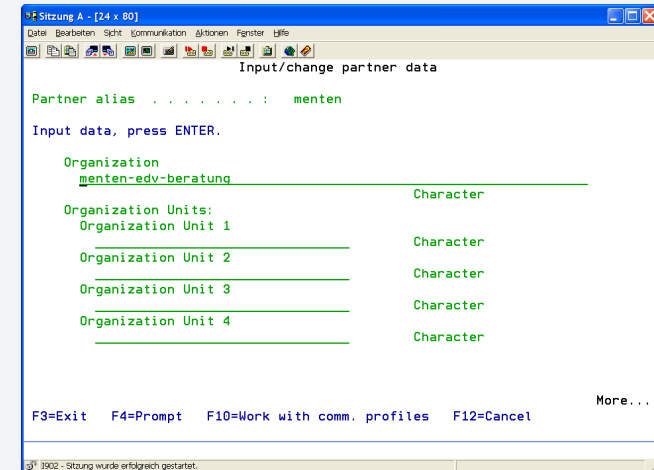
Enter the recipient's surname. The usual X.400 abbreviation for this field is "S".

First name:

Enter the recipient's first name. The usual X.400 abbreviation for this field is "G".

Generation:

Enter the abbreviation of the recipient's name suffix. The usual X.400 abbreviation for this field is "GN".



```

Sitzung A - [24 x 80]
Datei Bearbeiten Sicht Kommunikation Aktionen Fenster Hilfe
-----
Input/change partner data

Partner alias . . . . . : menten

Input data, press ENTER.

Organization
menten-edv-beratung Character
-----
Organization Units:
Organization Unit 1 Character
Organization Unit 2 Character
Organization Unit 3 Character
Organization Unit 4 Character
-----
More...

F3=Exit F4=Prompt F10=Work with comm. profiles F12=Cancel
1902 - Sitzung wurde erfolgreich gestartet.

```

Initials:

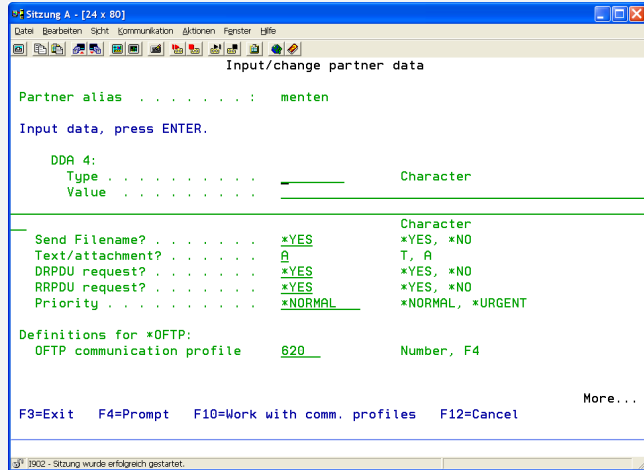
Enter the partner's initials. The usual X.400 abbreviation for this field is "I".

Organization:

Specifications about the organization. The usual X.400 abbreviation for this field is "O".

Organization Unit 1 to 4:

Enter the organization units. The usual X.400 abbreviation for these fields is "OU".



DDA 1 to 4:

Type:

One of four possible DDA definitions (Direct Distribution Attribute). The usual X.400 abbreviation for DDA definitions is "DDA".

Value:

Definition of a value being displayed together with the corresponding DDA type entry, i.e. the one having the same number. Both are required and must be defined together.

Send File Name?

When sending attachments via the interface, it might be preferable (depending on the recipient) to suppress the transmission of the file name. In certain cases, the forwarding ADMD generates an additional text bodypart for the file name, which can cause processing problems on the recipient's side. Use this parameter to suppress the transmission of the file name.

Options are:

- *YES Yes, the file name is transmitted.
- *NO No, the file name is not transmitted.

Text/Attachment?

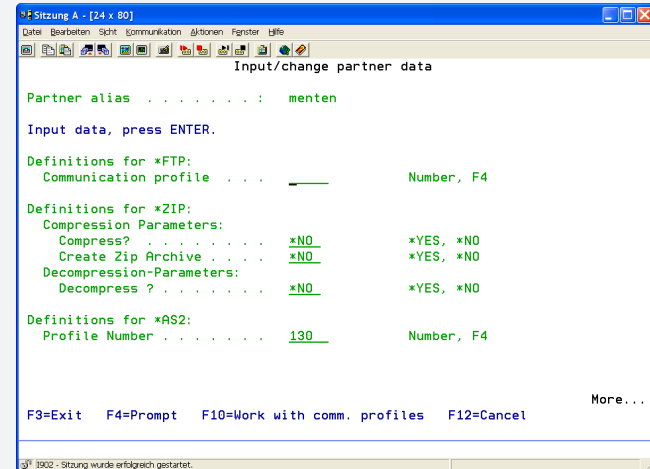
Determine whether text or attachment is to be processed.

DRPDU Request?

Determine if a DRPDU transmission confirmation (delivery report data unit) is necessary.

RRPDU Request?

Determine if a RRPDU confirmation of receipt (receipt report data unit) is necessary.



Priority:

Determine the priority of the communication of this entry. Choose either *URGENT or *NORMAL.

Partner Master Data for the *OFTP Module

OFTP Communication Profile:

In order to assign data to an i-effect profile (and therefore to an OFTP partner to connect with), enter the number of the i-effect profile describing the remote OFTP partner. Use function key F4 to display a list of profiles defined in the system.

Partner Master Data for the *FTP Module

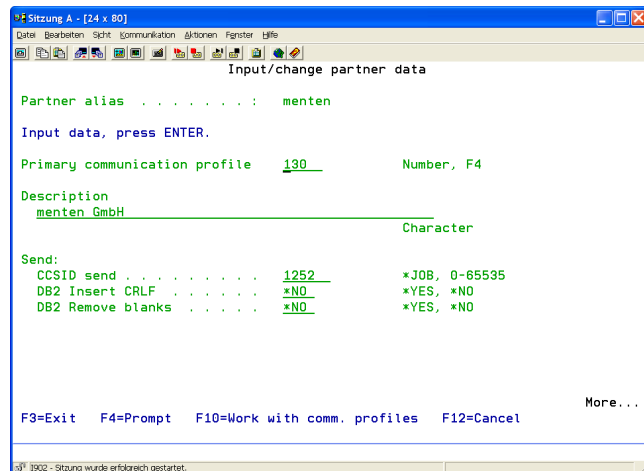
FTP Communication Profile:

In order to assign data to an i-effect profile (and therefore to an FTP partner to connect with), enter the number of the i-effect profile describing the remote FTP server. Use function key F4 to display a list of profiles defined in the system.

Partner master data for the *AS2 Module

Reception Path Attachment

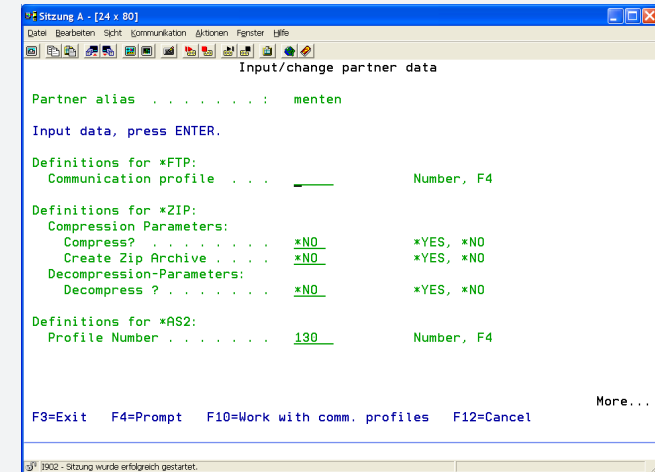
AS2 messages sent by a partner will be filed here. The directory/library defined by the parameter "Reception Path Text" is not used by AS2.



Profile Number:

Enter an AS2 communication profile (sending profile) for this entry.

In order to assign data to an i-effect profile (and therefore to an AS2 partner to connect with), enter the number of the i-effect profile describing the remote AS2 server. Use function key F4 to display a list of profiles defined in the system.



Please note: An AS2 communication profile is NEVER assigned to several partners at the same time. The link between partner and a sending profile forms a one-to-one relation. When receiving AS2 messages, the partner will be assigned in the opposite direction. It will be checked which partner is assigned to a certain AS2 sending profile. If the AS2 sending profile is assigned to several partners, a clear identification of the partner is not possible.

Partner Master Data for the *EMAIL Module

Email Profile:

In order to assign data to an i-effect profile (and therefore to an email partner to connect with), enter the number of the i-effect profile describing the email partner. Use function key F4 to display a list of profiles defined in the system.

SMTP Encryption Alias

Alias name under which the key is stored in the keystore.

SMTP Encryption Algorithm

Algorithm by which the message is encrypted.

<i>*DEFAULT</i>	The algorithm is taken from the *EMAIL module's default setting (menu item 80).
<i>*NONE</i>	The email is not encrypted.
<i>*TRIPLEDES</i>	The email is encrypted by a Triple-DES algorithm (3 x 56 bits).

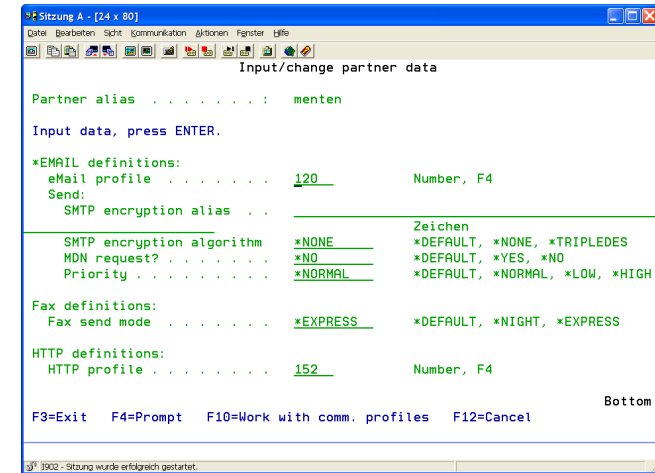
MDN Request?

Determine if an MDN (Message Delivery Notification) is needed.

Priority:

Specify the priority of the email.

<i>*DEFAULT</i>	The priority is taken from the default setting of the *EMAIL module (menu item 80).
<i>*NORMAL</i>	The email is sent with normal priority.
<i>*HIGH</i>	The email is sent with high priority.
<i>*LOW</i>	The email is sent with low priority.



For a variable control of email addresses, recipient, CC and BCC addresses can be stored for every partner. If a partner in "Recipient Partner ID" is specified in the command SNDEMAIL (alternatively: i-effect main menu 13, then menu item 30), an email will be sent to all addresses defined for this partner.

In the same manner, emails can be received and filed according to the partner sender addresses that are stored in the corresponding partner profile. When receiving emails with the command RCVEMAIL (alternatively: i-effect main menu 13, then menu item 31), the sender address of every email will be compared with the sender addresses stored in the partner master data. If the addresses match, the email will be assigned to the respective partner and partner definitions (path, CCSID, etc.) will be used for receiving.

Partner Master Data for the *FAX Module

Fax Send Mode

Specify the priority of the fax.

<i>*DEFAULT</i>	The priority is taken from the *FAX module's default setting.
<i>*NIGHT</i>	The fax is sent with cost-effective low priority (night rate).
<i>*EXPRESS</i>	The fax is sent immediately with high priority (day rate)

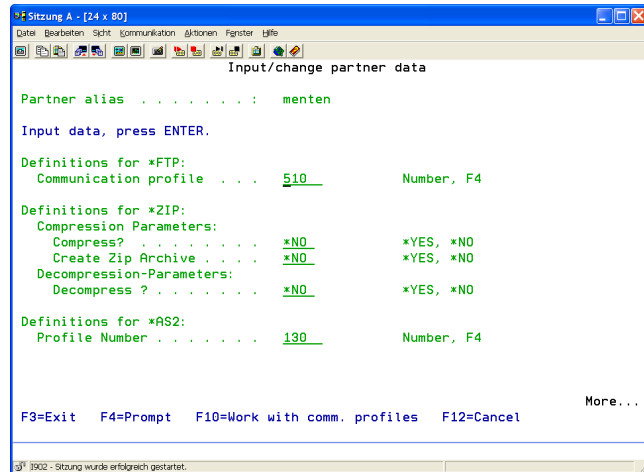
Partner Master Data for the *HTTP Module

HTTP Profile:

In order to assign data to an i-effect profile (and therefore to an HTTP partner to connect with), enter the number of the i-effect profile describing the remote HTTP server. Use function key F4 to display a list of profiles defined in the system.

Partner Master Data for the *FTP Module

The following details describe the parameters that are only available if the *FTP module is installed.

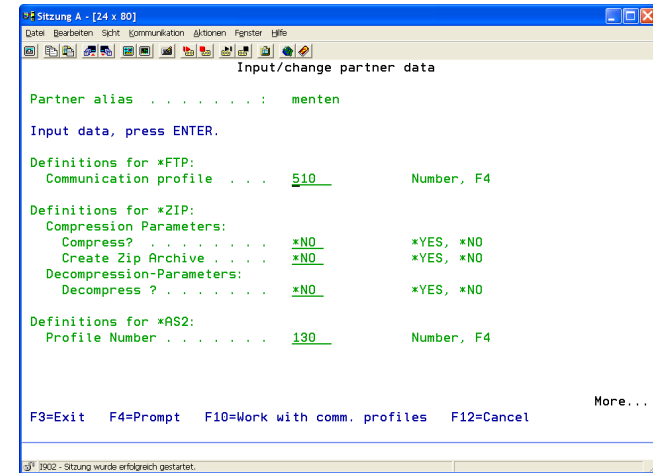


Communication Profile

In order to assign data to an i-effect profile (and therefore to an FTP partner to connect with), enter the number of the i-effect profile describing the remote FTP server. Use function key F4 to display a list of profiles defined in the system.

Partner Master Data in the *ZIP Module

The following describes the parameters that are only available if the *ZIP module is installed.



Compression Parameter:

Compress?

Determines if outbound data is to be compressed automatically with i-effect for the designated partner.

- | | |
|------|---------------------------------------|
| *YES | Yes, data will be compressed. |
| *NO | No, send data will not be compressed. |

Create ZIP archive:

By compression, either a gzip file or a ZIP archive will be created.

- | | |
|------|---|
| *YES | Yes, a ZIP archive will be created. |
| *NO | No, a simple gzip file will be created. |

Decompression Parameter:

Decompress?

Determines if received data is to be decompressed automatically with i-effect for the designated partner.

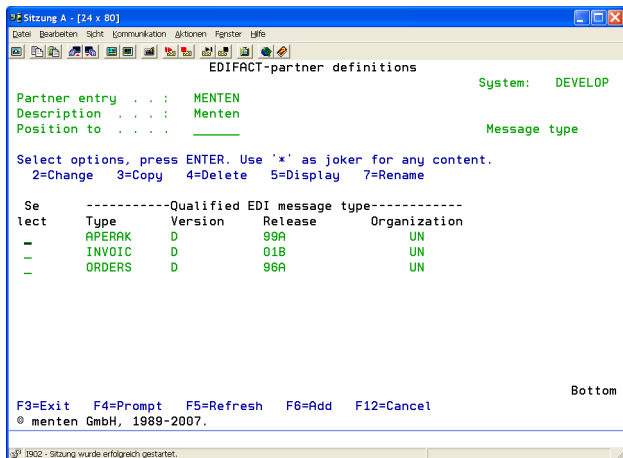
Possible values:

- *YES Yes, data is decompressed
- *NO No, send data is not decompressed.

Please note: when using the *AS2, *EMAIL, *HTTP *FTP and *TELEBOX modules with GZIP compression: If a partner is recognized/specified for sending/receiving, the ZIP settings will be used for the sent/received file(s). If specified, all input files packed by GZIP, and all files received will be automatically unpacked.

Details: 8=EDIFACT Definitions

Using option 8, an overview of all message types assigned for this partner will be displayed. Message types that can be processed for this partner can be specified. Every received or outbound message will be checked by i-effect whether this message type is enabled for this partner. If not, conversion will not be effected.



Add (option F6)

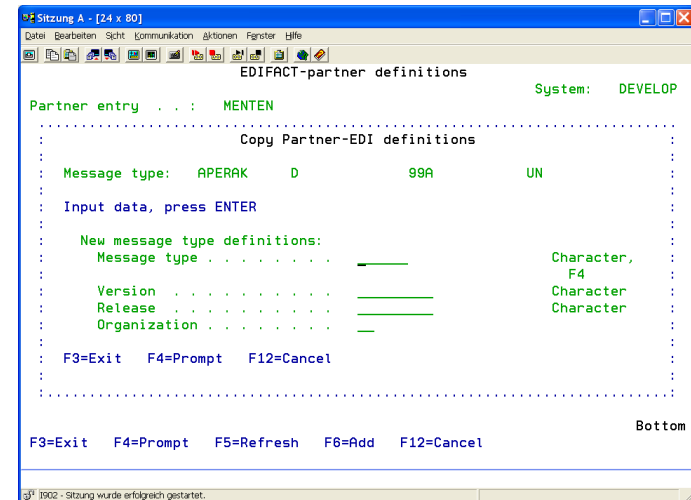
Use option F6 (function key F6) to create a new entry. In the appearing program interface, enter further required data.

Change (option 2)

To change an entry, use option 2 in the corresponding choice box. The partner's data concerning the chosen message type will be displayed and can be modified.

Copy (option 3)

To copy the existing entry, use option 3 in the corresponding choice box.



In the following display, fill in the key fields for the entry to be created. Press enter and the copied entry will be filed under the new message type.

Delete (option 4)

To delete an entry, use option 4 in the corresponding choice box.

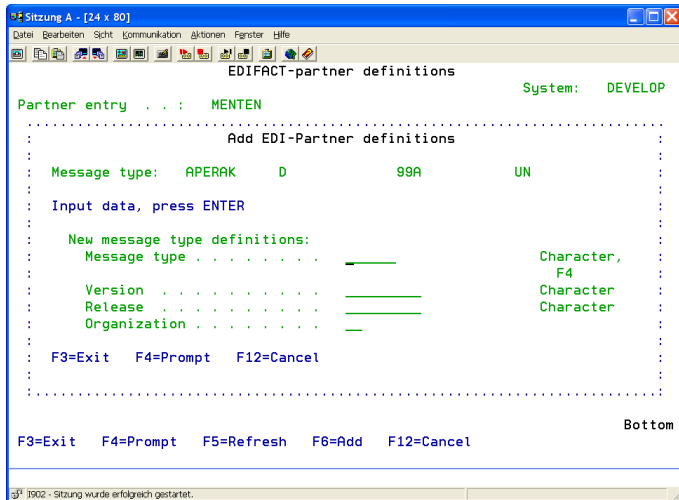
Display (option 5)

To display an entry, use option 5 in the corresponding choice box.

Rename (option 7)

To rename an entry, use option 7 in the corresponding choice box.

F6=Add, 2=Change, 5=Display EDIFACT Partner Details



Message Type - message type for EDI definitions

The qualified message type for which EDI definitions are to be made. Us function key F4 to display a list of currently loaded EDIFACT directories for the selection of a message type.

Version – version number of message type

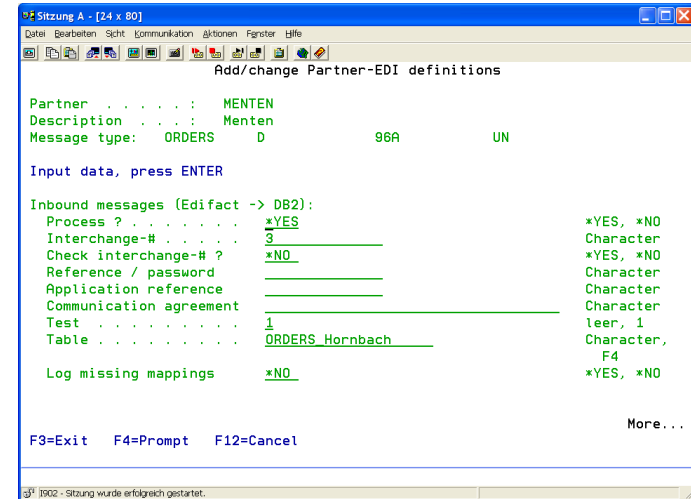
The version number of the EDIFACT standard by which the message type is defined.

Release – release number of the message type

The release number of the EDIFACT standard by which the message type is defined.

Responsible organization

Enter the abbreviation of the organization responsible for the definition of the EDIFACT standard.



In the following, the parameters to edit EDIFACT Partner Details are described.

Inbound Messages (EDIFACT --> DB/2)

Partner master data for inbound EDIFACT messages can be defined here.

Process

Determines if EDIFACT files for the displayed message type and partner are to be converted.

- *YES EDIFACT files are processed.
- *NO EDIFACT files are not processed.

Interchange # - the next expected interchange number

If the option "Check Interchange" is activated for checking the sequence number in the UNB segment, the next file to be processed for this partner with this message type MUST have the sequence number defined here. If not, conversion will be canceled. For every successful conversion, i-effect automatically adds 1 to this number.

Check Interchange

Switches the checking of the UNB sequence number on of off.

- *YES The interchange number is checked. Conversion will be canceled if the number of the previous field does not match the sequence number.
- *NO The interchange number is not checked

Reference / Password

If a value is entered into this field, the corresponding field in the UNB segment of the EDIFCAT file to be processed (service segment, header) is checked. Processing is continued only if these values match.

Application Reference

If a value is entered into this field, the corresponding field in the UNB segment of the EDIFCAT file to be processed is checked. Processing is continued only if these values match.

Communication Agreement

If a value is entered into this field, the corresponding field in the UNB segment of the EDIFCAT file to be processed is checked. Processing is continued only if these values match.

Test

If a value is entered into this field, the corresponding field in the UNB segment of the EDIFCAT file to be processed is checked. Processing is continued only if these values match.

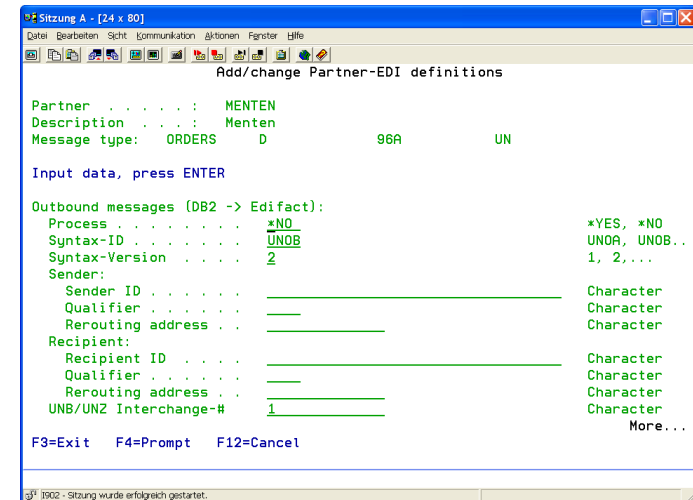
Table

The name of the i-effect conversion table that is to be used for this conversion. The table must describe the conversion of the defined message type. Use function key F4 to display a list containing all loaded mapping tables.

LOG Missing Mappings

If desired, all EDIFCAT data elements, for which no assignment to a DB2 field is defined, are logged in the logbook. Missing mappings can be easily found in a test run.

- *YES Unassigned data elements are logged in the logbook.
- *NO No logging of unassigned data elements.



Outbound messages (DB/2 --> EDIFACT)

Partner master data for outbound EDIFACT messages can be defined here.

Process

*YES EDIFACT files are processed.
*NO EDIFACT files are not processed.

Syntax ID

If a value is entered into this field, the field S001-0001 in the UNB segment will be filled with this value as soon as the function *SYNID is used when mapping.

Syntax Version

If a value is entered into this field, the field S001-0002 in the UNB segment will be filled with this value as soon as the function *SYNVER is used when mapping.

Sender

Sender ID

If a value is entered into this field, the field S002-0004 in the UNB segment will be filled with this value as soon as the function *SNDID is used when mapping.

Sender Qualifier

If a value is entered into this field, the field S002-0007 in the UNB segment will be filled with this value as soon as the function *SNDQUAL is used when mapping.

Sender Rerouting Address

If a value is entered into this field, the field S002-0008 in the UNB segment will be filled with this value as soon as the function *SNDRE-ROUTE is used when mapping.

Recipient

Recipient ID

If a value is entered into this field, the field S003-0010 in the UNB segment will be filled with this value as soon as the function *RCPID is used when mapping.

Recipient Qualifier

If a value is entered into this field, the field S003-0007 in the UNB segment will be filled with this value as soon as the function *RCPQUAL is used when mapping.

Recipient Rerouting Address

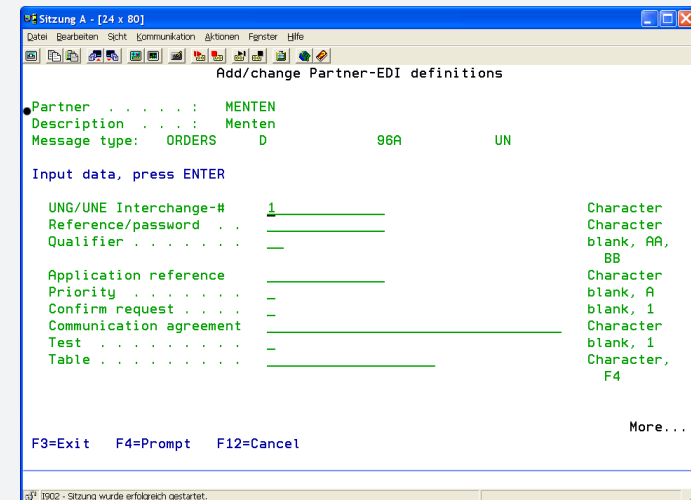
If a value is entered into this field, the field S003-0014 in the UNB segment will be filled with this value as soon as the function *RCPRE-ROUTE is used when mapping.

UNB/UNZ Interchange

If a value is entered into this field, the field 0020 in the UNB segment will be filled with this value as soon as the function *INTREF is used when mapping. After every EDIFACT file that has been generated for this partner, the displayed value is automatically increased by "1".

UNG/UNE Interchange

If a value is entered into this field, the field 0048 in the UNB segment will be filled with this value as soon as the function *GRPREF is used when mapping. After every group that has been generated for this partner, the displayed value is automatically increased by "1".



Reference / Password

If a value is entered into this field, the field S005-0022 in the UNB segment will be filled with this value as soon as the function *REFPW is used when mapping.

Qualifier

If a value is entered into this field, the field S005-0025 in the UNB segment will be filled with this value as soon as the function *REFQUA is used when mapping.

Application Reference

If a value is entered into this field, the field 0026 in the UNB segment will be filled with this value as soon as the function *APPREF is used when mapping.

Priority

If a value is entered into this field, the field 0029 in the UNB segment will be filled with this value as soon as the function *PRIO is used when mapping.

Acquisition Request

If a value is entered into this field, the field 0031 in the UNB segment will be filled with this value as soon as the function *ACQREQ is used when mapping.

Communication Request

If a value is entered into this field, the field 0032 in the UNB segment will be filled with this value as soon as the function *COMREQ is used when mapping.

Test

If a value is entered into this field, the field 0035 in the UNB segment will be filled with this value as soon as the function *TEST is used when mapping.

Table

The name of the i-effect conversion table that is to be used for this conversion. The table must describe the conversion of the defined message type. Us function key F4 to display a list containing all loaded mapping tables.

Insert CRLF

Determines if CRLF control characters are to be inserted at the end of every generated EDIFACT segment.

- *YES Control characters are inserted.
- *NO No control characters are inserted.

CCSID

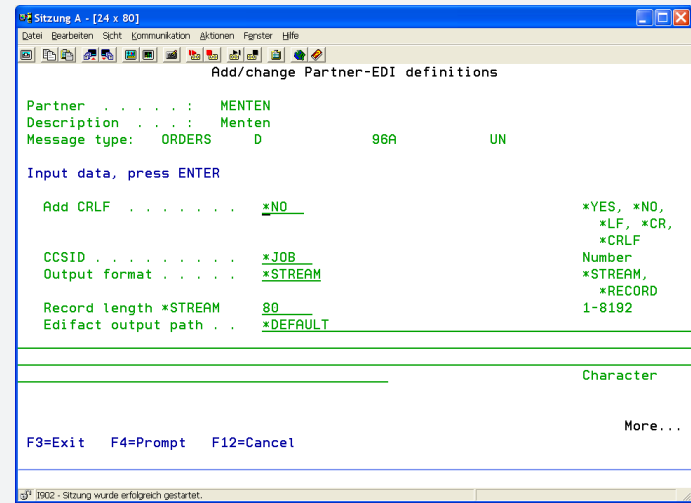
Enter a CCSID (Coded Character Set Identification) to convert EDIFACT files to the corresponding character set when processing. Both EBCDIC and ASCII character sets can be defined. If source and destination CCSID are identical, transformation is not effected.

Typical CCSID values are:

- 273 (EBCDIC Germany)
- 037 (EBCDIC England/America)
- 1252 (ASCII Windows)
- 850 (ASCII DOS)

Possible special values:

- *JOB The job's CCSID is used.



Output Format

Only valid if output file system *DB2 is selected. This parameter defines the output format of the physical file into which EDIFACT data is written.

- *STREAM All EDIFACT segments are put out successively. The record end is not the end of the segment.
- *RECORD Every EDIFACT segment is put out in a separate record.

Record Length *STREAM

Only valid if output file system *DB2 is selected and output format *STREAM is defined. The generated EDIFACT file is created with the record length defined here.

EDIFACT Output Path

Output path that is to be used for the currently edited partner and EDIFACT message type. The generated EDIFACT file is filed in this output path.

Possible special values

*DEFAULT The output path is taken from the *EDIFACT module's default setting.

EDIFACT File Name

The name of the generated EDIFACT file. The file name can be defined dynamically according to the models entered here. The following variables are possible:

%MSGTYPE%	Message type
%APPREF%	Application Reference
%SENDER%	Sender ID
%RECIPIENT%	Recipient ID
%YEAR%	Year YYYY
%MONTH%	Month MM
%DAY%	Day DD
%INTREF%	Interchange Reference (Interchange Number)
%PARTNER%	Assigned Partner Entry
%TIMESTAMP%	Timestamp of Generation of EDI file

Different *TELEBOX Addressing - EDIFACT Productive

This parameter allows selection of different addressing, depending on the test marker, to send data via the *TELEBOX module. If the selected EDIFACT message types are to be transmitted to the selected partner and if the file was created WITHOUT a test marker, the address entered here is valid (the entry under this alias) as data source of addressing definition.

With the help of this parameter, an addressing differing between test and productive run can be realized without changing the UNB recipient alias.

Different *TELEBOX Addressing - EDIFACT Test

This parameter allows selection different addressing, depending on the test marker, to send data via the *TELEBOX module. If the selected EDIFACT message types are to be transmitted to the selected partner and if the file was created WITH a test marker, the address entered here is valid (the entry under this alias) as data source of addressing definition.

With the help of this parameter, an addressing differing between test and productive run can be realized without changing the UNB recipient alias.

Details: 10=Additional Addresses

To add addresses to an entry, select menu item 50. Then, enter option number 10 "Additional Addresses" into the corresponding choice box.

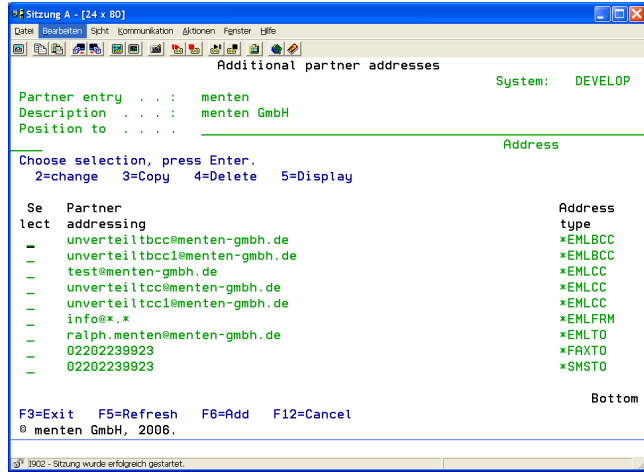
```

Sitzung A - [24 x 80]
Datei Bearbeiten Sicht Kommunikation Aktionen Fenster Hilfe
Work with EDI Partner Master Data System: DEVELOP
Position to . . . . .
Type options, press Enter.
2=Change 3=Copy 4=Delete 5=Display 7=Rename 8=EDIFACT definitions
10=Additional addresses 18=FLATFILE Definitions 20=Statistics

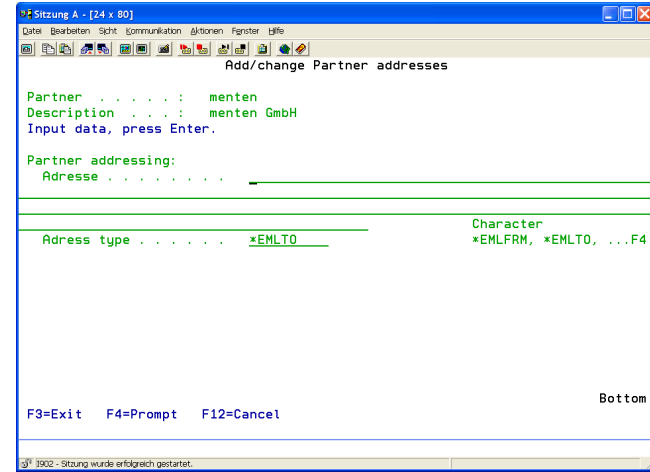
Partner
Opt Alias Description
---
ikkftp test ftp pc-ilja
ikkftprcv test rcvftp from iSereis
ikkftp1 test ftp pc-ilja
ikk15ftp ikk test partner for ftp i5effect
ikktelebox
ilja Test für eMail & AS2
iseries FTP Server auf iseries.meb.de [asci
as400e FTP Server AS400E FTP SERVER
iseries2
kleine Spedition-Kleine
10 menten menten GmbH
menten_iktbx menten EDV-Beratung GmbH
More...
F3=Exit F5=Refresh F6=Add F10=Work with comm. profiles F12=Cancel
3 1902 - Sitzung wurde erfolgreich gestartet.

```

The following display will appear:



Press F6 to enter a new address. The following display will appear:



The following overview describes the available options of the program interface.

- Add (option F6)** To add a new address, use option F6 (function key 6). In the appearing program interface, choose an address name and define the type of address.
- Change (option 2)** To change an address, use option 2 in the corresponding choice box.
- Copy (option 3)** To copy an existing address to a new entry, use option 3 in the corresponding choice box.
- Delete (option 4)** To delete an address, use option 4 in the corresponding choice box.
- Display (option 5)** To display an address, use option 5 in the corresponding choice box.

Address

Enter the additional address that is to be used for the selected partner. This must be a valid email address, fax number or mobile phone number, depending on the desired use.

Address Type

Enter the type of the entered address.

Possible values are:

**EMLFRM* The entered address is treated as email sender address.

Using address type **EMLFRM*, wild cards can be added to the address name. Valid are " * " and " ? ". By this, when receiving emails all emails coming from the USA for example will be assigned to a standard partner and will be filed accordingly.

Examples:

@.com – for every email coming from the USA

@myCompany. – for every email coming from myCompany

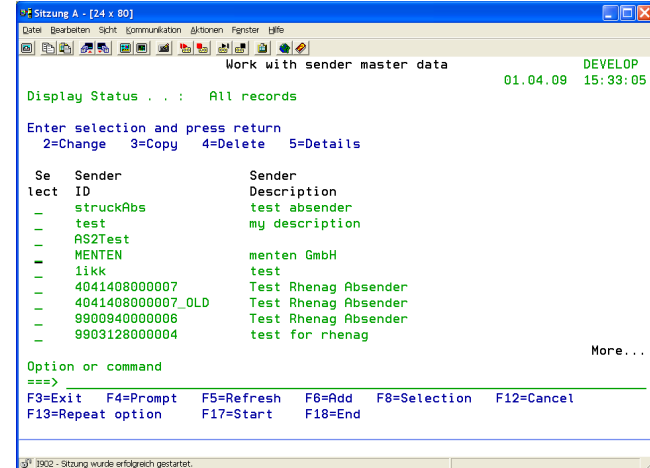
marketing@*.de / sales@*.de – for all emails coming from Germany having the sender "marketing" / "sales"

*EMLTO	The entered address is treated as email addressee.
*EMLCC	The entered address is treated as CC email address.
*EMLBCC	The entered address is treated as BCC email address.
*FAXTO	The entered address is treated as fax addressee number.
*SMSTO	The entered address is treated as SMS addressee number.

Menu Item 51: Work with EDI Originator Master Data

Originator master data is created by the program interface 51 (Work with EDI Sender Master Data). Select menu item 51 in the i-effect main menu.

The following display will appear:



```

Sitzung A - [24 x 80]
Datei Bearbeiten Sicht Kommunikation Aktionen Fenster Hilfe
Work with sender master data                                DEVELOP
01.04.09 15:39:05
Display Status . . . : All records

Enter selection and press return
2=Change 3=Copy 4=Delete 5=Details

Se      Sender      Sender
lect   ID           Description
-      -            -
-      struckAbs     test absender
-      test          my description
-      AS2Test      my description
-      MENTEN       menten GmbH
-      likk         test
-      4041408000007  Test Rhenag Absender
-      4041408000007_OLD  Test Rhenag Absender
-      9900940000006   Test Rhenag Absender
-      9903128000004   test for rhenag
More...

Option or command
===>
F3=Exit  F4=Prompt  F5=Refresh  F6=Add  F8=Selection  F12=Cancel
F13=Repeat option  F17=Start  F18=End

3902 - Sitzung wurde erfolgreich gestartet.

```

In this menu, originator information for the *AS2, *EMAIL, *OFTP and *HTTP modules can be created and edited.

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. The following overview describes the available options of the program interface.

Add (option F6)

Use option F6 (function key F6) to add an originator entry. To edit the newly created originator entry, use option 2.

Change (option 2)

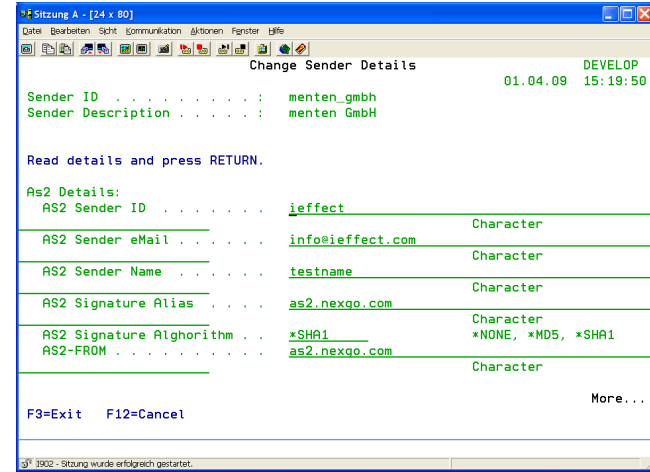
To change an entry, use option 2 in the corresponding choice box. The originator's data will be displayed and can be modified

Copy (option 3)

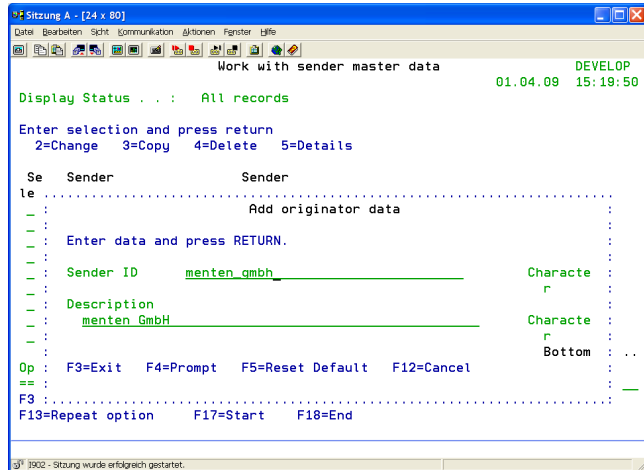
To copy an existing entry to a new originator entry, use option 3 in the corresponding choice box.

- Delete (option 4)** To delete an entry, use option 4 in the corresponding choice box.

- Display (option 5)** To display an entry, use option 5 in the corresponding choice box.



Details: F6=Add, 2=Change, 5=Display



When adding a new originator entry, a unique ID/name and a description of the entry will be requested. The entry will then be accessible under the defined ID. The description may contain a detailed text and will not be used. Nevertheless, a description is recommended for a better documentation of the entry.

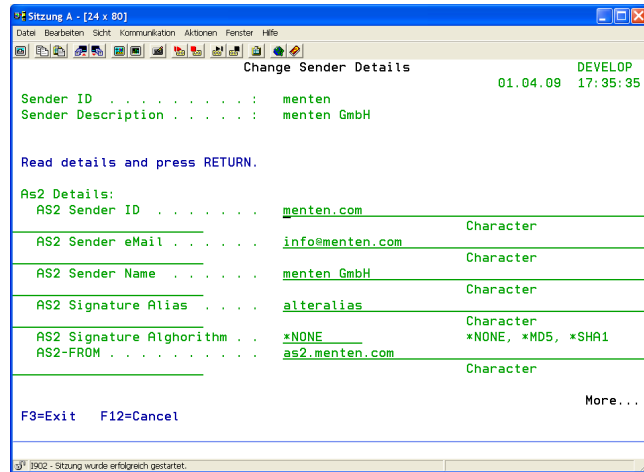
After selecting an entry to change, the following parameters can be configured:

Originator Details for the *AS2 Module

In "AS2 Details," originator specific AS2 details for communication can be stored. If necessary, it is possible to use different AS2 originator detail sets for communication with different partners. All AS2 details can be referred to by entering the entry's name into the command SNDAS2 in the parameter "Originator ID." Unnecessarily repeated entry of the same data is avoided.

To reach the menu where an AS2 originator partner can be added, select menu item 51 in the i-effect main menu. A list of existing originator partner entries will appear. Press F6 to call up the menu where a new originator partner can be added. Enter a unique ID/name and a description for the originator partner. Press enter and the new entry appears on the list. To change the entry, use option 2 in the corresponding choice box.

The following display will appear:



AS2 Sender 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 Sender Email Address

An email address can be entered here. It serves as general contact information and is the address where error messages about failed AS2 transactions are sent. Usually the address of the EDI department or the AS2 contact person is used.

AS2 Sender 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 only 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.

AS2 Signature Alias

Enter the alias name under which the key pair is stored in the keystore. This key pair (more precisely: the private key) serves to digitally sign an AS2 message. The alias name entered here **MUST** be identical to the alias name under which the key pair is stored in the keystore.

AS2 Signature Algorithm

This parameter defines the algorithm by which the *AS2 message is signed.

The following values are possible:

*NONE	The message is not signed.
*MD5	The message is signed by a MD5 (Message Digest 5) signature algorithm.
*SHA1	The message is signed by a SHA1 (Secure Hash Algorithm 1) signature algorithm.

AS2-FROM

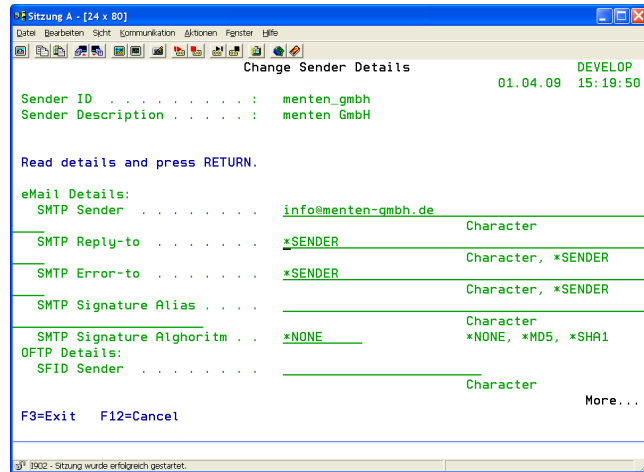
This is the distinct AS2 originator ID. It is inserted as sender into the outbound message. This ID enables the recipient to clearly identify the originator of the AS2 message.

Sender Details for the *EMAIL Module

In an EMAIL sender partner entry, sender specific EMAIL details for communication can be filed. If necessary, it is possible to use different EMAIL sender details for the communication with different partners. Furthermore, an EMAIL sender partner has the advantage that all sender specific EMAIL data is filed. Entering the command SNDEMAIL, the data will be given in the parameter "Sender ID". Unnecessarily repeated entry of the same data is avoided.

To reach the menu where an EMAIL sender partner can be added, select menu item 51 in the i-effect main menu. A list of existing sender partner entries will appear. Press F6 to call up the menu where a new sender partner can be added. Enter a unique ID/ name and a description for the sender partner. Press enter and the new entry appears on the list. To change the entry, use option 2 in the corresponding choice box and scroll down to EMAIL details.

The following display will appear:



SMTP Sender

This email address is inserted into the email as sender. If no "SMTP Reply-to" is entered, a reply is automatically sent to the email address entered here.

SMTP Reply-to

This email address is inserted into the email as Reply-to address. A reply is automatically sent to the email address entered here.

SMTP Error-to

In the case of error, email servers send a note to the email address entered here. If no Error-to address is entered, error messages will be sent to the "SMTP Sender" or "SMTP Reply-to" address.

SMTP Signature Alias

Enter the alias name under which the private key is stored in the keystore. The private key serves to sign the email. The alias name entered here MUST be identical to the alias name under which the key pair is stored in the keystore.

SMTP Signature Algorithm

This parameter defines the algorithm by which the *EMAIL message is encrypted.

The following values are possible:

*NONE	The email is not signed.
*MD5	The email is signed by a MD5 (Message Digest 5) algorithm.
*SHA1	The email is signed by a SHA1 (Secure Hash Algorithm 1) algorithm.

Sender Details for the *OFTP Module

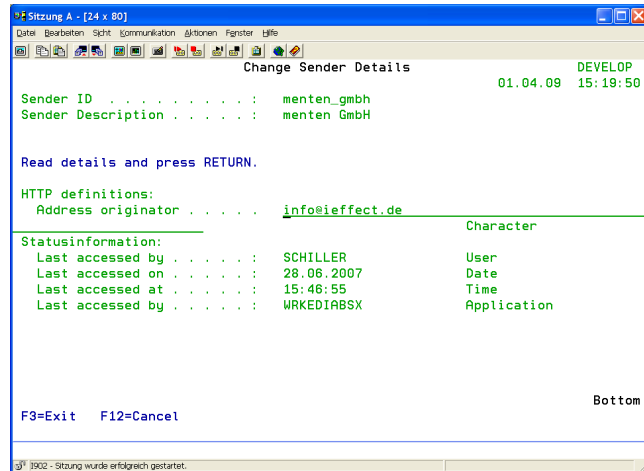
To reach the menu where an OFTP sender partner can be added, select menu item 51 in the i-effect main menu. A list of existing sender partner entries will appear. Press F6 to call up the menu where a new sender partner can be added. Enter a unique ID/ name and a description for the sender partner. Press enter and the new entry appears on the list. To change the entry, use option 2 in the corresponding choice box and scroll down to OFTP details.

SFID Sender

In an OFTP transmission, the SFID segment (Start File Identification) indicates the originator of a file. The SFID will be filled by the defined ID if a corresponding originator ID is selected when starting an OFTP communication. If no originator is selected, the SFID originator ID is the SSID originator ID. The originator of the file is identical to the initiator of the communication.

Sender details for the *HTTP module

To reach the menu where an HTTP sender partner can be added, select menu item 51 in the i-effect main menu. A list of existing sender partner entries will appear. Press F6 to call up the menu where a new sender partner can be added. Enter a unique ID/ name and a description for the sender partner. Press enter and the new entry appears on the list. To change the entry, use option 2 in the corresponding choice box and scroll down to HTTP definitions.



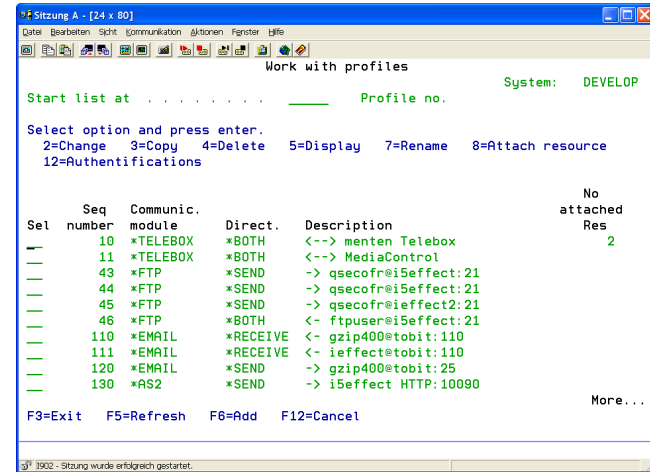
Originator Address

Enter a sender email address that is inserted as sender address into HTTP header.

Menu Item 52: Work with EDI Communication Profiles

Communication profiles are created by program interface 52 (Work with EDI Communication profiles). Enter option 52 in the i-effect main menu.

The following program interface will appear:



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. The following overview describes the available options of the program interface, followed by a more detailed description.

Add (option F6)

Use option F6 (function key F6) to add a communication profile. In the appearing program interface, possible communication profiles of the installed i-effect modules are displayed and can be selected.

Change (option 2)

To change an entry, use option 2 in the corresponding choice box. The details of the selected communication profile will be displayed and can be modified according to new specifications.

Copy (option 3)

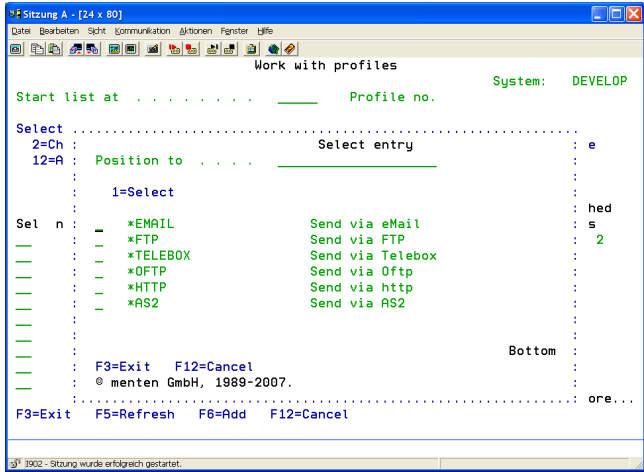
To copy an existing entry to a new entry, use option 3 in the corresponding choice box.

- Delete (option 4)** To delete an entry, use option 4 in the corresponding choice box.
- Display (option 5)** To display an entry, use option 5 in the corresponding choice box.
- Rename (option 7)** To rename an entry, use option 7 in the corresponding choice box.
- Allocate resource (option 8)** To allocate a communication profile to the existing entry, use option 8 in the corresponding choice box.

Details: F6=Add

Use option F6 (function key F6) to add a communication profile. In the appearing program interface, possible communication profiles of the installed i-effect modules are displayed and can be selected.

The program interface below shows the possible options if all i-effect modules are successfully installed. To select an entry, enter option number 1 in the corresponding choice box.



Create AS2 Communication Profiles

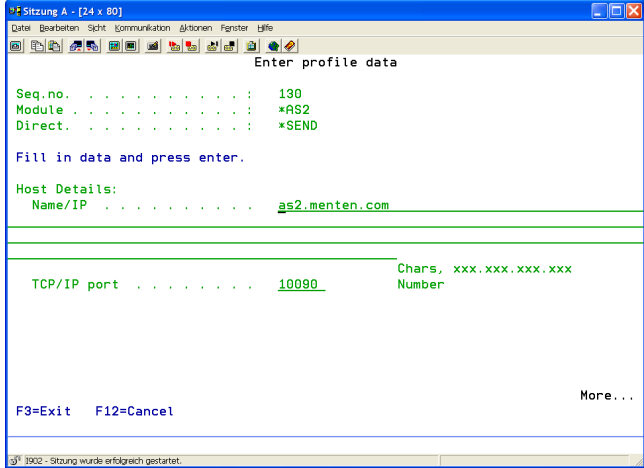
Create an *AS2 Sending Profile

In order to send data to a partner, an AS2 sending profile is required for each partner. All sender specific AS2 details being necessary for AS2 communication towards the partner are filed in this profile.

To reach the menu where an AS2 sending profile can be added, select menu item 52 in the i-effect main menu. A list of existing communication profiles will appear.

Press F6 to call up the menu where a new communication profile can be added. Then, select AS2 communication using option number 1 in the corresponding choice box. In the following menu, please select *SEND.

The following display will appear:



The following parameters can be configured:

Name/IP:
Enter the IP number or the DNS hostname of the partner's AS2 server.

TCP/IP port:
Enter the port number of the partner's AS2 server.

Path for Inbound MDN

If necessary, define a different IFS directory in which MDN files of inbound MDNs are stored.

Note: This parameter allows IFS directories only.

Path for Sent Headers

The default IFS path in which header data of sent AS2 messages is stored. If necessary, define a different IFS directory.

Note: This parameter allows IFS directories only.

AS2-TO (Recipient ID)

Enter the communication partner's AS2 ID. This ID is distinct for every partner and must be communicated to you by the partner. Most often, this ID is the partner's GLN (Global Location Number). Via this ID, a clear partner assignment is achieved in i-effect when receiving AS2 messages.

AS2 Encryption Alias

The AS2 encryption alias determines the partner certificate's entry in the keystore. The certificate is the communication partner's public key and must be communicated to you by the partner. It serves to digitally encrypt the message. The recipient needs his private key to encrypt the messages. How to import a certificate into the keystore is described in Chapter 12 "Additional Graphical Applications".

AS2 Encryption Algorithm

This parameter determines if encryption for AS2 messages is required.

**NONE* No encryption.

The AS2 message is not encrypted.

**TRIPLEDES* The message is encrypted by a Triple-DES encryption.

The Data Encryption Standard (DES) is a widespread symmetric encryption algorithm with a key length of 3DES (=168 bits), which is three times as much as with DES encryption (=56 bits).

MDN Request

This parameter determines if and how a MDN is requested. Usually, the partner informs about the expected setting.

Three values are possible:

- *SYNCH* An MDN will be requested when the AS2 message is sent, which should be received shortly after the transmission of the message. It is sent back by the recipient via the EXISTING connection.
- *ASYNCH* An MDN is requested but is received with a time delay after the transmission of the AS2 message. It is sent back by the recipient via a NEW connection.
- *NONE* MDN is not requested.

MDN Signature

The parameter "MDN Signature" defines the algorithm that the recipient of an AS2 message must use to sign the MDN. Note that if sent AS2 messages are signed with the SHA1 algorithm, the recipient must sign the MDN with the SHA1 algorithm, too. Option **MD5* in this parameter will be ignored in this case. Only if an AS2 messages is sent unsigned, an option must be selected.

- *MD5* The requested MDN must be signed by a MD5 algorithm.
- *SHA1* The requested MDN must be signed by a SHA1 algorithm.

MDN Protocol

Define the protocol that is to be used to send back an asynchronous MDN. This value is only relevant concerning asynchronous MDNs because synchronous MDNs use the existing connection, and therefore the protocol by which the AS2 message is transmitted.

Possible values are:

- *SERVER* Default value. The MDN is sent to your system's AS2 server defined for receiving asynchronous MDNs. This server must be created beforehand. How to create an AS2 server is described in this chapter "Create an AS2 Reception Profile".
- *SMTP* The MDN is sent back per SMTP (email) to the AS2 sender email address defined in menu 80. Please note that this way of transmission is rarely used.

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.

Receive 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 determine this value.

Recommended value: 120 seconds.

Content Type

Determine the AS2 message's type of content

Possible values:

<i>*CONSENT</i>	The AS2 message contains EDI files in none of the following formats (application/edi-consent).
<i>*EDIFACT</i>	The AS2 message contains data in the EDIFACT format (application/EDIFACT).
<i>*X12</i>	The AS2 message contains data in the X12 format (application/EDI-X12).
<i>*XML</i>	The AS2 message contains data in the XML format (text/xml).
<i>*BINARY</i>	The AS2 message contains binary data (application/octet-stream).
<i>*FRMFILE</i>	The type of content is identified by the file extension of the input file (.edi = application/EDIFACT). Using *FRMFILE for DB2 files, the content type is always *BINARY (application/octet-stream) because DB2 does not have typical file extensions.

Bodypart Type

Determine if one or more files are transmitted with the AS2 message.

Possible values:

<i>*SINGLE</i>	Default value. One file is transmitted with the AS2 transmission.
<i>*MULTI</i>	Several files are transmitted with the AS2 transmission.

The transmission of several files is not supported in the current *AS2 version. Please use the value *SINGLE for every transmission.

Proxy Server

If using a Proxy server for AS2 communication is desired, parameters to be applied can be defined here.

Possible parameters:

<i>Host name/IP</i>	Enter the IP address or DNS name.
<i>TCP/IP Port</i>	Enter the TCP/IP port.
<i>User ID</i>	Enter (if required) the authorized user's ID.
<i>Password</i>	Enter (if required) the authorized user's password.

SSL

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

<i>*YES</i>	Yes, the connection is established via SSL/HTTPS
<i>*NO</i>	No, the connection is established via standard HTTP.

Import Untrustworthy Certificates

Enter the value *YES into this parameter to automatically import server certificates that do not exist in the keystore via a HTTP (SSL/TLS) connection. In this case, be aware of the fact that every server connected with HTTPS and whose certificate does not exist in the key store is trusted.

If the value *NO is entered into this parameter and the certificate of the server to connect with does not exist in the keystore, the connection will automatically be closed. It is correct to abort the connection because the server's identity cannot be verified due to the missing certificate in the keystore.

<i>*YES</i>	Yes, untrustworthy certificates are automatically imported.
<i>*NO</i>	No, untrustworthy certificates are not automatically imported.

Use Client Authentication?

Determine if the AS2 client must authenticate with an X.509 certificate when establishing a connection to the partner's server. Using the value *YES for the "SSL" parameter, the partner's AS2 server will accept the incoming connection only in the case of successful verification of the certificate sent by the client. If not, the established connection will be closed failing identification as authorized partner trying to send an AS2 message to the server.

The partner should explicitly state if this form of SSL authentication is required.

<i>*AUTO</i>	Default setting. Automatic verification if client authentication is requested from the server when connecting (SSL Handshake). If so, the corresponding certificate will be transmitted to the server, if possible.
<i>*YES</i>	Yes, client authentication is used. This setting is valid for every connection establishment. Servers not using client authentication cause an error. Consequently, the connection will be closed.

Please note that this form of SSL authentication is requested by only a few servers and is generally not common on the Internet.

SSL Connection Certificate

By using the value *YES in the "Use Client Authentication ?" parameter, the name of key pair containing your public key (the certificate) can be entered. This certificate is transmitted to the server when sending AS2 messages. Of course, it must exist in the partner's AS2 server keystore before establishing a connection.

Description

A short description of the AS2 sending profile can be created here. This field has only a descriptive character, its content is arbitrary.

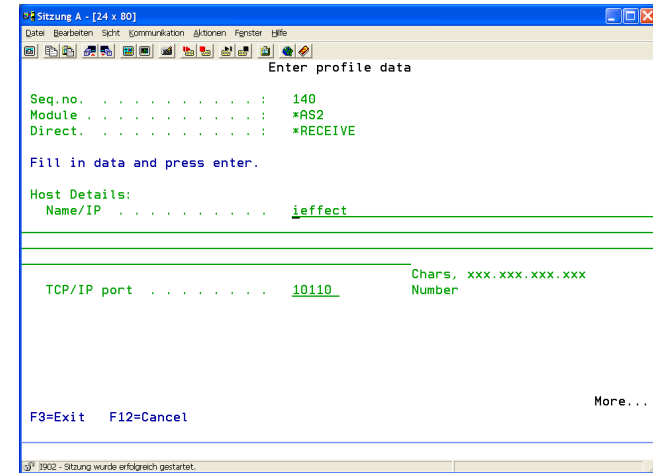
Create an AS2 Reception Profile (AS2 Server)

In order to receive AS2 messages and MDNs from a partner, an AS2 server needs to be created. Several AS2 server entities may be created on the system. Every created AS2 server must be bound to a free address/port. For instance, it is possible to create an AS2 server for every partner. On the defined address/port, the AS2 server waits for inbound AS2 messages. Furthermore, if AS2 messages are to be sent with asynchronous MDN request, one server must be defined as reception server for requested asynchronous MDNs. For further information see parameter description "Asynch MDN Server?"

To reach the menu where an AS2 reception profile can be added, select menu item 52 in the i-effect main menu. A list of existing communication profiles will appear.

Press F6 to call up the menu where a new communication profile can be added. Then, select AS2 communication using option number 1 in the corresponding choice box. In the following menu, please select *RECEIVE.

The following display will appear:



The following parameters can be configured:

Name/IP

Enter the hostname/IP address to which the AS2 server is bound.

TCP/IP port

The port on which the AS2 server waits for incoming connections.

Path for Received Data

Determine an IFS directory to store received data.

This parameter will be dropped in the next version. Indicating a general reception path is unnecessary because AS2 messages are always received partner related.

Path for Received Headers

If necessary, define a different IFS directory in which header files of inbound AS2 messages are stored.

Note: This parameter allows IFS directories only.

Path for Received MDN

If necessary, define a different IFS directory in which successfully received MDNs are stored.

Note: This parameter allows IFS directories only.

Path for Sent MDN

If necessary, define a different IFS directory in which successfully sent MDNs are stored.

Note: This parameter allows IFS directories only.

Path for Open MDN (asynchronous)

If necessary, define a different IFS directory in which received AS2 messages with asynchronous MDN request are temporarily stored until the requested MDN is transmitted.

Hinweis: : This parameter allows IFS directories only.

Async MDN Server

AS2 allows to request receipt confirmations for sent AS2 messages. These receipts, so-called MDNs (Message Disposition Notification), can be synchronous or asynchronous.

Synchronous means: The requested MDN is returned to the originator during the same connection. If a synchronous MDN is not successfully transmitted via the established connection, the sending process is considered invalid, even if the transmission of the AS2 message was successful. This is necessary due to the lack of proof of reception and processing of the AS2 message on the partner's system without a received MDN.

This might happen if an AS2 message is relatively large. The time required to process this message and to return an MDN to the sender on the same connection may exceed the maximum configured time defined in the AS2 sending profile reception timeout.

The AS2 client cancels the established connection before the MDN could have been sent to the partner. In order to avoid these situations, an asynchronous MDN for AS2 messages can be requested. But before, please check whether your partner's AS2 system supports asynchronous MDN requests.

Asynchronous means: The connection will be closed after the AS2 message has been transmitted to the partner. The requested MDN is sent on a separate connection established by the partner after successful processing on the receiving system. This option is very practical with large messages because processing huge amounts of data easily exceeds the maximum configured time defined in the AS2 sending profile reception timeout. Regrettably, there is no general rule to define the maximum size of a message that still allows a synchronous MDN requests because too many factors have an impact on this process (processing time on the target system, root, etc.).

In order to receive asynchronous MDNs for sent AS2 messages, one of the created AS2 servers must be determined as reception server for requested asynchronous MDNs. If only one server was created, use option *YES in this parameter in order to make sure that asynchronous MDNs can be received on this server. This server is then determined as reception server for requested asynchronous MDNs.

*YES	This AS2 server receives all asynchronous MDNs sent back by the partners.
*NO	Default setting. This AS2 server does not receive asynchronous MDNs sent back by the partners.

In the current AS2 version only ONE server can be determined to receive asynchronous MDNs. It is not possible to define several MDN servers in the system.

Maximum Server Threads

This parameter defines the maximum number of connections an AS2 server will process at the same time. If this maximum number of simultaneous connections is reached, further incoming connections will be put into a waiting line. They are processed as soon as a free connection is available.

Reception Timeout

Define the maximum time (in seconds) an AS2 server will wait for data of an incoming connection. If no data is received within the configured time, a timeout error notification is sent and the connection will be closed.

Scan Interval Open MDN

After decryption and verification, received AS2 messages with asynchronous MDN request are stored as AS2 object files (.as2) in the IFS directory defined in the parameter "Path for Open MDN (asynchronous)". Therefore, it is necessary to scan this directory for new AS2 object files in regular time intervals to send back outstanding MDNs. The time (in seconds) for this interval can be defined in this parameter.

MDN Retry Count

Determine the maximum number of attempts to send requested asynchronous MDNs.

External IP, DNS Name

Enter an URL/IP for requested asynchronous MDNs. The partner sends the requested MDN to this address. Therefore, it must be transmitted to the partner system when sending an AS2 message with asynchronous MDN request. In a HTTP/HTTPS transmission, it is the AS2 server's external DNS name or the external IP address. This address must be accessible from outside.

External TCP/IP Port

Enter the AS2 server's external TCP/IP port. On this port, the AS2 server accepts MDNs. It must be accessible from outside.

SSL

This parameter determines the protocol to be used by the AS2 server. Possible options are *YES and *NO. If *NO is selected, the AS2 server uses the HTTP protocol and is therefore reachable via standard HTTP connections. If *YES is selected, the AS2 server uses the SSL (TLS) protocol and is therefore only reachable via HTTPS connections. If option *YES is set, AS2 server settings can be specified in the parameters "Use Client Authentication ?" "Import Untrustworthy Certificates ?" and "SSL Connection Certificate".

*NO	The AS2 server uses the HTTPS protocol.
*YES	The AS2 server uses the standard HTTP protocol.

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.

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.

SSL Connection Certificate

Enter the name of the key pair containing the public key (certificate) in the keystore. The certificate is transmitted to every client establishing an SSL connection to the AS2 server. The server identifies itself to the client. Therefore the certificate must exist in the client's keystore before connecting.

This form of HTTPS authentication is standard practice on the Internet.

Description

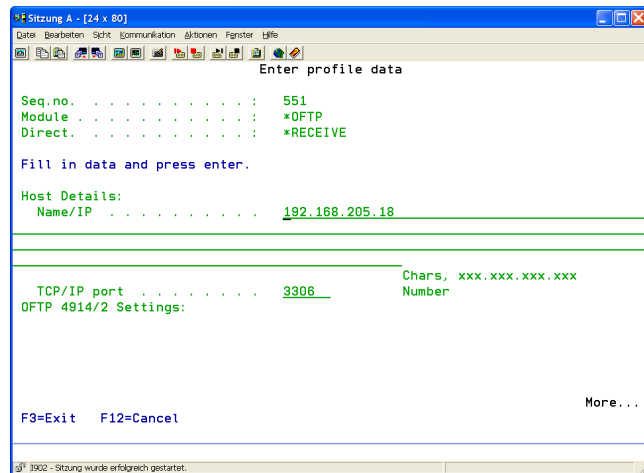
A short description of the created AS2 server can be created here. This field has only a descriptive character, its content is arbitrary.

Create OFTP Communication Profiles

Create an *OFTP Reception Profile (OFTP Server)

To reach the menu where an OFTP reception profile can be added, select menu item 52 in the i-effect main menu. Press F6 to call up the menu where a new communication profile can be added. Then, select OFTP communication using option number 1 in the corresponding choice box. In the following menu, please select *RECEIVE.

The following parameters can be configured:



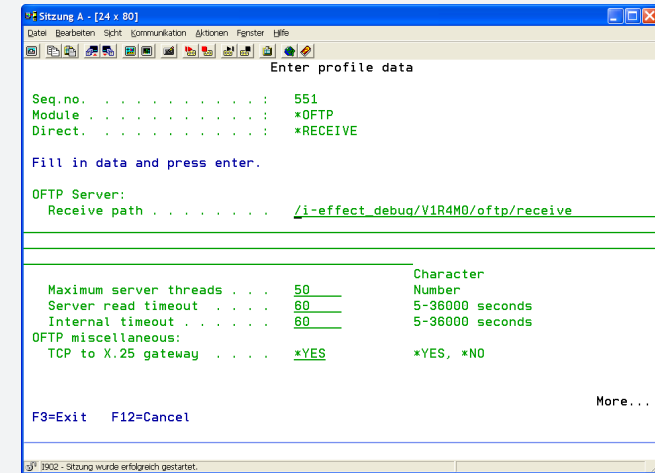
Host Details:

Name/IP:

Enter the hostname/IP address under which the server is accessible. Please make sure that these parameters match the System i and network settings (see WRKTCPSTS -> option 1). If in doubt, contact the system administrator.

TCP/IP port:

Enter the port number under which the server is accessible. The default OFTP port is 3305, but generally the port number is arbitrary (>1023). Please make sure that the port does not conflict with other applications listening on the port. Check with WRKTCPSTS -> option 3 -> F14 (Display Port Addresses). If in doubt, contact the system administrator.



OFTP Server:

Reception Path:

Determine the default reception path for received files. To improve performance, it is recommended that an IFS path is defined because storing data on DB2 paths requires more processing power. When receiving data, it will be stored in the partner's corresponding reception directories. Therefore, a partner profile must be created.

Maximum Server threads:

This parameter determines the maximum number of connections an OFTP server will process at the same time. If this maximum number of simultaneous connections is reached, further incoming connections will not be accepted. A common value is 50.

Server Read Timeout:

Determine after how much time (in seconds) a connection is considered as failed. If an idle time occurs, the connection will be canceled.

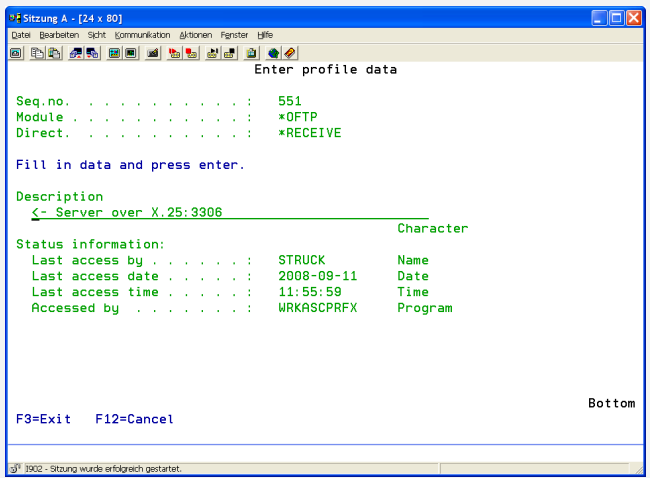
Internal Timeout:

Determine after how much time a server entity is declared irresponsive, e.g. because a storage process takes too long to process a file.

OFTP Other:

TCP/IP to X.25 Gateway:

Use option *YES in this parameter if PFTP server communication is not effected via TCP/IP, but a connection to X.25 networks is established via a Bintec Router (see configuration Bintec Router). Otherwise select *NO if communication is effected via TCP/IP.



Description

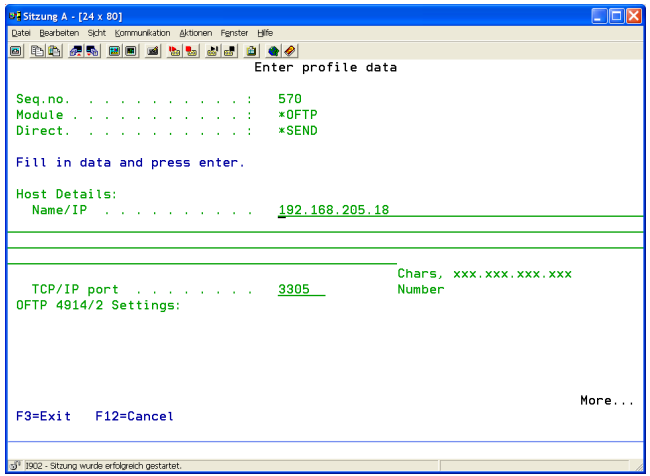
A short description of the server entity can be created here. It is recommended that a short form of the IP/hostname port combination the server is listening on, e.g.: OFTPMENTEN.DE:3305, is entered.

After having created a server entry, partner user authentications can be stored.

Create an *OFTP Sending Profile

To reach the menu where an OFTP sending profile can be added, select menu item 52 in the i-effect main menu. Press F6 to call up the menu where a new communication profile can be added. Then, select OFTP communication using option number 1 in the corresponding choice box. In the following menu, please select *SEND.

The following parameters can be configured:



Host Details:

Name/IP:

Enter the IP number or the DNS hostname of the partner's server.

TCP/IP port:

Enter the port number of the partner's server. The default port for the OFTP protocol is 3305, but it may differ. This parameter is to be requested from the partner.

```

Sitzung A - [24 x 80]
Datei Bearbeiten Sicht Kommunikation Aktionen Fenster Hilfe
Enter profile data

Seq.no. . . . . : 570
Module . . . . . : *OFTP
Direct. . . . . : *SEND

Fill in data and press enter.

OFTP Client:
Maximum send retries . . . . . 1          Number
Send retry pause . . . . . 10         5-99000 seconds
Connection timeout . . . . . 60        5-36000 seconds
Read timeout . . . . . 60          5-36000 seconds
Internal timeout . . . . . 60         5-36000 seconds
SFID destination . . . . . *SSID

SFID user data . . . . . _____ *SSID, Zeichen
SFID user data . . . . . _____ Character
Buffer size . . . . . 1024         Bytes
Window size/Credit . . . . . 7          Number
Compression . . . . . *YES         *YES, *NO

F3=Exit  F12=Cancel

More...

1002 - Sitzung wurde erfolgreich gestartet.

```

OFTP Client:

Maximum Send Retries

Determine the maximum number of attempts to retry to connect after connection failure.

Send Retry Pause

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

Connection Timeout

Determine the timeout in seconds for connection establishment.

Read Timeout

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

Internal Timeout

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

SFID Destination Address

Determine the recipient's Odette ID. Usually it is identical to the partner's Odette ID. It may differ if data is transmitted via an OFTP gateway.

SSID User Data

Generally, this parameter is only required in the case of bilateral agreement between the partners.

SFID User Data

Generally, this parameter is only required in the case of bilateral agreement between the partners.

Buffer Size

Determine the maximum buffer size used in data transmission. A common value for TCP/IP connections is 2048 or 4096, for X.25 via ISDN connections it is 256 to 512.

Window Size / Credit

This parameter determines the number of buffers that can be transmitted until the partner is requested to refill the credit. This parameter is comparable to the TCP common term "Window Size". A common value is 7.

```

Sitzung A - [24 x 80]
Datei Bearbeiten Sicht Kommunikation Aktionen Fenster Hilfe
Enter profile data

Seq.no. . . . . : 570
Module . . . . . : *OFTP
Direct. . . . . : *SEND

Fill in data and press enter.

Restart . . . . . *YES          *YES, *NO
Strict protocol . . . . . *YES         *YES, *NO
Default data type . . . . . *UNSTRUCT   *FIX, *VARIABLE, *UNSTRUCT,
                                         *TEXT

OFTP miscellaneous:
TCP to X.25 gateway . . . . . *NO         *YES, *NO
Description
-> ieffect:3305_1024/*UNSTRUCT/YYY
                                         Character

F3=Exit  F12=Cancel

More...

1002 - Sitzung wurde erfolgreich gestartet.

```

Compression

This parameter determines if a simple compression for *TEXT files (see "Fix, Variable, Unstruct, Text") is to be used. This must be supported by the remote side.

Restart

If transmission was interrupted in a previous data transmission, this parameter determines if data transmission will be continued at the point of interruption. This must be supported by the remote side.

Strict Protocol

This parameter determines if data transmission is done without deviating from the standard protocol. Setting this parameter to *NO might be necessary if the partner uses an ODEX system, or if protocol errors occur regularly on the remote side.

Fix, Variable, Unstruct, Text

In *OFTP data transmission, data can be sent/received in one of 4 different types of transmission: *FIX, *VARIABLE, *TEXT and *UNSTRUCT (explanation below):

<i>*FIX</i>	Data is split into sets of equal length – if necessary filled with blanks – and is converted into the partner specific CCSID.
<i>*VARIABLE</i>	Before sending, the longest set is determined, conversion into the partner specific CCSID is effected. Filling the set with blanks is not required.
<i>*UNSTRUCT</i>	Data is sent without conversion as binary file.
<i>*TEXT</i>	The file is converted into the partner specific CCSID before sending. If the outbound file is in a database, a line feed will be inserted at the end of every database record (CR LF).

OFTP Other:**TCP/IP to X.25 Gateway**

This parameter determines if the OFTP connection is to be established via a TCP/X.25 gateway, or a native TCP/IP connection is to be used. In the first case, a X.25 compatible router is connected with the local network via TCP/IP and forwards the OFTP transmission request to a native X.25 or ISDN network (X.25 via ISDN B-channel).

Possible options:

<i>*YES</i>	A TCP/IP to X.25 gateway is used.
<i>*NO</i>	A direct TCP/IP connection is used.

Description

A brief description of the sending profile can be created here. Indicating the IP/hostname port combination or X.25 addresses that is used to connect with the partner, e.g. OFTP.MENTEN.DE:3305, is recommended.

After a partner entry has been created, authentication details for an entry can be stored by entering option number 12 into the corresponding choice box.

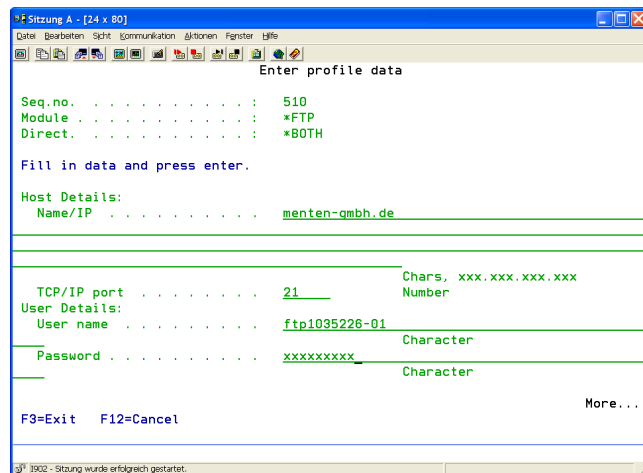
Create a FTP Communication Profile

Create a FTP Sending/Reception Profile

To reach the menu where a FTP sending/reception profile (working in both directions) can be added, select menu item 52 in the i-effect main menu.

Press F6 to call up the menu where a new communication profile can be added. Then, select FTP communication using option number 1 in the corresponding choice box. In the following menu, please select *BOTH.

The following parameters can be configured:



```

Sitzung A - [24 x 80]
-----
Enter profile data

Seq.no. . . . . : 510
Module . . . . . : *FTP
Direct. . . . . : *BOTH

Fill in data and press enter.

Host Details:
Name/IP . . . . . : menten-gmbh.de

TCP/IP port . . . . . : 21
                                     Chars, xxx.xxx.xxx.xxx
                                     Number

User Details:
User name . . . . . : ftp1035226-01
                                     Character
Password . . . . . : xxxxxxxx
                                     Character

F3=Exit  F12=Cancel

More...

1902 - Sitzung wurde erfolgreich gestartet.
  
```

Host Details:

Name/IP

Enter the IP number or the DNS hostname of the partner's FTP server.

TCP/IP port

Enter the port number of the partner's FTP server. The default port for the FTP protocol is 21.

User Details:

User ID

Enter the user ID needed to login to the FTP server.

Password

Enter the password corresponding to the user ID.

FTP Details:

Default Transmission Type

This parameter determines the type of transmission commonly used with this FTP server. The default setting can be overwritten for every single transmission.

Possible values:

- *ASCII This setting is required to exchange data with ASCII machines that do not support EBCDIC.
- *EBCDIC This setting is required to exchange data with EBCDIC machines. An unnecessary translation between ASCII and EBCDIC on both machines is avoided.
- *BINARY This setting is required to exchange binary data (e.g. Save Files). Data is transmitted one-to-one.

Default Mode

Enter the default FTP mode that is to be used.

Possible special values:

- *ACTIVE The FTP mode „ACTIVE“ is used.
- *PASSIVE The FTP mode „ PASSIVE „ is used.

Description

A short description of the FTP profile can be created here. This field has only a descriptive character, its content is arbitrary.

Create TELEBOX Communication Profiles

Menu item 53 “EDI communication resources” describes how to configure the Telebox Hardware Resource in i-effect. This resource can be assigned to a Telebox communication profile (*RECEIVE or *SEND).

Create a TELEBOX Sending/Reception Profile

To reach the menu where a TELEBOX sending/reception profile (working in both directions) can be added, select menu item 52 in the i-effect main menu.

Press F6 to call up the menu where a new communication profile can be added. Then, select TELEBOX communication using option number 1 in the corresponding choice box. In the following menu, please select *BOTH.

The following parameters can be configured:

```

Sitzung A - [24 x 80]
Datei Bearbeiten Sicht Kommunikation Aktionen Fenster Hilfe
Enter profile data

Seq.no. . . . . : 10
Module . . . . . : *TELEBOX
Direct. . . . . : *BOTH

Fill in data and press enter.

User Details:
User name . . . . . : menten                Character
Password . . . . . : password              Character

Telebox400 Details:
Own PBID . . . . . : 2018851                Number
Description
<--> menten Telebox                Character

More . . .

F3=Exit  F12=Cancel
  
```

User Details

User ID

Enter the user ID needed to login to the X.400 Telebox.

Password

Enter the password corresponding to the user ID.

Telebox Details

Personal PBID

This parameter describes the personal identification PBID (personal box ID) for this Telebox system profile

Description

A short description of the Telebox profile can be created here. This field has only a descriptive character, its content is arbitrary.

Create HTTP Communication Profiles

This part describes how to create and configure a HTTP sending profile and how a HTTP server is to be configured in a system.

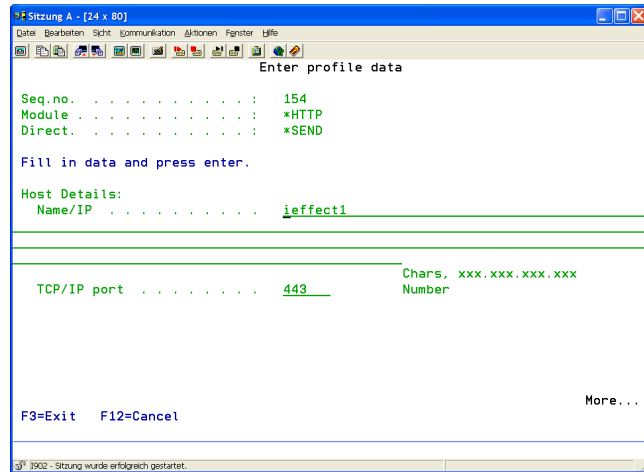
Create a HTTP Sending Profile

In order to send data via a HTTP POST to a partner, a HTTP sending profile is required for each partner. All sender specific HTTP details being necessary for communication towards the partner are filed in this profile.

To reach the menu where a HTTP sending profile can be added, select menu item 52 in the i-effect main menu. A list of existing communication profiles will appear.

Press F6 to call up the menu where a new communication profile can be added. Then, select HTTP communication using option number 1 in the corresponding choice box. In the following menu, please select *SEND.

The following display will appear:



The following parameters can be configured:

Host Details

Name/IP:

Enter the IP number or the DNS hostname of the partner's HTTP server.

TCP/IP Port:

Enter the port number of the partner's HTTP server.

HTTP Details

Connection Timeout

The HTTP 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

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

Recommended value: 120 seconds.

Internal Timeout

This parameter determines a timeout value in seconds until an internal timeout is reported.

Maximum Send Retries

Determine the maximum number of attempts to retry to connect after connection failure.

Send Retry Pause

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

Content Type

Determine the AS2 data's type of content.

Possible values:

<i>*CONSENT</i>	Data has none of the following formats (application/edi-consent).
<i>*EDIFACT</i>	Data has the EDIFACT format (application/EDIFACT).
<i>*X12</i>	Data has the X12 format (application/EDI-X12).
<i>*XML</i>	Data has the XML format (text/xml).
<i>*BINARY</i>	Data is binary data (application/octet-stream).
<i>*FRMFILE</i>	The type of content is identified by the file extension of the input file (.edi = application/EDIFACT). Using *FRMFILE for DB2 files, the content type is always *BINARY (application/octet-stream) because DB2 does not include typical file extensions.

Proxy Server

If using a Proxy server for HTTP communication is desired, parameters to be applied can be defined here.

Possible parameters:

<i>Host name/IP</i>	Enter the IP address or DNS name.
<i>TCP/IP Port</i>	Enter the TCP/IP port.
<i>Benutzername</i>	Enter (if required) the authorized user's ID.
<i>Kennwort</i>	Enter (if required) the authorized user's password.

SSL

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

<i>*YES</i>	Yes, the connection is established via SSL/HTTPS
<i>*NO</i>	No, the connection is established via standard HTTP.

Import Untrustworthy Certificates

Enter the value **YES* into this parameter to automatically import server certificates that do not exist in the keystore via an HTTPS (SSL/TLS) connection. In this case, be aware of the fact that every server connected with HTTPS and whose certificate does not exist in the keystore is trusted.

If the value **NO* is entered into this parameter and the certificate of the server to connect with does not exist in the keystore, the connection will automatically be closed. It is correct to abort the connection because the server's identity cannot be verified due to the missing certificate in the keystore.

<i>*YES</i>	Yes, the connection is established via SSL/HTTPS
<i>*NO</i>	No, the connection is established via standard HTTP.

Use Client Authentication ?

Determine if the HTTP client must authenticate with an X.509 certificate when establishing a connection to the partner's server by using the value **YES* for the "SSL" parameter. The partner's HTTP server will accept the incoming connection only in the case of successful verification of the certificate sent by the client. If not, the established connection will be closed failing identification as authorized partner trying to send data to the server.

The partner should explicitly state if this form of SSL authentication is required.

<i>*AUTO</i>	Default setting. Automatic verification if client authentication is requested from the server when connecting (SSL Handshake). If so, the corresponding certificate will be transmitted to the server, if possible.
<i>*YES</i>	Yes, Client authentication is used. This setting is valid for every connection establishment. Servers not using client authentication cause an error. Consequently, the connection will be closed.

Please note that this form of SSL authentication is requested by just a few servers and is generally not common on the Internet.

SSL Connection Certificate

By using the value **YES* in the "Use Client Authentication ?" parameter, the name of key pair containing your public key (the certificate) can be entered. This certificate is transmitted to the server. Of course, it must exist in the partner's HTTP server keystore before establishing a connection.

Description

A short description of the AS2 sending profile can be created here. This field has only a descriptive character, its content is arbitrary.

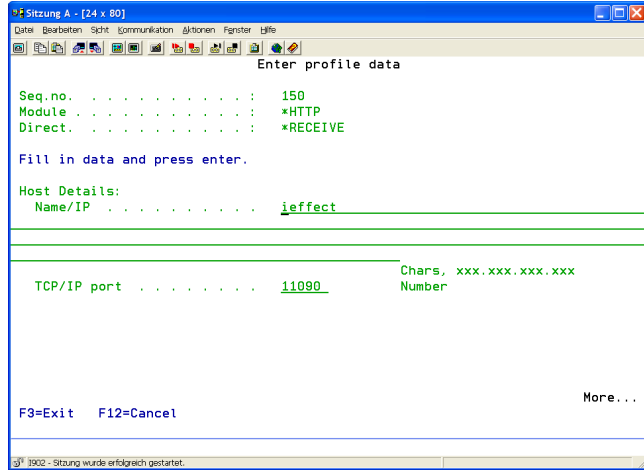
Create an HTTP Reception Profile (HTTP Server)

In order to receive HTTP POST data from a partner, an HTTP server needs to be created. Several HTTP server entities may be created on the system. Every HTTP server must be bound to a free address/port. For instance, it is possible to create an HTTP server for every partner. On the defined address/port, the HTTP server waits for inbound data.

To reach the menu where a HTTP reception profile can be added, select menu item 52 in the i-effect main menu. A list of existing communication profiles will appear.

Press F6 to call up the menu where a new communication profile can be added. Then, select HTTP communication using option number 1 in the corresponding choice box. In the following menu, please select **RECEIVE*.

The following display will appear:



The following parameters can be configured:

Host Details:

Name/IP
Enter the hostname/IP address to which the HTTP server is bound.

TCP/IP Port
The port on which the HTTP server waits for incoming connections.

HTTP Details:

Connection Timeout
Determine the timeout in seconds for an inactive connection.
Recommended value: 120 seconds.

Read Timeout
This parameter determines the time (in seconds) the HTTP server waits for data of an incoming connection. If the time has expired, a timeout error notification is sent and the connection will be closed.
Recommended value: 120 seconds.

Internal Timeout
This parameter determines a timeout value in seconds until an internal timeout is reported.

HTTP Server

Maximum Server Threads
This parameter determines the maximum number of connections an HTTP server will process at the same time. If this maximum number of simultaneous connections is reached, further incoming connections will be put into a waiting line. They are processed as soon as a free connection is available.

Reception Path
Define an IFS directory in which inbound files are stored.

Note: This parameter allows IFS directories only.

Authentication Request?
This parameter determines if authentication with user ID and password is required for connections to the server. See HTTP "Basic Authentication" (RFC 2617) for further description.
How to set up authentication data for a server as well as for a partner is described in section "User Authentication" in this chapter.

It is recommended that user authentication is activated for the server. Partner related processing of the server's received data is ONLY possible using user ID and password. For this, a partner alias (menu item 50) can be assigned to every user ID.

*YES	Yes, authentication via user ID and password is used.
*NO	No, no authentication is used

Maximum File Size

Determine the maximum file size (in KB) transmitted during a connection to the server via HTTP POST.

SSL

This parameter determines the protocol to be used by the HTTP server. Possible options are *Yes and *NO. If *NO is selected, the HTTP protocol is used. If *YES is selected, the HTTP server uses the SSL (TLS) protocol and is therefore only reachable via HTTPS connections. If option *YES is set, HTTP server settings can be specified in the parameters "Use Client Authentication?"; "Import Untrustworthy Certificates?" and "SSL Connection Certificate".

- *NO The HTTPS protocol is used.
*YES The standard HTTP protocol is used.

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.

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.

SSL Connection Certificate

Enter the name of the key pair containing the public key (certificate) in the keystore. The certificate is transmitted to every client establishing a SSL connection to the HTTP server. The server identifies itself to the client. Therefore the certificate must exist in the client's keystore before connecting.

This form of HTTPS authentication is standard practice on the Internet.

Description

A short description of the created HTTP server can be created here. This field has only a descriptive character, its content is arbitrary.

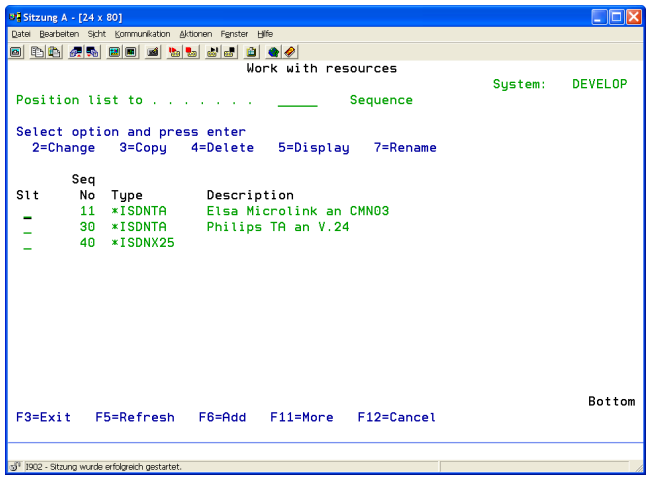
Menu Item 53: EDI- Communication Resources

Menu item 53 is only relevant if communication is to be realized via TELEBOX.

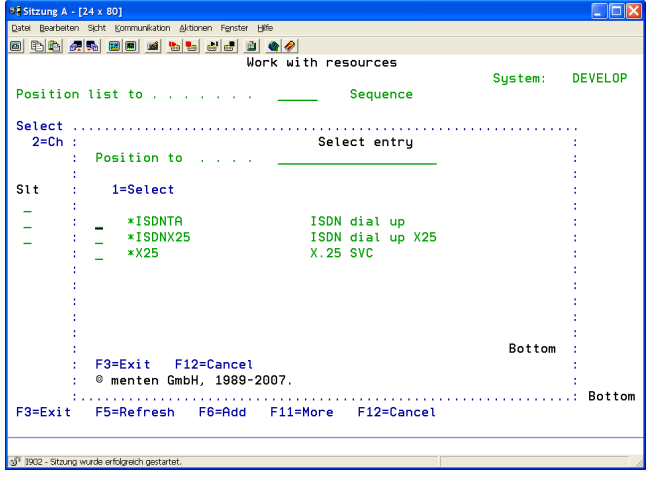
This menu serves to manage all hardware resources available for communication tasks. A hardware configuration can be assigned to the corresponding Telebox communication profile in menu item 52 (using option 8). The following hardware types are available as resources:

- o ISDN (*ISDNATA)
Digital ISDN Terminal Adapter on the AS/400 V.24
- o ISDN X25 (*ISDNX25)
X.25 ISDN Terminal Adapter on the AS/400 V.24 or X.21 on the PC.
- o X.25 SVC (*X25)
Datex-P Main Access

The following display shows menu item 53 with two created resources:



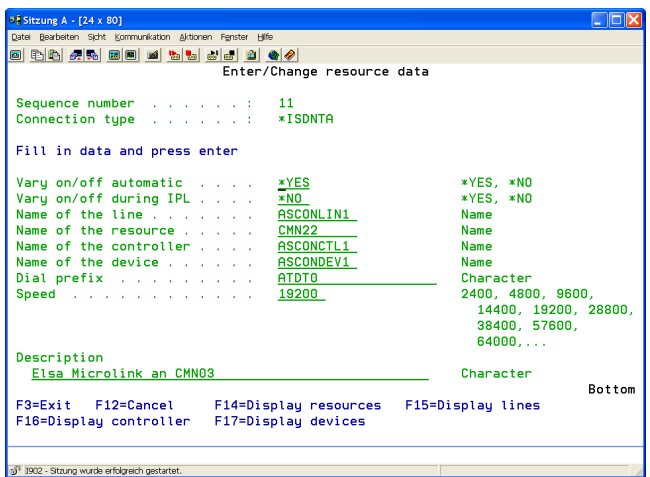
To create a communication resource, press F6. The following program interface will appear:



Select the resource type by entering option number 1 into the corresponding choice box and press enter.

Below, the different resource's parameters will be explained.

*ISDNATA Resource



Line on / off

This parameter determines if lines are to be varied on and off automatically. In this case, the line need not be activated by operating staff.

- *YES Yes, lines are varied on and off automatically
 *NO No, lines must be varied on and off by the system user

Vary on and off during IPL

Lines managed here can be varied on automatically after system reboot. This field's entry controls the IPL () value in the line description

- *YES Yes, the line is to be varied on after system reboot. IPL(*YES).
 *NO No, lines are not varied on after system reboot. IPL(*NO).

Line Name

Enter a line description name that is to be used for the resource.

Resource Name

Enter the AS/400 resource name (CMN01/LIN011...).

Controller Name

Enter a controller description name that is to be used for the resource

Device Name

Enter a device description name that is to be used for the resource

Connection Prefix

This parameter determines additional numbers to be dialed before the connection number stored in the profile-resource-allocation. Using for example ATX1DT0 a "0" is prefixed to reach a subscriber line in a telephone system

Speed

This parameter determines the resource's line speed.

Valid values: 2400,4800,9600,14400,19200,38400,57600,64000....

Description

Enter a short description of the resource entry.

***ISDNX25 Resource**

```

Sitzung A - [24 x 80]
Datei Bearbeiten Sicht Kommunikation Aktionen Fenster Hilfe
Enter/Change resource data

Sequence number . . . . . : 40
Connection type . . . . . : *ISDNX25

Fill in data and press enter

Use existing line . . . . . : *NO          *YES, *NO
Vary on/off automatic . . . . . : *YES       *YES, *NO
Vary on/off during IPL . . . . . : *YES       *YES, *NO
Name of the line . . . . . : ASCONLIN01   Name
Name of the resource . . . . . : CMN01     Name
Name of the controller . . . . . : ASCONCTL01 Name
Name of the device . . . . . : ASCONDEV01  Name
Dialin allowed . . . . . : *NO           *YES, *NO
Name of controller (dialin) . . . . . : ASCONINCTL Name
Name of device (dialin) . . . . . : ASCONINDEV Name
Dial prefix . . . . . : ATX1DT0         Character

F3=Exit  F12=Cancel  F14=Display resources  F15=Display lines  More...
F16=Display controller  F17=Display devices

31 1902 - Sitzung wurde erfolgreich gestartet.

```

Use Existing Line

This parameter determines if an already existing line description on the system will be used or a new line description is to be created. Usually, there will be an existing line if a Datex-P connection running several logical channels is in use.

- *YES Yes, an existing line is to be used.
 *NO No, a new line will be created.

Line on / off

This parameter determines if lines are to be varied on and off automatically. In this case, the line needs not to be activated by operating staff.

- *YES Yes, lines are varied on and off automatically.
 *NO No, lines must be varied on and off by the system user.

Vary on and off during IPL

Lines managed here can be varied on automatically after system reboot. This field's entry controls the IPL () value in the line description

- *YES Yes, the line is to be varied on after system reboot. IPL(*YES).
 *NO No, lines are not varied on after system reboot. IPL(*NO).

Line Name

Enter a line description name that is to be used for the resource.

Resource Name

Enter the AS/400 resource name (CMN01/LIN011....).

Controller Name

Enter a controller description name that is to be used for the resource.

Device Name

Enter a device description name that is to be used for the resource.

Dial-in allowed?

For certain communication modules (e.g. OFTP), the partner's dial-in to this AS/400 system can be allowed. This parameter determines if this is generally allowed for this resource

- *YES Yes, dial-in for certain modules is allowed.
- *NO No, dial-in for this resource is not allowed.

Controller Name (dial-in)

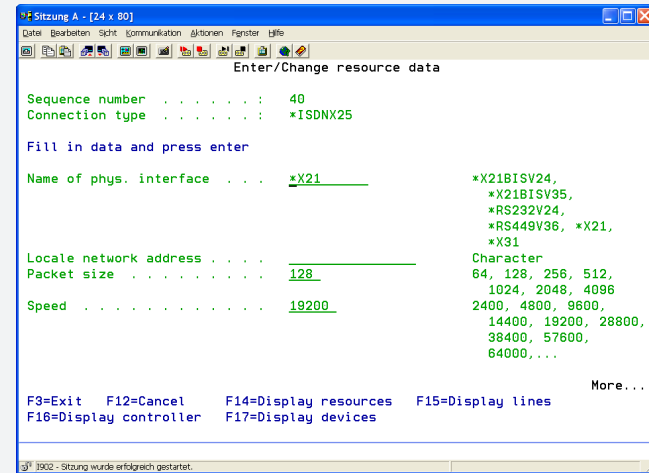
Enter, if allowed, a controller description name which is to be used here

Device Name (dial-in)

Enter, if allowed, a device description name that is to be used here

Connection Prefix

This parameter determines additional numbers to be dialed before the connection number stored in the profile-resource-allocation. Using for example ATX1DT0 a "0" is prefixed to reach a subscriber line in a telephone system.



```

Sitzung A - [24 x 80]
Datei Bearbeiten Sicht Kommunikation Aktionen Fenster Hilfe
Enter/Change resource data

Sequence number . . . . . : 40
Connection type . . . . . : *ISDNX25

Fill in data and press enter

Name of phys. interface . . . : *X21                *X21BISV24,
                                                *X21BISV35,
                                                *RS232V24,
                                                *RS449V36, *X21,
                                                *X31
Locate network address . . . . :                    Character
Packet size . . . . . : 128                        64, 128, 256, 512,
                                                1024, 2048, 4096
Speed . . . . . : 19200                            2400, 4800, 9600,
                                                14400, 19200, 28800,
                                                38400, 57600,
                                                64000, ...

F3=Exit  F12=Cancel  F14=Display resources  F15=Display lines
F18=Display controller  F17=Display devices

1002 - Sitzung wurde erfolgreich gestartet.

```

Name of Physical Interface

Enter the name of the interface to which the resource is connected.

Possible values: *X21BISV24, *X21BISV35, *RS232V24, *RS449V36, *X21, *X31

Local Network Address

Enter the address (connection number) allocated to the line.

Packet Size

Enter the packed size to be used.

Possible values: 64, 128, 256, 512, 1024, 2048, 4096

Speed

This parameter determines the resource's line speed.

Valid values: 2400,4800,9600,14400,19200,38400,57600,64000....

Description

Enter a short description of the resource entry.

***X25 Resource**

```

Enter/Change resource data

Sequence number . . . . . : 50
Connection type . . . . . : *X25

Fill in data and press enter

Use existing line . . . . . : *NO          *YES, *NO
Vary on/off automatic . . . . : *YES     *YES, *NO
Vary on/off during IPL . . . . : *YES     *YES, *NO
Name of the line . . . . . : ASCONLIN    Name
Name of the resource . . . . . : CMN01     Name
Name of the controller . . . . : ASCONCTL  Name
Name of the device . . . . . : ASCONDEV    Name
Dialin allowed . . . . . : *NO          *YES, *NO
Name of controller (dialin) . . : ASCONINCTL Name
Name of device (dialin) . . . . : ASCONINDEV Name
Dial prefix . . . . . : ATX1DT0      Character

F3=Exit  F12=Cancel  F14=Display resources  F15=Display lines
F16=Display controller  F17=Display devices

More...

1902 - Sitzung wurde erfolgreich gestartet.

```

Use Existing Line

This parameter determines whether an existing line description on the system will be used or a new line description is to be created. Usually there will be an existing line if a Datex-P connection running several logical channels is in use.

- *YES Yes, an existing line is to be used.
- *NO No, a new line will be created.

Line on / off

This parameter determines if lines are to be varied on and off automatically. In this case, the line needs not to be activated by operating staff.

- *YES Yes, lines are varied on and off automatically.
- *NO No, lines must be varied on and off by the system user.

Vary on and off during IPL

Lines managed here can be varied on automatically after system reboot. This field's entry controls the IPL () value in the line description

- *YES Yes, the line is to be varied on after system reboot. IPL(*YES).
- *NO No, lines are not varied on after system reboot. IPL(*NO).

Line Name

Enter a line description name that is to be used for the resource.

Resource Name

Enter the AS/400 resource name (CMN01/LIN011....).

Controller Name

Enter a controller description name that is to be used for the resource.

Device Name

Enter a device description name that is to be used for the resource.

Dial-in allowed

For certain communication modules (e.g. OFTP), the partner's dial-in to this AS/400 system can be allowed. This parameter determines if this is generally allowed for this resource.

- *YES Yes, dial-in for certain modules is allowed.
- *NO No, dial-in for this resource is not allowed.

Controller Name (dial-in)

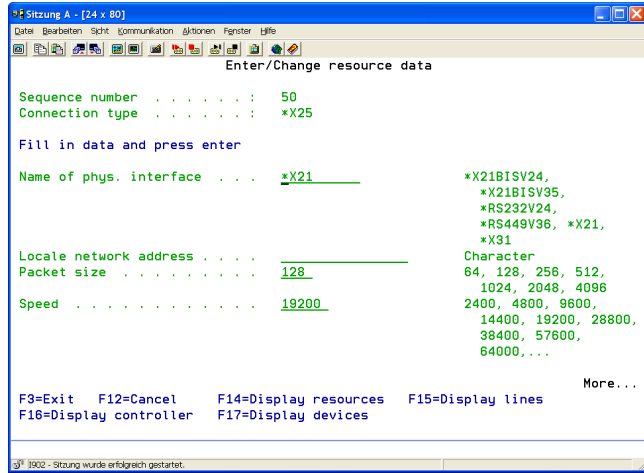
Enter, if allowed, a controller description name which is to be used here.

Device Name (dial-in)

Enter, if allowed, a device description name that is to be used here.

Connection Prefix

This parameter defines additional numbers to be dialed before the connection number stored in the profile-resource-allocation. Using for example ATX1DT0 a "0" is prefixed to reach a subscriber line in a telephone system.



Name of Physical Interface

Enter the name of the interface to which the resource is connected.

Possible values: *X21BISV24, *X21BISV35, *RS232V24, *RS449V36, *X21, *X31

Local Network Address

Enter the address (connection number) allocated to the line.

Packet Size

Enter the packed size to be used.

Possible values: 64, 128, 256, 512, 1024, 2048, 4096

Speed

This parameter determines the resource's line speed

Valid values are 2400,4800,9600,14400,19200,38400,57600,64000....

Description

A short description of the resource entry.

User Authentication for Communication Servers

User authentication is only available for modules *HTTP and *OFTP.

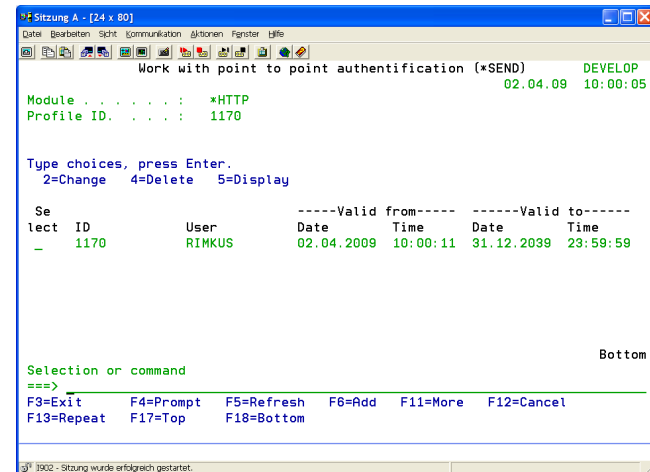
Using user authentication, it is possible to manage every partner's access to i-effect communication servers by user ID/password. Linking these credentials with a partner profile from menu item 50, partner controlled processing of received data is possible. User data can be entered into the particular server profile (*RECEIVE) in menu item 52.

For user authentication by user ID/password on a remote server, credentials can be allocated to a sending profile (*SEND) in menu item 52.

For more flexibility in administration and more security, it is possible to define validity periods for all credentials. It is no problem if periods overlap because in this case, the first valid entry is used for authentication.

To reach the menu where user data can be generated, select menu item 52 in the i-effect main menu. A list of existing *HTTP and *OFTP communication profiles will appear. Select the desired *RECEIVE or *SEND communication profile and enter option number 12 in the corresponding choice box.

The following display (example of a HTTP *SEND profile with one created user for authentication on the remote side) will appear:



Dialog Program 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. The following overview describes the available options of the program interface, followed by a more detailed description.

- | | |
|---------------------------|---|
| Add (option F6) | With option F6 a new user ID and password will be created and linked to the user in the corresponding partner profile in menu item 50. |
| Change (option 2) | To change an entry, use option 2 in the corresponding choice box. Only the validity period can be modified for an existing user. Once created, user ID, password and corresponding partner cannot be changed. |
| Copy (option 3) | To copy an existing user entry to a new alias name, use option 3 in the corresponding choice box. |
| Delete (option 4) | To delete an entry, use option 4 in the corresponding choice box. |
| Display (option 5) | To display an entry, use option 5 in the corresponding choice box. |

User Authentication for HTTP Servers

This section describes how to create a user for authentication on HTTP servers. A distinction between authentication on a local i-effect HTTP Server (*RECEIVE) and a remote HTTP Server (*SEND) is made.

Authentication on Remote HTTP Servers

If login with user ID and password is required to connect with an HTTP server, these credentials can be defined for an HTTP sending profile. Once they exist in the sending profile, they will be transmitted automatically to the remote server. If several credentials are defined, the entry matching the validity period is used for authentication.

Call up menu item 52. Select the desired HTTP sending profile and enter option number 12 in the corresponding choice box. In the following program interface press F6.

The following display will appear:

The screenshot shows a window titled 'Sitzung A - [24 x 80]' with a menu bar (Datei, Bearbeiten, Sicht, Kommunikation, Aktionen, Fenster, Hilfe) and a toolbar. The main area is titled 'Add entry' and contains the following text:

```

DEVELOP
02.04.09 10:01:42
Module . . . . . : *HTTP
Profile . . . . . : 1170

Input data, press enter.

User data:
User . . . . . : _____
Password . . . . . : _____
Valid from:
From date . . . . . : 02.04.09      Date, *LOVAL
From time . . . . . : 10:01:44     Time, *LOVAL
Valid until:
Until date . . . . . : 31.12.39      Date, *HIVAL
Until time . . . . . : 23:59:59     Time, *HIVAL

Bottom
F3=Exit  F4=Prompt  F12=Cancel
  
```

At the bottom of the window, a status bar displays '31 1902 - Sitzung wurde erfolgreich gestartet.'

User Details

Enter user authentication data for server login.

User ID

Enter the user ID to be used for HTTP server login.

Password

Enter the password to be used for HTTP server login.

Start of Validity Period:

Determine the starting point of the validity period.

From Date

Enter the starting date of the validity period.

From Time

Enter the starting time of the validity period.

End of Validity Period:

Determine the end of the validity period. User data will lose its validity and cannot be used anymore.

To Date

Enter the date when user data will lose its validity.

To Time

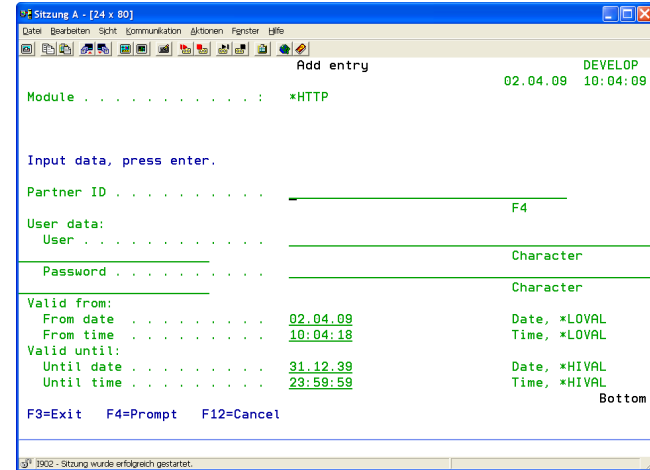
Enter the time when user data will lose its validity.

Authentication on the i-effect HTTP Server

For user/partner authentication on an i-effect *HTTP server, it is possible to create user accounts for every *HTTP server defined in the system. A user who wants to send data to the *HTTP server must login with user ID and password. Every user account requires a partner profile (menu item 50) to which it is allocated. This allows processing of received data according to the corresponding without any problems. It is no problem if several user accounts are allocated to one partner because in this case, the account with a matching validity period is used for authentication.

To create a user account for a *HTTP server, call up menu item 52. Select the desired HTTP server profile (*RECEIVE) and enter option number 12 in the corresponding choice box. In the following program interface press F6.

The following display will appear:



```

Sitzung A - [24 x 80]
Datei Bearbeiten Sicht Kommunikation Aktionen Fenster Hilfe
Add entry
Module . . . . . : *HTTP
Partner ID . . . . . : F4
User data:
User . . . . . :
Password . . . . . :
Valid from:
From date . . . . . : 02.04.09
From time . . . . . : 10:04:18
Valid until:
Until date . . . . . : 31.12.39
Until time . . . . . : 23:59:59
Bottom
F3=Exit F4=Prompt F12=Cancel
3002 - Sitzung wurde erfolgreich gestartet.
  
```

Partner ID

Enter the partner ID of the partner profile created in Partner Master Data, menu item 50. The user account is then allocated to this profile. Use function key F4 to display a list of all created partner profiles.

User Details

Enter user authentication data for server login.

User ID

Enter the user ID to be used for HTTP server login.

Password

Enter the password to be used for HTTP server login.

Start of Validity Period:

Determine the starting point of the validity period.

From Date

Enter the starting date of the validity period.

From Time

Enter the starting time of the validity period.

End of Validity Period:

Determine the end of the validity period. User data will lose its validity and cannot be used anymore.

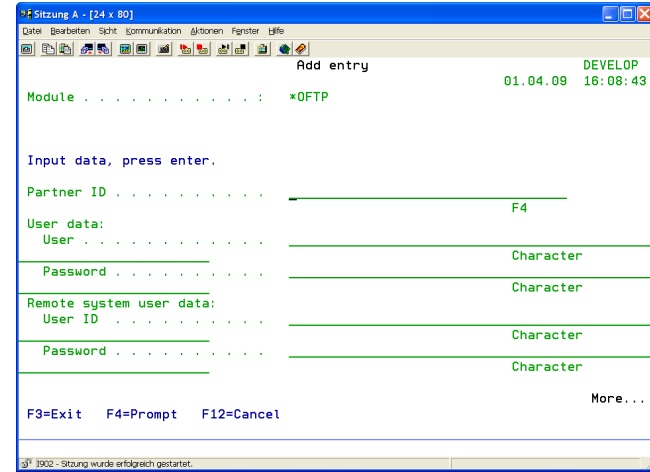
To Date

Enter the date when user data will lose its validity.

To Time

Enter the time when user data will lose its validity.

The following display will appear:



Authentication on the i-effect OFTP Server

For user/partner authentication on an i-effect *OFTP server, it is possible to create user accounts for every *OFTP server defined in the system. A user who wants to send data to the *OFTP server will must login with user ID and password. Then, the server identifies to the client using the used ID and password created for the client. Every user account requires a partner profile (menu item 50) to which it is allocated. This allows partner controlled processing of received data without any problems. It is no problem if several user accounts are allocated to one partner because in this case, the account with a matching validity period is used for authentication.

To create a user account for a *OFTP server, call up menu item 52. Select the desired *OFTP server profile (*RECEIVE) and enter option number 12 in the corresponding choice box. In the following program interface press F6.

Partner ID

Enter the partner ID of the partner profile created in Partner Master Data, menu item 50. The user account is then allocated to this profile. Using function key F4, a list of all created partner profiles will appear.

User Details

Enter user authentication data for *OFTP server login.

User ID

Enter the user ID used for client authentication on the *OFTP server.

Password

Enter the password used for client authentication on the *OFTP server.

User Details Remote Side

Enter user authentication data for server login.

User ID

Enter the user ID to be used for *OFTP server login.

Password

Enter the password to be used for *OFTP server login.

Start of Validity Period:

Determine the starting point of the validity period.

From Date

Enter the starting date of the validity period.

From Time

Enter the starting time of the validity period.

End of Validity Period:

Determine the end of the validity period. User data will lose its validity and cannot be used anymore.

To Date

Enter the date when user data will lose its validity.

To Time

Enter the time when user data will lose its validity.