

Chapter 6

Communication

This chapter contains information about i-effect's many types of communication. The chapter is divided according to communications channels into the following sections:

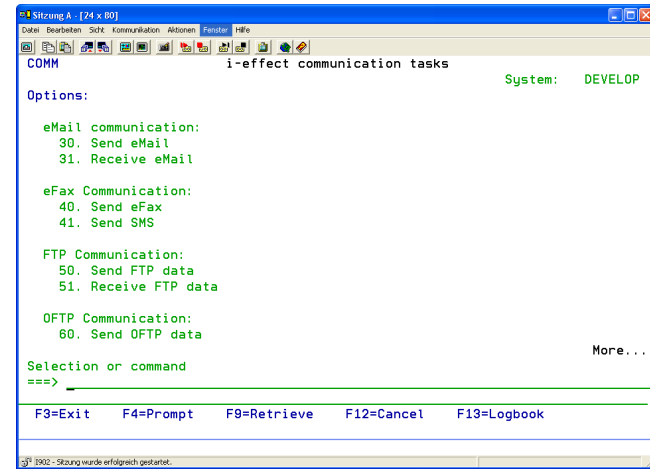
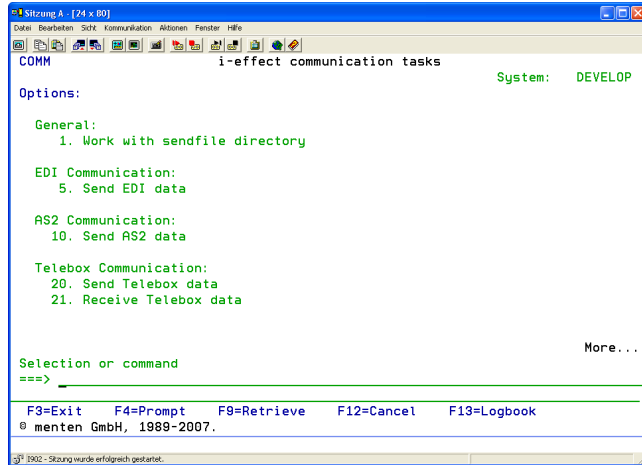
- o AS2
- o Telebox
- o Email
- o eFax/SMS
SMS transmission is performed by the FAX module and is included in this subchapter.
- o FTP
- o OFTP
- o HTTP

To reach the communications tasks, select 13 from i-effect's main menu. This selection opens a menu in which all communications tasks are listed. From here all supported communications types can be used.

In the section "old commands" all commands that are retained in i-effect for compatibility, but not reachable from menu 13, can be found. These commands must be entered manually.

Currently, the *SPOOL module is effected.

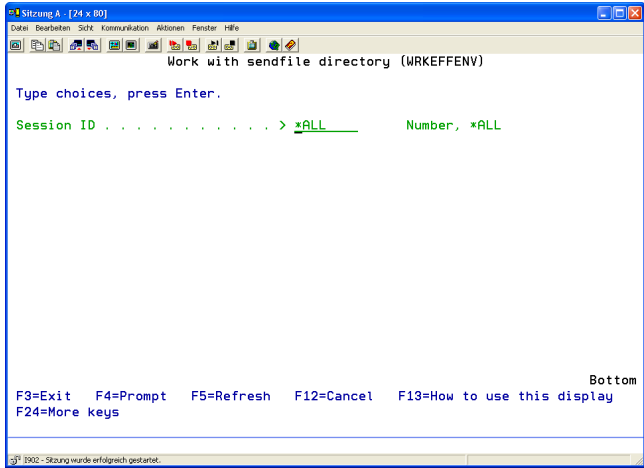
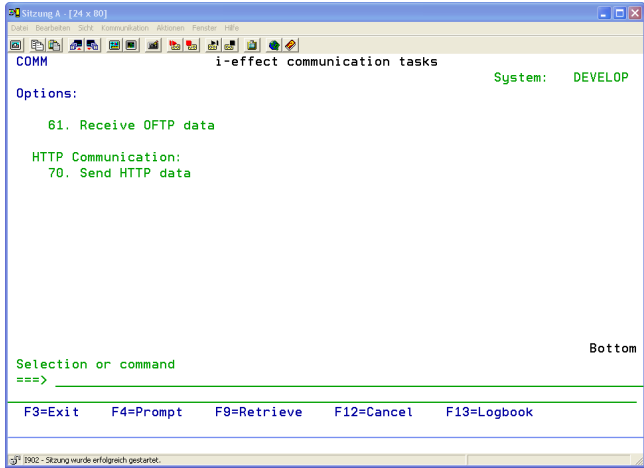
In the section "General commands" commands that are used for more than one communication type are found.



Explanation of the menu items:

- Work with Sendfile Directory (Option 1)** Select this menu item to work with i-effect's sendfile directory.
- Send EDI Data (SNDFILE) (Option 5)** Select this option to send EDIFACT files.
- Send AS2 Data (Option 10)** Use this option to send files via AS2.
- Send Telebox Data (Option 20)** Use this menu item to send data via Telebox.
- Receive Telebox Data (Option 21)** Use this menu item to receive data via Telebox.

- Send email (Option 30)** Use this menu item to send text or file attachments via email.
- Retrieve email (Option 31)** Use this menu item to retrieve email from an inbox.
- Send eFax (Option 40)** Use this menu item to send existing PDF files as a fax. The files will be sent by the *EMAIL module to an Internet service provider who, then sends the telefax to the designated recipient.
- Send SMS (Option 41)** Use this menu item to send text as an SMS. The text will be sent by the *EMAIL module to an Internet service provider, who then sends the SMS to the designated recipient.
- Send FTP Data (Option 50)** Use this menu item to send data via FTP.
- Receive FTP Data (Option 51)** Use this menu item to receive data via FTP.



- Send OFTP Data (Option 60)** Use this menu item to transmit data via OFTP.
- Retrieve OFTP Data (Option 61)** Use this menu item retrieve data from an OFTP server.
- Send HTTP Data (Option 70)** Use this menu item to transmit data via HTTP POST.

Session ID

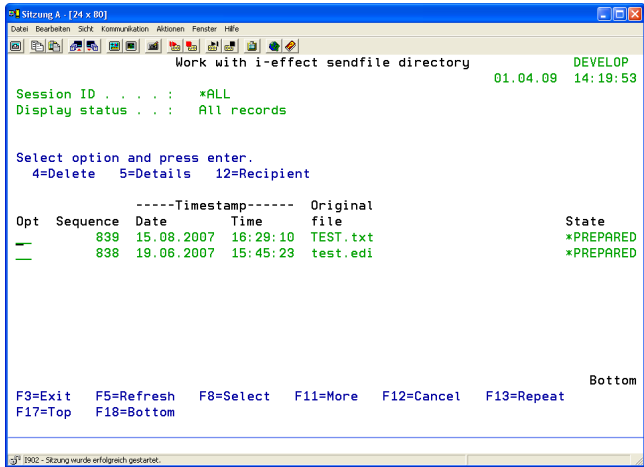
Session number, in which the transmission preparations are carried out.

Possible Values:

- *ALL All transmission preparations will be selected (default).
- Number Only the preparations of the session number entered here will be displayed.

**Menu Item 1:
Work with Sendfile Directory (WRKEFFENV)**

The command "Work with Sendfile Directory" opens a display for management of files in the sendfile directory. The sendfile directory contains a list of the data and files which are ready to be sent. Entries can be added, edited, and deleted using this dialogue.



To edit the entries, the following option can be used. Therefore, 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.

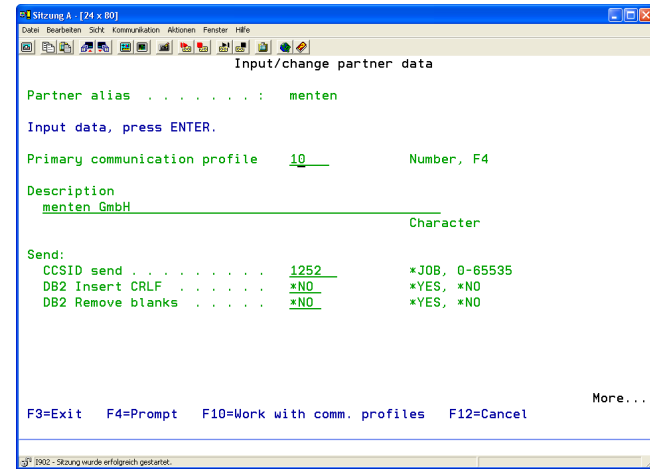
| | |
|---------------------------------|--|
| Add (Option F6) | F6 adds a new communications resource. In the following dialogue the communications resources of the installed i-effect modules can be selected. |
| Delete (Option 4) | Enter option 4 in the corresponding choice box to delete an entry. |
| Details (Option 5) | Enter option 5 in the selection column of the corresponding choice box to display details of existing entries. |
| Prepare again (Option 9) | Enter option 9 into the selection column of the corresponding choice box to prepare the entry again. |
| Recipient (Option 12) | Enter option 12 in the selection column of the corresponding choice box to display the recipient of the existing entry. |

EDI Communication

Menu Item 5: Send EDI Data (SNDFILE)

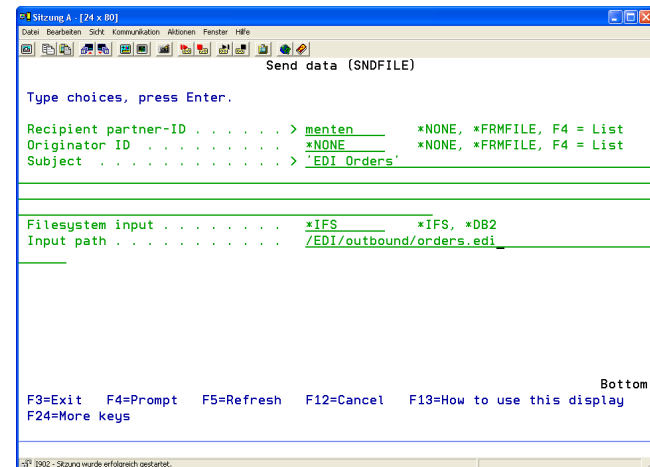
The SNDFILE command sends any file(s) via predefined partner and communication profiles. Licenses for the i-effect *BASE module and all participating i-effect communications or conversion (if conversion is required before transmission) modules are required.

When SNDFILE is used for transmission the partner and the communications channel are supplied by the recipient GLN in the outbound EDIFACT file. The program will only search for one partner with this exact GLN in the i-effect partner master data, and this partner's primary communications profile will be supplied. For this to function properly, the partner must already exist in the i-effect partner master data (menu 50) with this EXACT GLN as an alias. This partner must also have a primary communications profile. This communications profile will be used for SNDFILE for transmission of the EDFICAT file.



Chapter 9 "Master Data in i-effect" contains more information about adding partners and communications profiles.

- 1) Select menu item 5 "Send EDI Data" from the menu "i-effect Communications Tasks" or enter the command SNDFILE and F4.
- 2) Enter the desired parameter according to the following parameter explanations.



Recipient Partner ID (PARTNER)

Here it is possible to refer to a partner profile from the partner master data (see menu item 50). Definitions made there must not be re-entered here or after.

The following special values are possible:

| | |
|-----------------|---|
| <i>*NONE</i> | No partner-ID will be allocated. |
| <i>*FRMFILE</i> | The partner will be taken from the recipient GLN in the EDIFACT file. |
| <i>Text</i> | Enter a recipient partner-ID. |

Originator ID (ORIGINATOR)

Here it is possible to refer to an originator profile in the master data from menu item 51.

Subject (SUBJECT)

Text entered here will be sent as the message's subject.

File System Input (FS)

Enter the file system of the input file.

The following options are available:

| | |
|-------------|--|
| <i>*IFS</i> | The input file is in the IFS (Integrated File System). |
| <i>DB2</i> | The input file is in the DB2 file system. |

From File (FRMFILE)

The input file to be transmitted, is entered here.

The following options are available:

| | |
|-----------------|---|
| <i>*ALL</i> | All files in the source directory or library will be transmitted. |
| <i>Name</i> | Enter the name of the input file. |
| <i>generic*</i> | Use "*" as a wild card for generic input file selection. |

The parameter consists of 2 elements:**Library**

The library of the source file in the DB2 file system.

Member File

The source member file in the DB2 file system.

Possible Special Value:

| | |
|-------------|--|
| <i>*ALL</i> | All source member files in the DB2 input file will be transmitted. |
|-------------|--|

Input Path (FRMPATH)

Enter the path for the IFS input file.

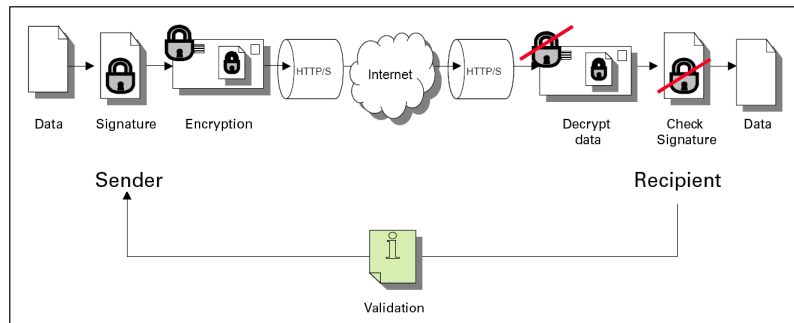
AS2 Communication

Note: Licenses for the i-effect modules *BASE, *AS2, and *CRYPT are required in order to use the following functions.

What is EDIINT AS2 ?

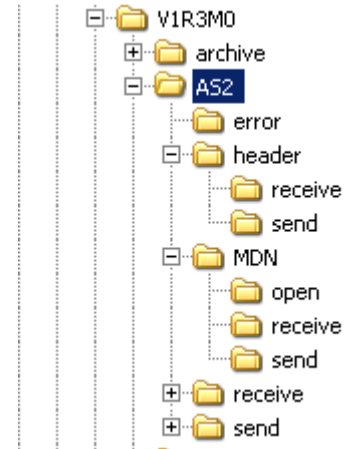
EDIINT (EDI over the Internet) was designed by the Internet Engineering Task Force (IETF). There are three specifications for this standard: AS1, AS2, and AS3 (Applicability Statement). These standards define communications profiles for secure and traceable data exchange over the Internet. AS1 transmits data over SMTP (Simple Mail Transfer Protocol), AS2 uses HTTP (Hypertext Transfer Protocol). This creates a direct connection for partners in the form of a point-to-point (Peer2Peer) connection to transmit data securely and in real-time. Electronic business documents in any desired format (EDI, XML, CSV, txt etc.) can be encrypted and signed electronically, and then transmitted to partners. EDIINT AS2 offers an inexpensive way for data exchange unlike Value Added Networks (VAN), which have higher user fees. Delays, which often occur with VANs because of batch transmission, are also avoided.

AS2 Communication Cycle:



i-effect *AS2's Default Working Directory

After i-effect has been successfully installed on the System i, the following directory structure that is relevant for the *AS2 module is found in the directory /i-effect/<version>. These directories are created during installation and are the default working directories for AS2.



- /i-effect/<version>/as2/error** Files not successfully sent or received are saved in this directory.
- /i-effect/<version>/as2/header/receive** Header files of AS2 messages that are successfully received are saved here.
- /i-effect/<version>/as2/header/send** Header files of successfully sent AS2 messages are saved here.
- /i-effect/<version>/as2/MDN/receive** MDNs that were successfully received and are without errors are saved here.
- /i-effect/<version>/as2/MDN/send** MDNs that were successfully sent and are without errors are saved here.

| | |
|---|---|
| /i-effect/<version>/as2/MDN/open | AS2 messages received with asynchronous MDN (Message Disposition Notification) request are saved in this temporary working directory. AS2 messages with an asynchronous MDN request will be saved in this directory, i.e. as an AS2 file after they are decrypted and verified, until the asynchronous MDN has been successfully sent back to the originator of the AS2 message. After the asynchronous MDN has successfully been returned to the AS2 message's sender, the AS2 message and the files belonging to it (file attachments, message header file, and MDN file) will be save in the appropriate directory. If an error occurs when returning the asynchronous MDN, all the corresponding files will be saved in the directory: /i-effect/<version>/as2/error. |
| /i-effect/<version>/as2/receive | File attachments of successfully received AS2 messages are saved here. |
| /i-effect/<version>/as2/send | Default IFS path from which data for transmission is selected. |

i-effect *AS2 Keystore

AS2's security features (encryption and digital signature) can only be used if a keystore with a keypair (private and public key) and the partner's certificates is maintained.

The *CRYPT module must first be configured so that AS2 can access the keystore. Setup of the keystore and the *CRYPT module is described in chapter 7a "Encryption and Advanced Electronic Signature". Other terms, such as keystore and certificate, are also defined and explained there in detail.

Configuration of the AS2 Subsystems

Requirements for i-effect *AS2

In order to use i-effect *AS2 certain requirements must be met and/or certain configurations must be made. An overview of the most important infrastructure requirements is listed here:

- o Internet access with a fixed or dynamic IP address.
- o Access to a DNS server to resolve host names and IP addresses
- o At least two open ports (1024<Port<=65535) for AS2 communication of AS2 client and AS2 server. The default AS2 port for HTTP is 4080.
- o If required, the port must be available for the AS2 server using the partner's IP address on the firewall.

If required, the public IP address/port must be changed to the IP address of the System i.

Configuration of the *AS2 Module

To start AS2 as a subsystem on the System i, certain profiles must be created and configured, as well as EDI partner master data added or existing master data complemented with the relevant AS2 parameters.

The basic configuration of the AS2 module can be see in Chapter 11 "Administration in i-effect." The "Additional Parameters of the *AS2 Module" explains the section parameters and the basic settings for AS2.

Adding of Communications Resources

In order to use i-effect AS2, it is necessary to add certain master data and communications profiles. The following changes must be made:

For reception of AS2 messages:

- o Adding one or more AS2 servers (HTTP/HTTPS).

To send AS2 messages:

For each AS2 communications partner the following must be changed:

- o create one AS2 sending profile
- o the partner must be added to the EDI master data
- o The partner must be linked with the newly created AS2 sender profile.

Once:

Creation of a AS2 sender partner that contains the sender specific AS2 data. This sender can be added by entering parameters when SNDAS2 is called up. i-effect AS2 uses these as the sender parameters for transmission.

A detailed explanation of communications profile and master data creation can be found in Chapter 10 "Master Data in i-effect" under the description of menu item 50, 51, and 52.

Links:

- Chapter 10 - Master Partner Data for the *AS2 Module
- Chapter 10 - Originator Details for the *AS2 Module
- Chapter 10 - Menu Item 52 – Create AS2 Communication Profiles

Menu Item 10: Send AS2 Data (SNDAS2)

The command SNDAS2 is used to send AS2 data. The AS2 is a standard for transmission of B2B data via HTTP to defined business partners. Licenses for the *BASE, *CRYPT, and *AS2 modules are required to use these functions.

A license for the *ZIP module is also required in order to send compressed AS2 messages.

Select menu item 13 "Communication Tasks" from the i-effect main menu to reach. From there select menu item 10 "Send AS2 Data."

The command SNDAS2 followed by F4 can also be entered directly from the i-effect main menu.

The following display will appear:

This dialogue is used to set the send parameters. A partner or a profile can be specified, from which the parameter information will be taken. A sender profile can also be specified, which can be selected from the list that appears when F4 is pressed.

The number of parameters that must be entered manually depends on whether a receiver and/or sender partner was specified in SNDAS2.

Explanation of the parameters:

Recipient Partner ID (PARTNER)

A partner profile entered in the master data under menu item 50 can be referred to here.

The following special values are possible:

| | |
|-----------------|--|
| <i>*NONE</i> | No receiver partner ID will be assigned. The required specifications for the recipient must be entered manually in the parameters of this command. |
| <i>*FRMFILE</i> | The partner alias will be taken from the EDIFACT file (recipient in the UNB segment). |
| <i>Text</i> | Enter the recipient partner ID. |

Profile No. (PROFILE)

A communications profile that was entered in menu item 52 of the master data can be referred to here.

The following special values are possible:

| | |
|--------------|--|
| <i>*NONE</i> | No communications profile will be assigned. The specifications required by the remote system must be entered manually in the parameters of this command. |
| <i>Text</i> | Enter a communications profile ID. |

Originator Alias (ORIGINATOR)

A sender profile from the master data from menu item 51 can be referred to here.

The following special values are possible:

| | |
|--------------|--|
| <i>*NONE</i> | No sender profile will be assigned. The required specifications for sender must be entered manually in the parameters of this command. |
| <i>Text</i> | Enter the originator profile ID. |

File System (FS)

Enter the file system of the input file.

The following options are available:

| | |
|-------------|---|
| <i>*IFS</i> | The AS2 source file is in the IFS (Integrated File System). |
| <i>*DB2</i> | The AS2 source file is in the DB2 file system. |

Please do always select the file system *IFS, even if a file in the DB2 system should be sent. Only then is it possible to enter wild cards for a name of DB2 files in the input path parameter. Example: /QSYS.LIB/MEINE.LIB/ODERS.FILE/*TEST*.MBR

Input File (FRMFILE)

The AS2 input file to be sent should be entered here.

The following options are available:

| | |
|-----------------|--|
| <i>*ALL</i> | All files in the source directory/ library will be sent. |
| <i>Name</i> | Enter the name of an AS2 input file. |
| <i>generic*</i> | Use "*" as a wild card for generic AS2 input file selection. |

Transmission of multiple files is not supported by the current AS2 version. For this reason, always enter a file name here.

This parameter consists of 2 elements:

Library

The library of the AS2 source file in the DB2 file system.

Member File

The AS2 member source file in the DB2 file system.

Possible Special Value:

| | |
|-------------|---|
| <i>*ALL</i> | All source member files of the DB2 input file will be sent. |
|-------------|---|

Input Path (FRMPATH)

Enter the path for the IFS input file.

Content Type (CONTENTT)

Determines the content type of the AS2 message.

| | |
|-----------------|---|
| <i>*CONSENT</i> | The AS2 message contains EDI data 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 will be taken from the file ending of the input file(.edi = application/EDIFACT). If <i>*FRMFILE</i> is selected for DB2 files the Content-Type is always <i>*BINARY</i> (application/octet-stream), because DB2 files do not have a typical file ending. |
| <i>*DEFAULT</i> | The data content type will be taken from the default setting of the AS2 module. (See menu 80) |

Broadcast File Name (BROADCAST)

Enter the name that is assigned to the AS2 input file being transmitted. This name will be placed in the header of the AS2 message sent with it.

Possible Special Values:

| | |
|-----------------|---|
| <i>*FRMFILE</i> | The alias name will be taken from the name of the input file. |
|-----------------|---|

Subject

The subject of the AS2 message is entered here.

Signature (SIGN)

This parameter determines if a signature will be assigned to this AS2 message. A message that is electronically signed with this parameter, can be checked for its integrity and its original source by the recipient using the public key.

This parameter consists of 2 elements

If the first element is set to **DEFAULT*, the values for the first two elements will be taken from the AS2 module's master data from menu item 80.

Algorithm

The first element determines the signature algorithm.

| | |
|-----------------|-------------------|
| <i>*DEFAULT</i> | Standard setting. |
|-----------------|-------------------|

The master data of the i-effect **AS2* module will be used to determine the signature algorithm (see menu item 80).

| | |
|--------------|--------------|
| <i>*NONE</i> | No Signature |
|--------------|--------------|

The AS2 message will NOT be signed.

| | |
|-------------|---------------|
| <i>*MD5</i> | MD5 Signature |
|-------------|---------------|

MD5 will be used to generate the signature. MD5 (Message Digest Algorithm 5) is a well know cryptographic hash function that creates a 128 bit hash value.

| | |
|--------------|----------------|
| <i>*SHA1</i> | SHA1 Signature |
|--------------|----------------|

SHA-1 will be used to generate the signature. The secure hash algorithm, SHA, is a group of standardized cryptographic hash functions. SHA-1 is a cryptographic hash function, that creates a 160 bit hash value.

Keystore Alias

This entry names the key pair in the keystore. The private key of this key pair is used to sign the AS2 message.

Encryption (ENCRYPT)

This parameter determines if AS2 messages will be encrypted. The message will be encrypted with the certificate (public key) of the recipient. The recipient can only decrypt the message with the corresponding private key.

This parameter consists of 2 elements

If the first is set to **DEFAULT* entered as its value, the values for the first two elements will be taken from the AS2 module's master data from menu item 80.

Algorithm

The first element determines the signature algorithm.

| | |
|-----------------|-------------------|
| <i>*DEFAULT</i> | Standard setting. |
|-----------------|-------------------|

The encryption algorithm will be taken from the master data in the i-effect **AS2* module.

| | |
|--------------|----------------|
| <i>*NONE</i> | No encryption. |
|--------------|----------------|

The AS2 message will not be encrypted.

**TRIPLEDES* 3DES 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).

Keystore Alias

This entry determines the key pair in the keystore. The public key of this key pair is used to encrypt the AS2 message.

Proxy Server (PROXY)

A proxy server (representative computer server or program) is a service program for computer networks, that mediates data communication. Data transfer with a proxy server is more efficient (lower network load through large data volume) and can increase security. If a proxy server is used in the network, the required parameters to access the server can be determined here.

This parameter consists of 4 elements.

If the first element has *DEFAULT entered as its value, the values for the first two elements will be taken from the AS2 module's master data from menu item 80.

DNS Name or IP

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

Port

Enter the TCP/IP port.

User Name

Enter (if required) the authorized user's ID.

Password

Enter (if required) the authorized user's password.

AS2 Server (SERVER)

This parameter consists of 8 elements that contain specifications of the AS2 server (target system).

DNS Name or IP

The first element is the name of the AS2 server. An IP address or a DNS name of the AS2 server can be entered here.

TCP/IP Port

The second element specifies the port which receives AS2 server tasks.

AS2-TO

The third element specifies the AS2 recipient. This is the AS2 ID of the partner. This ID is placed in the headers of the AS2 message and is sent with the message.

Connection Timeout

The fourth element specifies the timeout for connections. This value is the time in seconds, that the server waits until a connection is established, after this time a timeout error will occur. (e.g. when the target server does not answer).

Recommended value: 120 seconds.

Read Timeout

The fifth element determines a read-timeout. This value is the time in seconds, that the client waits when read request is made before a timeout error occurs.

Recommended value: 120 seconds.

Maximum Send Retries

The sixth element is the maximum number of transmission retries. A retry is started when a message cannot be delivered because of an error (e.g. the target system did not respond).

Retry Pause

The seventh element is the break between retries. Enter the length of the pause in seconds between retries.

Content-Disposition

This parameter determines how the payload of the AS2 message are labeled. This value should normally be set to the default setting *ATTACH.

AS2 communications partners should specify if *INLINE is required.

| | |
|---------|--|
| *ATTACH | (Default)The payload will be labeled as an "attachment." |
| *INLINE | The payload will be labeled as "inline." |

Protocol (PROT)

This parameter consists of six elements and determines the protocol for connection setup to the target AS2 server and other settings regarding MDNs (Message Disposition Notification).

MDN is a basic component of AS2. The recipient of the AS2 message (or the AS2 system of the recipient) sends them back to the sender to confirm reception. This guarantees the sender that the recipient received the document, and that the recipient did not reject it. This means that the recipient cannot claim that the document was not received. The sender determines how an MND will be sent: synchronously/asynchronously and signed/not signed.

Protocol

The first element determines the transmission protocol for AS2 messages.

Possible special values:

| | |
|----------|--|
| *DEFAULT | Specifies that the current value for this parameter should be taken from the AS2 module's master data. |
| *HTTP | The message will be sent by the HTTP protocol. |
| *HTTPS | The message will be sent by the HTTPS protocol. |

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. This protocol must agree with the protocol of the *AS2 server that is defined as the MDN recipient server.

Possible special values:

| | |
|--------|---|
| *HTTP | The HTTP protocol will be used to transmit MDNs. |
| *HTTPS | The HTTPS protocol will be used to transmit MDNs. |

MDN Address

The fifth element is the address of the MDN's recipient. All requested asynchronous MDNs will be sent to this address. The address is the external DNS name or the external IP address of the originators AS2 server when using HTTP or HTTPS. If using SMTP, it is the email address of the MDN's recipient. The address must be accessible externally.

MDN Port

The sixth element determines the TCP/IP port that the AS2 sever uses to receive MDNs. This port must be accessible externally.

Sender (MISC)

This parameter consists of four elements and specifies settings for the sender/creator of the AS2 messages.

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.

**DEFAULT* With the default setting the current value for this parameter will be taken from the i-effect master data (menu item 80).

Originator ID

Enter the originator ID (normally host@domain). This will be transmitted in the headers of AS2 messages.

Originator Email

Enter the sender's email address. This address will be transmitted in the headers of AS2 messages. This is normally the address of the EDI department of a contact person for AS2.

Originator Name

Enter the sender's name here (e.g. company name). This name is transmitted in the headers of AS2 messages.

Delete After Processing

Determine here if the file that was sent via AS2 should be deleted after it was successfully received. "Success" means the MDN returned from the recipient contains no error messages regarding the processing of the message.

**YES* The transmitted file will be deleted.
**NO* The transmitted file will NOT be deleted.

Compression

Specify here, if the AS2 message should be compressed. Compression is compatible with MIME (pkcs7-mime) by using the ZLIB algorithm.

**YES* The message will be compressed.
**NO* The message will not be compressed.

A valid license for the *ZIP module is required for AS2 compression.

i-effect Application Server (EFFSERVER)

It is possible, with i-effect, to remotely call up certain tasks from other IBM System i® in the network. It is also possible to call up this command remotely. The server on which i-effect is installed and licensed must be specified in this case.

This parameter consists of 3 elements

DNS Name or IP

Enter the DNS name or the IP address of the i-effect server.

**LOCALHOST* This default value specifies that the command is called up on the same system where i-effect is installed. It is required that a port be assigned in the next parameter.

TCP/IP Port

Enter the port from which the i-effect command will be called up. This port is dependent on the area for TCP/IP ports specified in the default settings of the *BASE module. (Menu item 80).

The following settings are possible:

| | |
|--------------------------|---------------|
| <i>Command SNDAS2</i> | Base port + 0 |
| <i>Command SNDEMAIL</i> | Base port + 1 |
| <i>Command SNDFAX</i> | Base port + 1 |
| <i>Command SNDSMS</i> | Base port + 1 |
| <i>Command RCVEMAIL</i> | Base port + 1 |
| <i>Command RUNREPORT</i> | Base port + 3 |
| <i>Command SNDBACK</i> | Base port + 4 |
| <i>Command SNDOFTP</i> | Base port + 6 |

Select the base i-effect TCP/IP port area and add a number that corresponds to the desired command.

Type of Call

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

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

Telebox Communication

Note: To use the functions described in the following, licenses for the i-effect modules *BASE and *TELEBOX are required.

Details about the basic configuration of the TELEBOX module can be found in Chapter 11 "Administration in i-effect." The section "Additional Parameters of the *TELEBOX Module" module explains the basic settings of *TELEBOX.

Menu Item 20: Send Data via TELEBOX.400 (SNDTELEBOX)

The SNDTELEBOX command is used to send data via TELEBOX.400. Licenses for the *BASE and *TELEBOX modules are required to use this command.

Recipient Partner ID (PARTNER)

Assign a partner profile from the master data from menu item 50 at this point.

The following values are possible:

| | |
|-----------------|---|
| <i>*NONE</i> | No recipient partner ID will be assigned. |
| <i>*FRMFILE</i> | The partner alias will be taken from the EDIFACT data (recipient in UNB segment). |
| <i>Text</i> | Enter the recipient partner ID. |

The CCSID and CRLF settings for DB2 files and Telebox specific parameters (e.g. transmission confirmation, file type, etc.) will be used for the specified partner (predefined settings in menu item 50) for data transmission with the SNDTELEBOX command.

Note: When sending EDIFACT files, the specifications in menu item 50, option 8 have priority. i.e. the specifications for CCSID, CRLF, and other parameters in menu item 50 option 2, will be overwritten with the specifications in menu item 50, option 8.

Profile No. (PROFILE)

Assign a communications profile from the master data in menu item 52 here.

The following values are possible:

| | |
|--------------|---|
| <i>*NONE</i> | No communications profile will be assigned. |
| <i>Text</i> | Enter a communications profile ID. |

File System Input(FS)

Enter the file system of the input file.

The following options are available:

| | |
|--------------|--|
| <i>*NONE</i> | No file system will be assigned. |
| <i>*IFS</i> | The input file is stored in the IFS (Integrated File System) |
| <i>DB2</i> | The input file is stored in the DB2 file system. |

Input File (FRMFILE)

The input file to be used is entered here.

The following options are available:

| | |
|-----------------|---|
| <i>*ALL</i> | All files in the source directory/library will be sent. |
| <i>Name</i> | Enter the name of the input file. |
| <i>generic*</i> | Use the wild card "*" for generic file selection. |

This parameter consists of 2 elements:**Library**

The library of the source file in the DB2 file system.

Member File

The source member file in the DB2 file system.

Possible Special Value:

| | |
|-------------|---|
| <i>*ALL</i> | All source member files of the DB2 input file will be sent. |
|-------------|---|

Input Path (FRMPATH)

Enter the path of the IFS input file.

Subject

Text entered here will be sent as the message's subject.

Text, Attachment (TA)

Specify how the data is to be sent, either as text (T) or as an attachment (A). Text data is data that only has printable characters and every line is usually ended with a carriage return (CRLF). Code page (CCSID) conversion must often be performed before transmission for this data type.

The attachment (A) data type generally contains all binary data that cannot be translated.

The following specifications are possible:

| | |
|---|---------------------------------------|
| T | Data is transmitted as text. |
| A | Data is transmitted as an attachment. |

Delivery Report Data Unit (DRPDU)

Determine here if delivery confirmation is required.

The following options are available:

| | |
|-------------|---|
| <i>*YES</i> | Delivery confirmation will be sent. |
| <i>*NO</i> | Delivery confirmation will not be sent. |

Receipt Report Data Unit (RRPDU)

Determine if receipt confirmation is required.

The following options are available:

| | |
|-------------|---|
| <i>*YES</i> | Receipt confirmation will be requested. |
| <i>*NO</i> | Receipt confirmation will not be requested. |

Priority (PRIO)

Determine the priority for transmission.

The following options are available:

| | |
|----------------|---|
| <i>*NORMAL</i> | The data will be sent with normal priority. |
| <i>*URGENT</i> | The data will be sent with high priority. |

X.400 Address (X400)**This parameter consists of 20 elements**

| | |
|-----------|--|
| Element1: | Country (c) Country key. The usual X.400 abbreviation for this field is "C". |
| Element2: | Administr. managm. domain (a) ADMD stands for Administration Management Domain. The usual X.400 abbreviation for this field is "A". |
| Element3: | Private managm. domain (p) PRMD stands for Private Management Domain. The usual X.400 abbreviation for this field is "P". |
| Element4: | Surname (s) Enter the recipient's surname. The usual X.400 abbreviation for this field is "S". |
| Element5: | Given Name (g) Enter the recipient's first name. The usual X.400 abbreviation for this field is "G". |

| | |
|------------|--|
| Element6: | <p>Generation (gn)</p> <p>Enter the abbreviation of the recipient's name suffix. The usual X.400 abbreviation for this field is "GN".</p> |
| Element7: | <p>Initials (i)</p> <p>Enter the partner's initials. The usual X.400 abbreviation for this field is "I".</p> |
| Element8: | <p>Organization (o)</p> <p>Specifications about the organization. The usual X.400 abbreviation for this field is "O".</p> |
| Element9: | <p>Organization Unit 1 (ou1)</p> <p>Organization Unit 1. X.400's normal abbreviation for specifications regarding organization units is "OU".</p> |
| Element10: | <p>Organisation Unit 2 (ou2)</p> <p>Organization Unit 2. X.400's normal abbreviation for specifications regarding organization units is "OU".</p> |
| Element11: | <p>Organisation Unit 3 (ou3)</p> <p>Organization Unit 3. X.400's normal abbreviation for specifications regarding organization units is "OU".</p> |
| Element12: | <p>Organisation Unit 4 (ou4)</p> <p>Organization Unit 4. X.400's normal abbreviation for specifications regarding organization units is "OU".</p> |
| Element13: | <p>DDA Type 1 (dda1)</p> <p>The first of four specifications for DDA (Direct Distribution Attribute). X.400's normal abbreviation for specifications regarding DDA is „DDA“.</p> |
| Element14: | <p>DDA Value 1 (dda1)</p> <p>Value specification for the previous entry. This specification can be seen in conjunction with the entry DDA Type. They are both required and must be specified together.</p> |
| Element15: | <p>DDA Type 2 (dda2)</p> <p>The second of four specifications for DDA (Direct Distribution Attribute). X.400's normal abbreviation for specifications regarding DDA is "DDA".</p> |
| Element16: | <p>DDA Value 2 (dda2)</p> <p>Value specification for the previous entry. This specification can be seen in conjunction with the entry DDA Type. They are both required and must be specified together.</p> |
| Element17: | <p>DDA Type 3 (dda3)</p> <p>The third of four specifications for DDA (Direct Distribution Attribute). X.400's normal abbreviation for specifications regarding DDA is "DDA".</p> |

| | |
|------------|--|
| Element18: | <p>DDA Value 3 (dda3)</p> <p>Value specification for the previous entry. This specification can be seen in conjunction with the entry DDA type. They are both required and must be specified together.</p> |
| Element19: | <p>DDA Type 4 (dda4)</p> <p>The fourth of four specifications for DDA (Direct Distribution Attribute). X.400's normal abbreviation for specifications regarding DDA is "DDA".</p> |
| Element20: | <p>DDA Value 4 (dda4)</p> <p>Value specification for the previous entry. This specification can be seen in conjunction with the entry DDA type. They are both required and must be specified together.</p> |

Delete after Transmission (DELETE)

Determine here if the transmitted source file should be deleted after transmission.

The following options are available:

| | |
|------|--|
| *NO | The source file will not be deleted after transmission |
| *YES | The source file will be deleted after transmission. |

Menu Item 21: Receive TELEBOX Data (RCVTELEBOX)

The command RCVTELEBOX is used to receive and file TELEBOX400 data. Licenses for the i-effect *BASE and *TELEBOX modules are required to use this command.

Profile No. (PROFILE)

Assign a communications profile from the master data under menu item 52.

The following values are possible:

| | |
|--------------|---|
| <i>*NONE</i> | No communications profile will be assigned. |
| <i>Text</i> | Enter a communications profile ID. |

Note: When receiving data using the RCVTELEBOX command, the partner will be read from the headers (by name) of the telebox message and assigned to a corresponding entry in the i-effect partner master data (menu item 50). The specifications in the master data for CCSID, reception path, record length for DB2 etc. will be used to save the data.

If no partner was found, the data will be saved in the default *TELEBOX directory with the CCSID 850 (see menu item 80 with option 8 for telebox).

Selection of Telebox/EMS Reception (TBXSELECT)

The range of data that is received is determined here.

| | |
|--------------|--|
| <i>*OLD</i> | All data in the mailbox with the status OLD will be received again. |
| <i>*NEW</i> | All data in the mailbox that is available and marked NEW will be received. This is new data that has not yet been opened. |
| <i>*ALL</i> | The entire contents of the mailbox will be downloaded. This selection reads new, old, and sent data from the mailbox again. |
| <i>*SENT</i> | All data that was sent will be downloaded. This selection reads all data that has already been sent. |
| <i>*ID</i> | By specifying an identification in the field TBXID, the IPMsgid (Interpersonal Message ID), a single message can be downloaded based on this message identification. |

| | |
|-----------------|---|
| <i>*SUBJECT</i> | By entering a subject text in the field TBXSUBJECT, all messages with the same subject will be downloaded in the same transmission. |
| <i>*NAME</i> | By entering a sender name in the field TBXNAME, all data from a specific sender will be downloaded in the same transmission. |
| <i>*SCAN</i> | By entering a message number in the field TBXSCAN, a single message will be read in the report based on its numbering. |

Message Identification (TBXID)

If *ID is selected in TBXSELECT, the message ID can be indicated here in order to retrieve the corresponding data.

Subject (TBXSUBJECT)

If *SUBJECT is selected in TBXSELECT, the message's subject can be indicated here in order to retrieve the corresponding data.

Sender's Name (TBXNAME)

If *NAME is selected in TBXSELECT, the name of the sender can be indicated here in order to retrieve the corresponding data.

Message Scan-Number (TBXSCAN)

If *SCAN is selected in TBXSELECT, the sequential number of a message can be indicated here in order to retrieve the corresponding data.

Email Communication

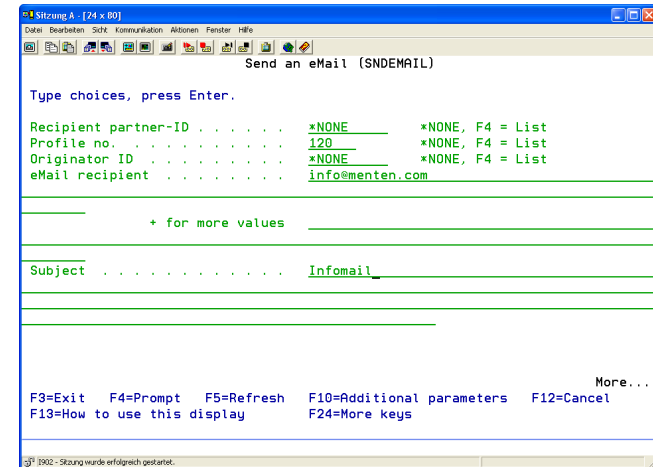
Note: To use the functions described below, a license for the i-effect modules *BASE and *EMAIL are required. If emails shall be signed and encrypted, a license for the *CRYPT module is also required.

The basic configuration of the *EMAIL module can be found in chapter 11 "Administration in i-effect". The section "Additional Parameters of the *EMAIL Module" explains the parameters of the basic settings for *EMAIL.

Menu Item 30: Send Email (SNDEMAIL)

The SNDEMAIL command is used to send a text or any file attachments from the IBM System i with email. Multiple recipients or CC recipients and up to 200 files from the IFS or DB2 files systems can be indicated. SNDMAIL sends these files as a MIME attachment and works with all standard SMTP mail servers.

- 1) Select menu item 30 "Send Email" from the menu "i-effect Communications Tasks," or enter the command SNDEMAIL followed by F4.
- 2) Enter the desired parameters according to the following parameter description.



The send parameters are determined with this dialogue. A partner or a profile can be assigned, from which the parameters will be taken. A sender profile can also be specified which can be selected from a list, that appears when the F4 key is pressed.

The number of parameters that can be selected depends on whether a recipient and/or sender partner and/or communications profile is specified in SNDEMAIL.

Recipient Partner ID (PARTNER)

A partner profile from the master data in menu item 50 can be assigned here.

The following special values are possible:

| | |
|-------|--|
| *NONE | No recipient partner ID will be assigned. The required specifications regarding recipient must be entered in the parameters of this command. |
| Text | Enter a recipient Partner ID. |

Hint: For a variable control of email addresses, recipient, CC and BCC addresses can be stored for every partner. These can be deposited in the partner master data using option 10 in the choice box of the corresponding partner entry (recipient list). More information concerning addresses can be found in Chapter 10 "Master Data in i-effect" in the section "Sender Details for the *EMAIL Module".

Profile No. (PROFILE)

A communications profile from the master data in menu item 52 can be assigned here.

The following special values are possible:

| | |
|--------------|--|
| <i>*NONE</i> | No communications profile will be assigned. The required specifications for the remote system must be entered in the parameters of this command. |
| <i>Text</i> | Enter a communications profile ID. |

Originator Alias (ORIGINATOR)

An originator profile from the master data in menu item 51 can be assigned here.

The following special values are possible:

| | |
|--------------|--|
| <i>*NONE</i> | No originator profile will be assigned. Specifications regarding originator must be entered in the parameters of this command. |
| <i>Text</i> | Enter an originator profile ID. |

Hint: It is not only possible to enter TO, CC, and BCC addresses for reception partners, but also to combine sender partner plus reception partners. The addresses of these combinations will only be used when this partner combination is specified. More information concerning this can be found in the section "Define Sender Specific Email addresses" in Chapter 10 "Master Data in i-effect."

Email Recipient (RECIPIENT)

Enter the email addresses to which the attached files and/or text are sent. The email address must be entered thus: „name@domain.xy“. Up to 100 recipients can be entered.

The following variables are also possible:

| | |
|------------------|--|
| <i>%USER%</i> | The email address of the current user from the system's SMTP mailing list will be used during processing. The SMTP mailing list is maintained with WRKNAMSMTP TBLTYPE(*SYSTEM) and WRKDIRE (Network user ID). |
| <i>%SPLUSER%</i> | Only in conjunction with the i-effect *SERVER *SPOOL/*MONITOR!: The email address of the user, who created the spooled file, will be taken from the SMTP mailing list during processing and inserted in this variable. The SMTP mailing list is maintained in the system with WRKNAMSMTP TBLTYPE(*SYSTEM) and WRKDIRE (network user ID). |

Subject (SUBJECT)

The text entered here is the subject header of the email

Message Text/File

Along with the attached file, a text can be entered here that will be displayed as the message text (INLINE) by the receiving mail client.

This text can also be taken from a file. Therefore, the complete file name must be entered in this parameter. (e.g. /tmp/document.txt or /QSYS.LIB/MYLIB/TEXT.FILE/TEST.MBR). Displaying data from external files INLINE in the recipient's mail client is only possible if the document type is supported there. This is usually the case with TEXT and HTML files. In all other cases the file will be displayed as an attached file. The following control characters can be used to help in simple formatting of manually entered text:

| | |
|----------|---|
| <i>␣</i> | Linefeed |
| | The text in the email is wrapped at this point. |
| <i>␣</i> | Tab |
| | A standard tab is inserted at this point in the text. |

Format

The parameter specifies the format in which the message text exists and in which format the message text will be transmitted.

The following values can be selected:

| | |
|-----------------|---|
| <i>*DEFAULT</i> | Default Value |
| | The value for this parameter is taken from the master data of the *EMAIL module. (see menu item 80) |
| <i>*PLAIN</i> | Plain Text |
| | The text entered or the text read from an external file is sent as an email with content type "text/plain" |
| <i>*HTML</i> | HTML Text |
| | The text entered or the text read from an external file is sent as an email with content type "text/html". The text is packed into a standard HTML skeleton. It must not already exist as a HTML file. If the file exists in HTML form already, the contents will not be converted, rather the file will be sent as is. It is thus possible to send HTML contents as an email |

***BOTH**

Text and HTML

The text, or the text from an external file will be sent as content type multipart/alternative (“text/plain” and “text/html”). The text will be packed into a standard HTML skeleton. The email client on the recipient’s side will then decide which of the parts will be displayed (favored display settings of the email client program).

Encoding

Enter the desired character set for this text. Data will be converted into the specified code page according to this number.

The following values can be selected:

***DEFAULT**

Default Value

The specifications for this parameter will be taken from the master data of the *EMAIL module. (see menu item 80).

***JOB**

Job Control

The CCSID of the current job will be read and transferred to the corresponding encoding scheme. The encoding scheme is *UNICODE if the CCSID of the job is not found in the following list.

Job CCSID – Encoding Scheme List

| Job's CCSID | Encoding Scheme |
|--|-----------------|
| 37; 273; 277; 278; 280; 284; 297; 500; 871; 65535 | *ISO-8859-1 |
| 870; 1122 | *ISO-8859-2 |
| 1112; 1132 | *ISO-8859-4 |
| 1025 | *ISO-8859-5 |
| 420 | *ISO-8859-6 |
| 875 | *ISO-8859-7 |
| 424 | *ISO-8859-8 |
| 1026 | *ISO-8859-9 |
| Any Other | *UNICODE |

***UNICODE**

Universal Character Set

***ISO-8859-1**

ISO-8859-1 (Latin1) Covers most of the Western European languages such as French (fr), Spanish (es), Catalan (ca), Basque (eu), Portuguese (pt), Italian (it), Albanian (sq), Rhaeto-Romanic (rm), Dutch (nl), German (de), Danish (da), Swedish (sv), Norwegian (no), Finnish (fi), Faroese (fo), Icelandic (is), Irish Gaelic (ga), Scottish Gaelic (gd) and English (en), partially Afrikaans (af) and Swahili (sw) which in turn covers the entire American continents, Australia, parts of Asia and a large portion of Africa.

***ISO-8859-2**

ISO-8859-2 (Latin2) Covers the languages of Central and Eastern Europe: Czech (cs), Hungarian (hu), Polish (pl), Romanian (ro), Croatian (hr), Slovak (sk), Slovenian (sl), Sorbian.

***ISO-8859-3**

ISO-8859-3 (Latin3) is used for Esperanto (eo) and Maltese (mt), and covered Turkish before the release of Latin5 in 1988.

***ISO-8859-4**

ISO-8859-4 (Latin4) contains letters for Estonian (et), the Baltic languages Latvian (lv, Lettish) and Lithuanian (lt), Greenlandic (kl) and Sami languages.

***ISO-8859-5**

Cyrillic letters that cover Bulgarian (bg), Belorussian (be), Macedonian (mk), Russian (ru), Serbian (sr), and before 1990 Ukrainian (uk).

***ISO-8859-6**

The Arabic alphabet. Only the simple alphabet for Arabic (ar) without the four extra Persian (fa) and eight Pakistani (Urdu, ur) letters.

***ISO-8859-7**

The modern (monotonic) Greek (el) Alphabet.

***ISO-8859-8**

Hebrew script used in Hebrew (iw) and Yiddish (ji).

***ISO-8859-9**

ISO-8859-9 (Latin 5) Replaces the rarely used Icelandic special characters from Latin1 with Turkish ones.

***ISO-2022-JP**

Japanese Katakana DBCS character set.

*ISO-2022-KR

Korean DBCS character set.

Attachment (ATTACH)

This parameter can handle the names of up to 200 files that can be attached to emails. Generic names are also allowed!

All PDF files in the directories tmp can be attached to the email by entering /tmp/*.pdf.

If /tmp/*. * is entered, all files from /tmp will be attached to the email

The following variables are possible in conjunction with i-effect *SERVER:

%TMP%

"/TMP" is used as the input path.

%HOME%

This option assigns the home path („/HOME/USERNAME“), of the user who issued the job. If this user does not have a home path, then an error message will appear requesting the creation of a home path for the current user.

%CURDIR%

Current Directory.

%USER%

Name of the current user.

%DATE%

Date DD.MM.YYYY.

%YEAR%

Current Year YYYY.

%YEAR2%

Current Year YY.

%MONTH%

Current Month MM.

%MONTHNAME%

Current Month's Name

%WEEKDAY%

Current weekday, e.g. ‚Friday‘.

%TIME%

Current Time HH:MM:SS.

%TIMESTAMP%

Current Time Stamp, YYYY-MM-DD-HH.MM.SS.MSMSMS

%DEFAULTPATH%

This variable will be filled with the default value from the *SERVER module's default settings.

%SRVDIR%

This variable is filled in with *SERVER's temporary working directory. This unique directory is used by i-effect *SERVER for transfer of files between processing steps.

Use e.g. „/%SRVDIR%/*. *” to send all files in this directory.

/%IFSPATH%/%IFSFILE%

These variables can only be used in the i-effect server jobs *IFS/*MONITOR!

They will be filled with qualified names of all files that match the selection criteria of the server's processing table.

Accessing the DB2 file system is possible too.

/QSYS.LIB/%DB2LIB%.LIB/%DB2FILE%.FILE/%DB2MBR%.MBR%

These variables can only be used by the i-effect server jobs *DB2/*MONITOR!

They will be filled with qualified names of all files that match the selection criteria of the server's processing table.

CC

Email addresses to which a copy of the text and/or attachments is sent should be entered here. The email address must be in the following form: "name@domain.xy" Up to 100 recipients can be entered.

BCC

Email addressee, to which a blind copy of the text and/or attachments is sent should be entered here. Blind, because no recipients appear in To and Cc by those receiving the message as a blind carbon copy. The email address must be in the following form: "name@domain.xy" Up to 100 recipients can be entered.

Hint: For a variable control of email addresses, recipient, CC and BCC addresses can be stored for every partner. These can be deposited in the partner master data using option 10 in the choice box of the corresponding partner entry (recipient list). If a partner in "Recipient Partner ID" is specified in the command SNDEMAIL, an email will be sent to all addresses defined for this partner.

Priority (PRIO)

Sets the priority, with which the email will be marked when it reaches it's recipient.

| | |
|-----------------|--|
| <i>*DEFAULT</i> | Default Setting. The settings for this parameter will be taken from the master data of the *EMAIL module. |
| <i>*NORMAL</i> | Normal Priority. The email will be marked with normal priority. |
| <i>*LOW</i> | Low Priority. The email will be marked with low priority. |
| <i>*HIGH</i> | High Priority. The email will be marked with high priority. |

Receipt Confirmation (MDN)

This parameter specifies if confirmation will be requested for the receipt of the email. If the recipient's system supports this function, an email will be generated automatically to confirm the email's reception.

| | |
|-----------------|--|
| <i>*DEFAULT</i> | Default Setting. The master data of the i-effect *EMAIL module will determine this setting. |
| <i>*YES</i> | Request Confirmation The recipient's system will be asked to confirm the email's reception. |
| <i>*NO</i> | Do not request confirmation NO confirmation will be requested. |

Maximum Mail Size in KB (SIZE)

Certain email systems limit the size of emails that are sent and received, either by the provider or the recipient's system. These requirements can be met here by entering the maximum size of email files. If the maximum size is exceeded, e.g. because of large attachments, the attachments will be sent with several emails

*NOMAX is a possible special value, specifying that there is no maximum size.

Signature Algorithm

This parameter can specify whether the outgoing email will be electronically signed or not. An email that is electronically signed can be checked for its validity and integrity, as well as it's origin by using the public key.

Possible Values are:

| | |
|-----------------|---|
| <i>*DEFAULT</i> | Default Setting. The master data of the i-effect *EMAIL module will be used to determine the signature algorithm (see menu item 80). |
| <i>*NONE</i> | No Signature. The email will NOT be signed. |
| <i>*MD5</i> | MD5 Signature MD5 will be used to generate the signature. MD5 (Message Digest Algorithm 5) is a well know cryptographic hash function that creates a 128 bit hash value. |
| <i>*SHA1</i> | SHA1 Signature SHA-1 will be used to generate the signature. The secure hash algorithm, SHA, is a group of standardized cryptographic hash functions. SHA-1 is a cryptographic hash function, that creates a 160-bit hash value. |

Signature Keystore Alias

This parameter names the entry (alias) of the private key in the keystore that is used for signatures.

Encryption Algorithm

This parameter determines if the email will be electronically encrypted with the certificate of the recipient. An email that is encrypted in this manner can be decrypted with the help of the recipient's private key.

Possible Values are:

| | |
|-------------------|--|
| <i>*DEFAULT</i> | Default Setting The algorithm for encryption will be taken from the master data of the i-effect *EMAIL module. If PARTNER is entered in this parameter the value will be taken from the partner profile (menu item 50). |
| <i>*NONE</i> | No Encryption The email will not be encrypted. |
| <i>*TRIPLEDES</i> | 3DES 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). |

Encryption Keystore Alias

This parameter names the entry (alias) of the public key/certificate in the keystore that will be used for encryption.

SMTP Server

This parameter consists of 6 elements that contain specifications of the mail server.

If *DEFAULT is entered in the parameter "DNS Name or IP", the values for SMTP elements will be taken from the *EMAIL modules master data (menu item 80).

DNS Name or IP

Enter the SMTP mail server's name. It can be an IP address or the DNS name of the mail server.

TCP/IP Port

Enter the port that the mail server uses to receive tasks in the SMTP protocol. The default port is 25.

User Name

Enter the user name to login to the mail server.

Password

Enter the password that corresponds to the user name above.

SSL

Specify here, if an SSL (Secure Socket Layer) will be used to connect to the mail server.

| | |
|-------------|--|
| <i>*YES</i> | Yes SSL will be used. |
| <i>*NO</i> | No, a standard connection will be established. |

Import Certificates

Specify here if certificates should be imported automatically by the mail server. The mail server identifies to the email client with its certificate by sending it to the client when the connection is established. If this certificate does not exist in the keystore, it will automatically be imported.

If *NO is entered, then an error will be reported if the server's certificate is not present in the i-effect keystore when the connection is established.

| | |
|-------------|--|
| <i>*YES</i> | Yes, certificates will be imported. |
| <i>*NO</i> | No, certificates will NOT be imported. |

Sender's Email Address

This is the email address entered into the email as sender.

The following values can be selected:

| | |
|-----------------|---|
| <i>*DEFAULT</i> | The default value takes the value for this parameter from the i-effect master data of the *EMAIL module. |
| <i>%USER%</i> | The email address of the current user will be taken from the SMTP mailing list of the system (WRKNAMSMTP TBLTYPE(*SYSTEM) and will be entered during processing into this variable. |

%SPLUSER% Only in conjunction with the i-effect *SERVER *SPOOL/*MONITOR!: The email address of the user who created the spooled file will be taken from the SMTP mailing list during processing and inserted in this variable. The SMTP mailing list is maintained in the system with WRKNAMSMTP TBLTYPE(*SYSTEM) and WRKDIRE (network user ID).

Reply-to Email Address

This is the email address that the recipient uses for responding to the email

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

**DEFAULT* The default value takes the value for this parameter from the i-effect master data of the *EMAIL module.

%USER% The email address of the current user will be taken from the SMTP mailing list of the system (WRKNAMSMTP TBLTYPE(*SYSTEM) and will be entered during processing into this variable.

%SPLUSER% Only in conjunction with the i-effect *SERVER *SPOOL/*MONITOR!: The email address of the user who created the spooled file will be taken from the SMTP mailing list during processing and inserted in this variable. The SMTP mailing list is maintained in the system with WRKNAMSMTP TBLTYPE(*SYSTEM) and WRKDIRE (network user ID).

Error Email Address

This is the email address that receives transmission error messages.

**SENDER* The error email address is the sender's address.

**DEFAULT* The default value takes the value for this parameter from the i-effect master data of the *EMAIL module.

%USER% The email address of the current user will be taken from the SMTP mailing list of the system (WRKNAMSMTP TBLTYPE(*SYSTEM) and will be entered during processing into this variable.

%SPLUSER% Only in conjunction with the i-effect *SERVER *SPOOL/*MONITOR!: The email address of the user who created the spooled file will be taken from the SMTP mailing list during processing and inserted in this variable. The SMTP mailing list is maintained in the system with WRKNAMSMTP TBLTYPE(*SYSTEM) and WRKDIRE (network user ID).

i-effect Application Server (EFFSERVER)

It is possible, with i-effect, to remotely call up certain tasks from other IBM System i® in the network. It is also possible to call up this command remotely. The sever on which i-effect is installed and licensed must be specified in this case.

This parameter consists of 3 elements.

DNS Name or IP

Enter the DNS name or the IP address of the i-effect server.

**LOCALHOST* This default value specifies that the command is called up on the same system where i-effect is installed. It is required that a port be assigned in the next parameter.

TCP/IP Port

Enter the port from which the i-effect command will be called up. This port is dependent on the area for TCP/IP ports specified in the default settings of the *BASE module. (Menu item 80).

The following settings are possible:

| | |
|--------------------------|---------------|
| <i>Command SNDAS2</i> | Base port + 0 |
| <i>Command SNDEMAIL</i> | Base port + 1 |
| <i>Command SNDFAX</i> | Base port + 1 |
| <i>Command SNDSMS</i> | Base port + 1 |
| <i>Command RCVEMAIL</i> | Base port + 1 |
| <i>Command RUNREPORT</i> | Base port + 3 |
| <i>Command SNDBACK</i> | Base port + 4 |
| <i>Command SNDOFTP</i> | Base port + 6 |

Select the base i-effect TCP/IP port area and add a number that corresponds to the desired command.

Type of Call

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

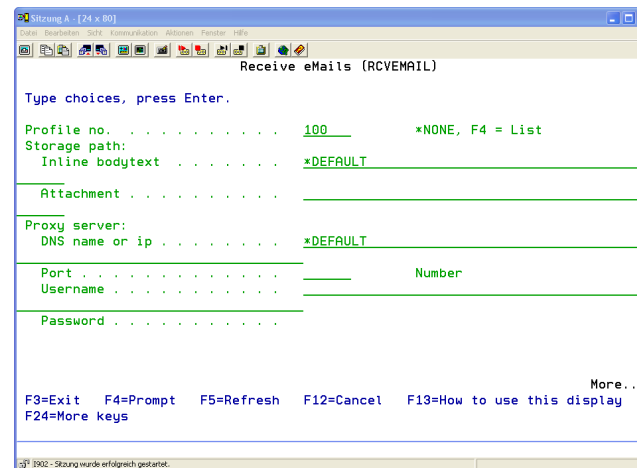
| | |
|---------|---|
| *SYNCH | Synchronous means that the system will wait for an answer from the remote side, with for example SNDEMAIL, all files will be sent, before further actions can be taken. |
| *ASYNCH | The i-Series server is immediately available for further actions, as processing of the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

Menu Item 31: Receive Email (RCVEMAIL)

The RCVEMAIL command is used to receive emails from a POP3 or IMAP compatible mail server. File appendixes or texts from email will automatically be decoded and stored in the appropriate directories.

Information about retrieving and processing partner-controlled emails is found in Chapter 10 "Partner Master Data for the *EMAIL Module"

- 1) Select menu item 31 "Receive Email" from the menu "i-effect Communications Tasks" or enter the command RCVEMAIL followed by F4.
- 2) Enter the desired partner according to the following parameter explanation.



With this dialogue the parameters for reception are determined. A profile can be specified from which the parameters will be taken. This can be selected from a list that appears when F4 is pressed.

The number of parameters that can be selected depends on whether a communications profile has been entered in RCVEMAIL.

Profile No. (PROFILE)

A communications profile that was entered in menu item 52 of the master data can be referred to here.

The following special values are possible:

| | |
|--------------|--|
| <i>*NONE</i> | No communications profile will be assigned. The specifications required by the remote system must be entered manually in the parameters of this command. |
| <i>Text</i> | Enter a communications profile ID. |

Drop Directory

This parameter consists of 2 elements. It determines the directories that are used to receive emails

Inline Bodytext

This directory stores inline texts from incoming emails

The following special value is possible:

| | |
|-----------------|--|
| <i>*DEFAULT</i> | The current values for this parameter will be taken from the master data of the i-effect *EMAIL module (menu item 80) if the default setting is specified. |
|-----------------|--|

Attachments

The decoded email file attachments will be placed in this directory.

The following special value is possible:

| | |
|-----------------|--|
| <i>*DEFAULT</i> | The current values for this parameter will be taken from the master data of the i-effect *EMAIL module (menu item 80) if the default setting is specified. |
|-----------------|--|

POP3/IMAP Server

This parameter consists of 8 elements, that contain specifications for the mail server. The mail server must use the either the POP3 or IMAP protocol.

If *DEFAULT is entered for DNS-Name, the values for all 8 elements will be taken from the master data of the *EMAIL module under menu item 80.

DNS Name

The mail server from which the mails will be received is specified here. Enter either a DNS name or a TCP/IP address in the form: xxx.xxx.xxx.xxx.

All mail servers that use POP3 or IMAP protocols can be used e.g. Lotus Notes or Microsoft Exchange. The mail server must have a corresponding account, that RCVEMAIL can read.

TCP/IP Port

The TCP/IP port number, from which the mail server can be accessed. The default value for an SMTP mail server is 25, for POP3 it is 110 and usually 143 for IMAP.

User Name

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

Password

Enter the password that corresponds to the user name above.

Delete Mail on the Server

Determines if the messages on a POP3 server should be deleted after they have been read.

The following values are possible:

| | |
|-------------|--|
| <i>*YES</i> | Emails will be deleted after they have been successfully processed and can be read when RCVEMAIL is run again. |
| <i>*NO</i> | Emails will be retained on the mail server and can be retrieved again. |

Protocol

The protocol used to receive emails

The following values are possible:

| | |
|--------------|-------------------------------------|
| <i>*POP3</i> | POP3 will be used to receive emails |
| <i>*IMAP</i> | IMAP will be used to receive emails |

SSL

Specify here, if an SSL (Secure Socket Layer) will be used to connect to the mail server.

The following values are possible:

| | |
|------|--|
| *YES | Yes SSL will be used. |
| *NO | No, a standard connection will be established. |

Import Certificates

Specify here if certificates should be imported automatically by the mail server. The mail server identifies to the email client with its certificate by sending it to the client when the connection is established. If this certificate does not exist in the keystore, it will automatically be imported.

If *NO is entered, then an error will be reported if the server's certificate does not exist in the i-effect keystore when the connection is established.

| | |
|------|--|
| *YES | Yes, certificates will be imported. |
| *NO | No, certificates will NOT be imported. |

i-effect Application Server (EFFSERVER)

It is possible with i-effect to remotely call up certain tasks from other IBM-System i® in the network. It is also possible to call up this command remotely. The sever, on which i-effect is installed and licensed must be specified, in this case.

This parameter consists of 3 elements.

DNS Name or IP

Enter the DNS name or the IP address of the i-effect server.

| | |
|------------|---|
| *LOCALHOST | The default value specifies that the command is called up on the same system where i-effect is installed. It is not required that a port be assigned in the next parameter. |
|------------|---|

TCP/IP-Port

Enter the port from which the i-effect command will be called up. This port is dependent on the area for TCP/IP ports specified in the default settings of the *BASE module. (Menu item 80).

The following settings are possible:

| | |
|-------------------|---------------|
| Command SNDAS2 | Base port + 0 |
| Command SNDEMAIL | Base port + 1 |
| Command SNDFAX | Base port + 1 |
| Command SNDSMS | Base port + 1 |
| Command RCVEMAIL | Base port + 1 |
| Command RUNREPORT | Base port + 3 |
| Command SNDBACK | Base port + 4 |
| Command SNDOFTP | Base port + 6 |

Select the base i-effect TCP/IP port area and add a number that corresponds to the desired command.

Type of Call

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

| | |
|---------|---|
| *SYNCH | Synchronous means that the system will wait for an answer from the remote side, with for example RCVEMAIL, all files will be sent, before further actions can be taken. |
| *ASYNCH | The i-Series server is immediately available for further actions, as processing of the remote-controlled call runs in the background. |

Additional Parameters**Partner Allocation**

Activates or deactivates the partner allocation for mail reception. If allocation is deactivated, no partner entry will be sought for the sender's address in an opened email. Allocation of email addresses defined to partners will be non-effective. Only either the parameters entered in the RCVEMAIL command or the module settings of the *EMAIL module will be used. If allocation has been activated, and configured, processing with partner settings will occur.

| | |
|------|----------------------------------|
| *YES | Default. Allocation is activated |
| *NO | Allocation is deactivated. |

eFax Communication

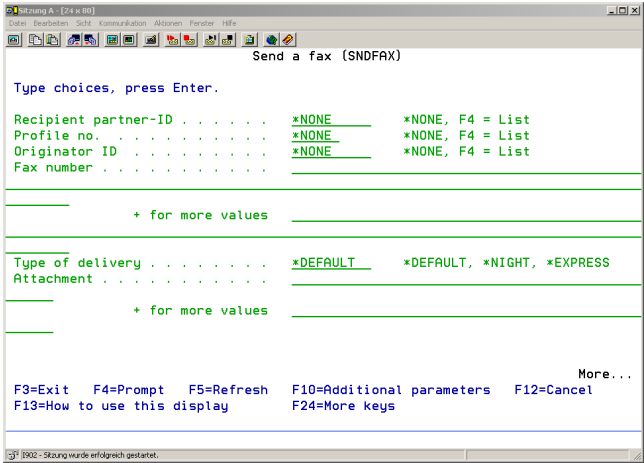
Note: To use the functions described here, licences for the i-effect modules *BASE, *EMAIL, and *FAX are required. An agreement with an internet fax service provider is required too.

The basic configurations of the *FAX modules can be read in Chapter 11 "Administration in i-effect." The section "Additional Parameter of the *FAX Module" explains the basic settings for *FAX.

Menu Item 40: Send eFax (SNDFAX)

The SNDFAX command is used to send spooled files from the IBM System i as a fax. The spooled file is converted to a PDF by the *SPOOL module and sent with the *EMAIL module to an Internet service provider, who sends it as a Telefax to the designated addressee(s).

- 1) Select in menu item 20 "Send eFax" under "i-effect Communications Tasks" or enter the command SNDFAX.
- 2) Fill in the desired parameters according to the following explanations.



This dialog is used to set send parameters. A partner or a profile can be assigned from which the parameter data will be taken. A originator profile can also be assigned. By pressing F4 a list will appear from which a profile can be selected.

The number of parameters that must be filled in depends on whether a recipient and/or an originator partner and/or communications profile is specified with SNDFAX.

Recipient Partner-ID (PARTNER)

A partner profile from the master data in menu item 50 can be referred to here.

The following special values are possible:

| | |
|-------|--|
| *NONE | No recipient partner ID will be assigned. The required specifications regarding recipient must be entered in the parameters of this command. |
| Text | Enter a recipient Partner ID. |

Hint: Any number of Telefax numbers CC, and BCC addresses can be added to a partner in order to variably control the Telefax numbers, CC-, and BCC addresses. These can be deposited in the partner master data with option 10 in the choice box of the corresponding partner entry (recipient list).

Profile No. (PROFILE)

A communications profile that was entered in menu item 52 of the master data can be referred to here.

The following special values are possible:

| | |
|--------------|--|
| <i>*NONE</i> | No communications profile will be assigned. The specifications required by the remote system must be entered manually in the parameters of this command. |
| <i>Text</i> | Enter a communications profile ID. |

Telefax No. (RECIPIENT)

Enter the telefax numbers to which the attached files are sent.

Transmission Mode (MODE)

Specify here if the fax should be sent immediately(express) or should be sent overnight.

The following special values are possible:

| | |
|-----------------|--|
| <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) |

Attachment (ATTACH)

Enter the name(s) of up to 200 files, from the IFS file system. (tmp/rech.pdf). These files will be sent as MIME-attachment with the email and then forwarded as a telefax from an Internet service provider. The attachments must be in PDF (portable document format).

CC

The email with the fax command file will be sent to these email addresses as a copy. This can be used, for example, in case of error, if the command file should be tested by software support. The email address must be in the following form: "name@domain.xy" Up to 50 recipients can be entered.

BCC

Enter the email addresses that should receive the fax command files as a blind carbon copy. Blind because the recipient cannot view the recipients in the "To" and "CC" fields. The email address must be in the following form: "name@domain.xy" Up to 50 recipients can be entered.

Priority

Marks the priority of the outbound email.

| | |
|-----------------|--|
| <i>*DEFAULT</i> | Default Setting The master data of the *EMAIL module sets the value for this parameter. |
| <i>*NORMAL</i> | Normal Priority The email is marked with normal priority. |
| <i>*LOW</i> | Low Priority. The email is marked with low priority. |
| <i>*HIGH</i> | High Priority. The email is marked with high priority. |

Receipt Confirmation

Receipt confirmation does not apply to fax transmission.

Signature

Signature parameters do not apply to fax transmission.

Encryption

Encryption parameters do not apply to fax transmission.

SMTP Server

This parameter consists of 6 elements that contain specifications of the mail server. If *DEFAULT is entered in the parameter "DNS Name or IP", the values for SMTP elements will be taken from the *EMAIL modules master data (menu item 80).

DNS Name or IP

Enter the SMTP mail server's name. It can be an IP address or the DNS name of the mail server.

TCP/IP Port

Enter the port that the mail server uses to receive tasks in the SMTP protocol. The default port is 25.

User Name

Enter the user name to login to the mail server.

Password

Enter the password that corresponds to the user name above.

SSL

Specify here, if an SSL (Secure Socket Layer) will be used to connect to the mail server.

- *YES Yes SSL will be used.
- *NO No, a standard connection will be established.

Import Certificates

Specify here if certificates should be imported automatically by the mail server. The mail server identifies to the email client with its certificate by sending it to the client when the connection is established. If this certificate does not exist in the keystore, it will automatically be imported.

If *NO is entered, then an error will be reported if the server's certificate is not present in the i-effect keystore when the connection is established.

- *YES Yes, certificates will be imported.
- *NO No, certificates will NOT be imported.

Sender's Email Address

This is the email address entered into the email as sender.

The following values can be selected:

- *DEFAULT The default value takes the value for this parameter from the i-effect master data of the *EMAIL module.

Reply-to Email Address

This is the email address that the recipient uses for responding to the email.

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

- *DEFAULT The default value takes the value for this parameter from the i-effect master data of the *EMAIL module.

Error Email Address

This is the email address that receives transmission error messages.

- *SENDER The error email address is the sender's address.
- *DEFAULT The default value takes the value for this parameter from the i-effect master data of the *EMAIL module.

i-effect Application Server (EFFSERVER)

It is possible, with i-effect, to remotely call up certain tasks from other IBM System i® in the network. It is also possible to call up this command remotely. The sever on which i-effect is installed and licensed must be specified in this case.

This parameter consists of 3 elements.

DNS Name or IP

Enter the DNS name or the IP address of the i-effect-Servers.

- *LOCALHOST The default value specifies that the command is called up on the same system where i-effect is installed. It is not required that a port be assigned in the next parameter.

TCP/IP-Port

Enter the port from which the i-effect command will be called up. This port is dependent on the area for TCP/IP ports specified in the default settings of the *BASE module. (Menu item 80).

The following settings are possible:

- Command SNDAS2 Base port + 0
- Command SNDEMAIL Base port + 1
- Command SNDFAX Base port + 1
- Command SNDSMS Base port + 1
- Command RCVEMAIL Base port + 1
- Command RUNREPORT Base port + 3

Command *SNDBACK* Base port + 4

Command *SNDOFTP* Base port + 6

Select the base i-effect TCP/IP port area and add a number that corresponds to the desired command.

Type of Call

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

**SYNCH* Synchronous means that the system will wait for an answer from the remote side, with for example SND-FAX, all files will be sent, before further actions can be taken.

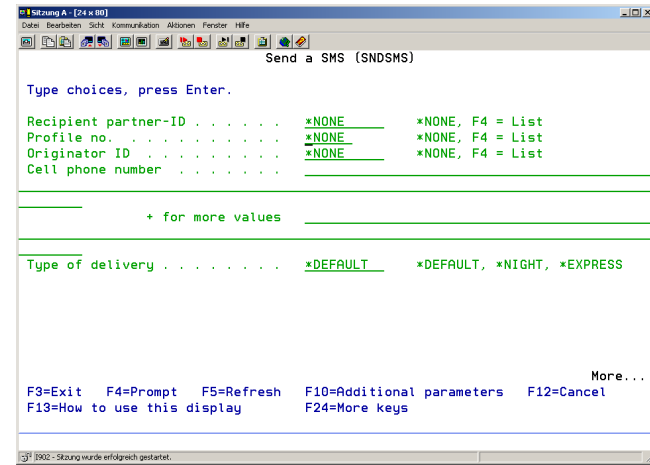
**ASYNCH* The i-Series server is immediately available for further actions, as processing of the remote-controlled call runs in the background.

Menu Item 34: Send SMS (SNDSMS)

The SNDSMS command is used to send text as an SMS. The text is sent by the *EMAIL module to an Internet service provider, who in turn sends it as an SMS.

Note: Because SMS and FAX transmission is handled by the same service provider, licenses for i-effect *BASE, *FAX, and the *EMAIL modules are required to use these functions.

- 1) Select menu item 41(Send SMS) from the menu "i-effect Communication Tasks" or enter the command SNDSMS.
- 2) Enter the desired parameters according to the following descriptions.



Recipient Partner ID (PARTNER)

A partner profile entered in the master data under menu item 50 can be referred to here.

The following special values are possible:

- *NONE* No recipient partner ID will be assigned. The required specifications for the recipient must be entered manually in the parameters of this command.
- Text* Enter a partner ID.

Hint: Any number of SMS numbers, CC, and BCC addresses can be added to a partner in order to variably control the SMS numbers, CC-, and BCC addresses. These can be deposited in the partner master data using option 10 in the choice box of the corresponding partner entry (recipient list).

Profile No. (PROFILE)

A communications profile that was entered in menu item 52 of the master data can be referred here.

The following special values are possible:

- *NONE* No communications profile will be assigned. The specifications required by the remote system must be entered manually in the parameters of this command.
- Text* Enter a communications profile ID.

Originator Alias (ORIGINATOR)

An originator profile from the master data in menu item 51 can be referred to here.

The following special values are possible:

| | |
|--------------|--|
| <i>*NONE</i> | No originator profile will be assigned. Specifications regarding originator must be entered in the parameters of this command. |
| <i>Text</i> | Enter an originator profile ID. |

Cellular Phone Number

Enter the mobile phone number to which the SMS will be sent. Up to 50 cellular phone numbers can be entered.

Transmission Mode (MODE)

Specify here if the SMS should be sent immediately (express) or should be sent overnight.

The following special values are possible:

| | |
|-----------------|---|
| <i>*DEFAULT</i> | The mode will be taken from the default settings of the fax module in menu item 80. |
| <i>*NIGHT</i> | The SMS will be sent overnight. |
| <i>*EXPRESS</i> | The SMS will be sent immediately. |

Message Text

This is the text of the SMS message that is sent to the recipient. Text from a text file can be used for message text. Therefore, the fully qualified file name of this file must be entered here.

Format

This parameter does not apply to SMS transmission.

Coding

This parameter does not apply to SMS transmission.

Attachment

This parameter does not apply to SMS transmission.

CC

The email with the SMS command file will be sent to these email addresses as a copy. This can be used, for example, in case of error, if the command file should be tested by software support. The email address must be in the following form: "name@domain.xy" Up to 50 recipients can be entered.

BCC

Enter the email addresses that should receive the SMS command files as a blind carbon copy. Blind because the recipient cannot view the recipients in the "to" and "CC" fields. The email address must be in the following form: "name@domain.xy" Up to 50 recipients can be entered.

Priority

This parameter does not apply to SMS transmission.

Reception Confirmation

This parameter does not apply to SMS transmission.

Signature

Signature parameters do not apply to SMS transmission.

Encryption

Encryption parameters do not apply to SMS transmission.

SMTP Server

This parameter consists of 6 elements that contain specifications of the mail server.

If **DEFAULT* is entered in the parameter "DNS Name or IP", the values for SMTP elements will be taken from the **EMAIL* modules master data (menu item 80).

DNS Name or IP

Enter the SMTP mail server's name. It can be an IP address or the DNS name of the mail server.

TCP/IP Port

Enter the port that the mail server uses to receive tasks in the SMTP protocol. The default port is 25.

User Name

Enter the user name to login to the mail server.

Password

Enter the password that corresponds to the user name above.

SSL

Specify here, if an SSL (Secure Socket Layer) will be used to connect to the mail server.

- | | |
|------|--|
| *YES | Yes SSL will be used. |
| *NO | No, a standard connection will be established. |

Import Certificates

Specify here if certificates should be imported automatically by the mail server. The mail server identifies to the email client with its certificate by sending it to the client when the connection is established. If this certificate does not exist in the keystore, it will automatically be imported.

If *NO is entered, then an error will be reported if the server's certificate is not present in the i-effect keystore when the connection is established.

- | | |
|------|--|
| *YES | Yes, certificates will be imported. |
| *NO | No, certificates will NOT be imported. |

Sender's Email Address

This is the email address entered into the email as sender.

The following values can be selected:

- | | |
|----------|--|
| *DEFAULT | The default value takes the value for this parameter from the i-effect master data of the *EMAIL module. |
|----------|--|

Reply-to Email Address

This is the email address that the recipient uses for responding to the email

- | | |
|----------|--|
| *SENDER | The Reply-to email address is the sender's address. |
| *DEFAULT | The default value takes the value for this parameter from the i-effect master data of the *EMAIL module. |

Error Email Address

This is the email address that receives transmission error messages.

- | | |
|----------|--|
| *SENDER | The error email address is the sender's address. |
| *DEFAULT | The default value takes the value for this parameter from the i-effect master data of the *EMAIL module. |

i-effect Application Server (EFFSERVER)

It is possible with i-effect to remotely call up certain tasks from other IBM System i® in the network. It is also possible to call up this command remotely. The sever, on which i-effect is installed and licensed must be specified, in this case.

This parameter consists of 3 elements.

DNS Name or IP

Enter the DNS name or the IP address of the i-effect server.

- | | |
|------------|---|
| *LOCALHOST | The default value specifies that the command is called up on the same system where i-effect is installed. It is not required that a port be assigned in the next parameter. |
|------------|---|

TCP/IP-Port

Enter the port from which the i-effect command will be called. This port is dependent on the area for TCP/IP ports, which are specified in the default settings of the *BASE module. (Menu item 80).

The following settings are possible:

- | | |
|------------------|---------------|
| Command SNDAS2 | Base port + 0 |
| Command SNDEMAIL | Base port + 1 |
| Command SNDFAX | Base port + 1 |

| | |
|-------------------|---------------|
| Command SNDSMS | Base port + 1 |
| Command RCVEMAIL | Base port + 1 |
| Command RUNREPORT | Base port + 3 |
| Command SNDBACK | Base port + 4 |
| Command SNDOFTP | Base port + 6 |

Select the base i-effect TCP/IP port area and add a number that corresponds to the desired command.

Type of Call

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

| | |
|---------|---|
| *SYNCH | Synchronous means that the system will wait for an answer from the remote side, with for example SNDSMS, all files will be sent, before further actions can be taken. |
| *ASYNCH | The i-Series server is immediately available for further actions, as processing of the remote-controlled |

FTP Communication

Note: To use the functions described here licenses for the i-effect *BASE and *FTP modules are required.

Basic functions of the FTP module can be found in Chapter 11 "Administration in i-effect." The sub-point "Additional Parameter of the *FTP Module" explains the parameters for basic settings for FTP.

Menu Item 50: Send Data via FTP (SNDFTP)

The SNDFTP command is used to transmit data from a predefined partner profile via FTP.

Note: When transmitting objects from DB2 (FS(*DB2)) to another IBM System i system (TARGETPATH(*FRMPATH) or TARGETPATH(/qsys.lib/...), i-effect uses the standard commands SAVOBJ and RSTOBJ. The standard parameters for these commands are set in the message file MESSAGE. If special parameters are required for certain environments, the following messages can be adapted:

IEF0066 as a guideline for the RSTOBJ command

IEF0067 as a guideline for the SAVOBJ command

Partner-ID (PARTNER)

Assign a partner profile from the master data in menu item 50 here.

The following special values are possible:

| | |
|-------|---|
| *NONE | No recipient partner ID will be assigned. |
| Text | Enter a partner ID. |

Settings for CCSID and CRLF for DB2 data will be taken from the specified partner (predefined settings in menu item 50) when transmitting data with SNDFTP.

Profile No. (PROFILE)

A communications profile that was entered in menu item 52 of the master data can be referred to here.

The following special values are possible:

| | |
|-------|---|
| *NONE | No communications profile will be assigned. |
| Text | Enter a communications profile ID. |

File System Input (FS)

Enter the file system of the input file.

The following options are available:

| | |
|--------------|--|
| <i>*NONE</i> | No file system will be assigned. |
| <i>*IFS</i> | The input file is stored in the IFS (Integrated File System) |
| <i>DB2</i> | The input file is stored in the DB2 file system. |

Input File (FRMFILE)

The input file that is used is entered here.

The following options are available:

| | |
|-----------------|---|
| <i>*ALL</i> | All files in the source directory/library will be sent. |
| <i>Name</i> | Enter the name of the input file. |
| <i>generic*</i> | Use the wild card "*" for generic file selection. |

This parameter consists of 2 elements:**Library**

The library of the source file in the DB2 file system.

Member File

The source member file in the DB2 file system.

Possible Special Values:

| | |
|--------------|---|
| <i>*ALL</i> | All source member files in the DB2 input file will be transmitted. |
| <i>*NONE</i> | The value *NONE is used to send *FILE objects of the SAVF type (backup file). Backup files are specific System i objects that contain secured objects that can be restored on other System i systems. Unlike physical files and source files, these files do not contain any members. |

Input Path (FRMPATH)

Enter the IFS input file path.

The character "*" can be entered as a wild card.

Target Path (TOPATH)

Enter the path where the file will be stored in the target system.

The following options are available:

| | |
|-----------------|---|
| <i>*FRMPATH</i> | The target path will be taken from the source path. |
| <i>Name</i> | Enter the target path. |

Replace (REPLACE)

Determine here if the transmitted file will replace a file with the same name in the target system.

The following options are available:

| | |
|-------------|--|
| <i>*NO</i> | If the file already exists in the target system, the new file will be given a new name according to the System i specifications of the FTP client. A sequential number will be added to the name for the new file. |
| <i>*YES</i> | Files with the same name in the target directory will be replaced. |

Target System Command (COMMAND)

A command for the target system can be sent via FTP. This command will be carried out remotely.

Time of Command (CMDTIME)

If a command is carried out by the remote system, this parameter defines whether this occurs before or after transmission.

The following options are available:

| | |
|----------------|---|
| <i>*AFTER</i> | The command will be carried out after the FTP transmission. |
| <i>*BEFORE</i> | The command is carried out before FTP transmission. |

New Name if Renamed (RENAME)

Enter the new name or the new naming pattern for files that should be renamed after transmission to the remote system. This can be necessary if the file must be protected from access from other applications before transmission is completed.

The following options are possible:

| | |
|--------------|--|
| <i>*NONE</i> | The source file will not be renamed after successful transmission. |
| <i>Name</i> | A new name or naming pattern can be entered here: |

e.g.

| | |
|-----------------|---|
| <i>*.DONE</i> | Changes "file1.txt" to "file1.DONE" |
| <i>*_DONE.*</i> | Changes "file1.txt" to "file1_DONE.txt" |
| <i>*_1055am</i> | Changes "file1.txt" to "file1.txt_1055am" |

Delete after Transmission (DELETE)

Specify here if the source file should be deleted after transmission.

The following options are available:

| | |
|-------------|--|
| <i>*NO</i> | The source file will not be deleted after successful transmission. |
| <i>*YES</i> | The source file will be deleted after successful transmission. |

Proxy Server (PROXY)

A proxy server (representative computer server or program) is a service program for computer networks, that mediates data communication. Data transfer with a proxy server is more efficient (lower network load through large data volume) and can increase security. If a proxy server is used in the network, the required parameters to access the server can be determined here.

This parameter consists of 4 elements.

If the value **DEFAULT* is entered for this element, the values for all elements will be taken from the master data of the AS2 module under menu item 80.

DNS Name or IP

Enter either the DNS name or IP address of the proxy server.

Port

Specifies the TCP/IP port of the proxy server.

User Name

Enter (if required) the authorized user's ID.

Password

Enter (if required) the authorized user's password.

FTP Server (SERVER)

This parameter consists of 4 elements that contain specifications for the FTP server. If **DEFAULT* is entered in the first element, the values for all elements will be taken from the FTP module's master data (menu item 80).

DNS Name or IP

Enter the FTP server's name. It can be an IP address or the DNS name of the FTP server.

TCP/IP Port

Enter the port from which the FTP sever can be reached. The default port is 21.

User Name/Password

To access the FTP server in the 3rd and 4th elements, enter the user name and password.

Data Type (DATATYPE)

Enter the type of data of the transmitted file contains.

The following options are available:

| | |
|----------------|---|
| <i>*BINARY</i> | The data is stored as binary data. |
| <i>*ASCII</i> | The data transmission is carried out in the ASCII format, and data must be converted. |

Mode (MODE)

Specify the mode of the FTP connection. FTP only has two modes for the establishment of connections.

The following options are available:

| | |
|-----------------|---|
| <i>*PASSIVE</i> | The client establishes a data connection to the sever on the selected port. Typically a port beyond 1023 is selected by both parties. This mode is used if the client cannot be reached by the server. This is often the case if the client is behind a router that masks the client's addresses using NAT, or if the network is protected by a firewall. |
|-----------------|---|

Menu Item 51: Receive FTP Data (RCVFTP)

The command RCVFTP is used to receive data over a predefined partner profile via FTP.

Partner ID (PARTNER)

Assign a partner profile from the master data in menu item 50 here.

The following special values are possible:

| | |
|--------------|---|
| <i>*NONE</i> | No recipient partner ID will be assigned. |
| <i>Text</i> | Enter a partner ID. |

Note: The partner will be read from the FTP message's headers and assigned to an entry (based on the name) in the i-effect partner master data (menu item 50) when data is received using RCVFTP. Specifications in the partner master data such as CC-SID, reception path, record length for DB2 etc. will be used to save the data.

If no partner was found, the data will be saved in *FTP's default directory with a CCSID of 850 (see menu item 80 selection 8 for FTP).

**ACTIVE* When active mode is selected, the server establishes a connection to a port that was selected by the client. This is typically a port that is beyond 1023, but can be another sever that is set to passive mode and waits for a connection (FXP).

Communication with commands is effected on the Control Port only, also referred to as Out of Band control. It remains possible that partners can communicate during data transmission.

Profile No. (PROFILE)

A communications profile that was entered in menu item 52 of the master data can be referred to here.

The following special values are possible:

| | |
|--------------|---|
| <i>*NONE</i> | No communications profile will be assigned. |
| <i>Text</i> | Enter a communications profile ID. |

Input Path (FRMPATH)

Enter the path for the received file.

The character "*" can be entered as a wild card.

Target File System (FS)

Enter the file system into which the file(s) will be saved.

The following options are available:

| | |
|--------------|--|
| <i>*NONE</i> | No file system will be assigned. |
| <i>*IFS</i> | The target file will be stored in the IFS (Integrated File System) |
| <i>DB2</i> | The target file will be stored in the DB2 file system. |

Target File (TOFILE)

Enter the name under which the file will be saved.

This parameter consists of 2 elements:

Library

The library of the target file in the DB2 file system.

Member File

The target member file in the DB2 file system.

Target Path (TOPATH)

Enter the path, where the file will be stored in the target system.

The following options are available:

| | |
|-----------------|---|
| <i>*FRMPATH</i> | The target path will be taken from the source path. |
| <i>Name</i> | Enter the target path. |

Replace (REPLACE)

Determine here if the transmitted file will replace a file with the same name in the target system.

The following options are available:

- *NO* If the file already exists in the target system, the new file will be given a new name according to the System i specifications of the FTP client. A sequential number will be added to the name for the new file.
- *YES* Files with the same name in the target directory will be replaced.

Target System Command (COMMAND)

A command for the target system can be sent via FTP. This command will be carried out remotely.

Time of Command (CMDTIME)

If a command is carried out by the remote system, this parameter defines whether this occurs before or after transmission.

The following options are available:

- *AFTER* The command is carried out after the FTP transmission.
- *BEFORE* The command is carried out before FTP transmission.

New Name if Renamed (RENAME)

Enter the new name or the new naming pattern for files that should be renamed after transmissions to the remote system. This can be necessary, if the file must be protected from access from other applications before transmission is complete.

The following options are possible:

- *NONE* The source file will not be renamed after successful transmission.
- Name* A new name or naming pattern can be entered here:

e.g.

- *.DONE* Changes "file1.txt" to "file1.DONE"
- *_DONE.** Changes "file1.txt" to "file1_DONE.txt"
- *_1055am* Changes "file1.txt" to "file1.txt_1055am"

Delete after Transmission (DELETE)

Specify here if the source file should be deleted after transmission.

The following options are available:

- *NO* The source file will not be deleted after successful transmission.
- *YES* The source file will be deleted after successful transmission.

Proxy Server (PROXY)

A proxy server (representative computer server or program) is a service program for computer networks, that mediates data communication. Data transfer with a proxy server is more efficient (lower network load through large data volume) and can increase security. If a proxy server is used in the network, the required parameters to access the server can be determined here.

This parameter consists of 4 elements.

If the value **DEFAULT* is entered for this element, the values for all elements will be taken from the master data of the AS2 module under menu item 80.

DNS Name or IP

Enter either the DNS name or IP address of the proxy server.

Port

Specifies the TCP/IP port of the proxy server.

User Name

Enter (if required) the authorized user's ID.

Password

Enter (if required) the authorized user's password.

FTP Server (SERVER)

This parameter consists of 4 elements that contain specifications for the FTP server. If **DEFAULT* is entered in the first element, the values for all elements will be taken from the **FTP module's* master data (menu item 80).

DNS Name or IP

Enter the FTP server's name. It can be an IP address or DNS name of the FTP server.

TCP/IP Port

Enter the port from which the FTP sever can be reached. The default port is 21.

User Name/Password

In the 3rd and 4th element, enter the user name and password to access the FTP server.

Data Type (DATATYPE)

Enter the type of data of the transmitted file.

The following options are available:

- **BINARY* The data is stored as binary data.
- **ASCII* The data transmission is carried out in the ASCII format, and data must be converted.

Mode (MODE)

Specify the mode of the FTP connection. FTP only has two modes for the establishment of connections.

The following options are available:

- **PASSIVE* The client establishes a data connection to the sever on the selected port. Typically a port beyond 1023 is selected by both parties.

This mode is used if the client cannot be reached by the server. This is often the case, if the client is behind a router that masks the client's addresses using NAT, or if the network is protected by a firewall.
- **ACTIVE* When active mode is selected, the server establishes a connection to a port that was selected by the client. This is typically a port that is beyond 1023, but can be another sever that is set to passive mode and waits for a connection (FXP).

Communication with commands is effected on the Control Port only, also referred to as Out of Band control. It remains possible that partners can communicate during data transmission.

OFTP Communication

Introduction to OFTP

The Odette File Transfer Protocol (OFTP) is a protocol for direct or indirect electronic transmission of files between communication partners. It conforms to recommendation 4914/2 of the German Association of the Automotive Industry, or the Odette Organization (Organization for Data Exchange by Tele Transmission in Europe).

OFTP does not function the way FTP does, but functions similarly to email. This is because directory lists are not scanned, but files are sent actively or must be deposited for retrieval. An important feature of OFTP, when compared to FTP (File Transfer Protocol), is that all partners are verified when the connection is established. The server compares the client's login information with those saved on the server and then, if they are authenticated, sends it's login information to the clients, who then verifies the information. Only after successful verification from both sides, data can be exchanged. The client and the server need two pairs of user name and password: user name and password, to login to the other side, and the peer user name and peer password, to verify the partner's information. User names usually are the Odette ID defined by RFC 2204. This is required if OFTP servers must route the communication. If direct communication occurs between 2 partners, any user name can be used.

Data exchange can occur in a session executed by either side. Successful reception is confirmed, depending on the mode of transfer, immediately or later with an „end to end response“ (EERP). The remote side will then acknowledge (RTR) this EERP. Only when the EERP has been received, is the exchange is considered successful.

OFTP transfers occur between clients, the active or initiator of the transfer, and the server, the passive or receiver of the transfer. The initiator can connect for different reasons: to send and receive data, or to only receive data (Files/EERP).

Advantages of OFTP:

- o A continuation is possible after the connection has been aborted so that it is not necessary to transmit the entire file again.
- o The implicit End-To-End-Response guarantees correct transmission and processing of the file by the recipient.
- o Many transportation layers are possible: ISDN (B- and D-Channel), X.25, TCP/IP.

Disadvantages of OFTP:

- o User names and passwords are transmitted in clear text.
- o Files are not encrypted for transfer.

Recommendations:

- o If using OFTP over the Internet, it is recommended that a secure connection be used (VPN).
- o Passwords should be changed at regular intervals.

i-effect *OFTP

i-effect supports all OFTP functions. The OFTP server can receive files from partners and send them to partners as well, as soon as they login to the server (SNDOFTP: Transfer mode *PASSIVE).

It is possible to receive files from an OFTP partner system with the command RCVOFTP.

Files can be sent to an OFTP partner system or to deposited for partner retrieval with the command SNDOFTP (SNDOFTP: Transfer mode *ACTIVE / *PASSIVE)

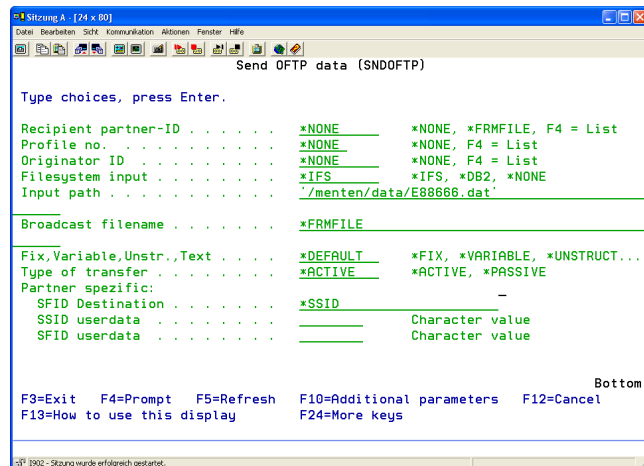
To send, retrieve, receive files, and/or create partner profiles, refer to chapter 10 "Master Data in i-effect". The dialogues in this chapter are shortened by the parameters stored in the partner profiles, when they are used.

OFTP: SNDOFTP Command

This chapter describes, in detail, transmission of System i files with the data exchange protocol OFTP.

Select menu item 13 in the main menu "Conversion Tasks" to open the menu "i-effect Communication Tasks."

Menu Item 60: Send OFTP Data (SNDOFTP)



With this program interface the send parameters are set. A partner or profile can be specified from which the parameters will be taken. A sender profile can also be specified. By pressing the F4 key, a list will appear, from which the profile or partner can be selected.

Recipient Partner ID:

Refer to a partner profile from the master data under menu item 50.

The following special values are available:

| | |
|----------|--|
| *NONE | No recipient partner ID will be assigned. All pertinent information for the recipient must be entered in the parameters of this command. |
| *FRMFILE | The partner-alias of the EDIFACT data (recipient in UNB segment) will be used. |
| Text | Enter a recipient partner ID. |

Profile No:

Refer to a communications profile from the master data under menu item 52.

The following special values are possible:

| | |
|-------|--|
| *NONE | No communications profile will be assigned. All pertinent information for the recipient must be entered in the parameters of this command. |
| Text | Enter a communications profile number. |

Originator ID:

Refer to a sender profile from the master data under menu item 51.

The following special values are possible:

| | |
|-------|---|
| *NONE | No sender will be assigned. All pertinent information for the sender must be entered in the parameters of this command. |
| Text | Enter a communications profile number. |

Input File System:

Enter the file system of the input file here.

The following options are available:

| | |
|--------------|---|
| <i>*NONE</i> | No file system will be assigned. |
| <i>*IFS</i> | The input file is stored in the IFS (Integrated File System). |
| <i>*DB2</i> | The input file is stored in the DB2 file system |

Input Path:

Enter the input file which will be sent here.

The following options are available:

| | |
|-----------------|--|
| <i>*ALL</i> | All files in the from directory/ in the source library will be sent. |
| <i>Name</i> | Enter the name of the input file. (IFS file system) |
| <i>generic*</i> | Use the wild card "*" for generic selection of input files. |

Library:

The library of the source file in the DB2 file system.

Member File:

The source member file in the DB 2 File System.

Possible Special Value:

| | |
|-------------|---|
| <i>*ALL</i> | All source member files of the DB2 input file will be sent. |
|-------------|---|

Name of Transmitted File:

The parameter "Name of Transmitted File" determines under which name the files will be transmitted to the communications partners:

| | |
|-------------------|--|
| <i>*FRMFILE</i> | The original file name will be used. |
| <i>'NAME.DAT'</i> | The file will be sent to partners with the name "NAME.DAT" |

Fix, Variable, Unstr., Text:

Discloses the structure of the transmitted files. This selection influences how line separators are processed how they are used on the opposite side.

The following values are possible:

| | |
|------------------|---|
| <i>*FIX</i> | Records with a fixed length. |
| <i>*VARIABLE</i> | Data records with a variable length. |
| <i>*UNSTRUCT</i> | Unstructured data (binary data). |
| <i>*TEXT</i> | Text data. |
| <i>*DEFAULT</i> | The default settings of the partner master data will be used. |

Transfer Type

There are two types of OFTP data transmission.

Possible Special Values:

| | |
|-----------------|---|
| <i>*ACTIVE</i> | An active connection to the specified partner will be established and the file will be transmitted to the partner directly if this command is carried out. |
| <i>*PASSIVE</i> | The file will be prepared for the partner system. The data will be saved with required information in a temporary directory. As soon as the partner logs on to the OFTP system, the data will be transferred to the partner's system. |

Section "Partner Specific":

If no partner was selected in the parameter PARTNER(), all parameters for communication with this partner must be entered in this parameter group.

This section contains 3 parameters:

- SFID Destination Odette Code
- SSID User Data
- SFID User Data

SFID Odette Code Destination:

This is the destination Odette code that is used for every transmission. The code can differ from the Odette code of the physical partner, if, for example, the recipient is a service provider and the data will be forwarded to another recipient. The special value *SSID can be used to specify that the SFID Odette code is the same as the Odette code in the SSID field which is used during session setup.

SSID User Data:

Depending on arrangement between partners, it may be necessary to enter specific data into the SSID user data field.

SFID User Data:

Depending on arrangement between partners, it may be necessary to enter specific data into the SFID user data field.

Section "OFTP Server":

```

Sitzung A: [24 x 80]
Datei Bearbeiten Sitz Kommunikation Aktionen Fenster Hilfe
Send OFTP data (SNDOFTP)

Type choices, press Enter.

OFTP server:
DNS name or ip . . . . . OFTP.PARTNER1.COM
TCP/IP Port . . . . . 3305      Number
Username . . . . . MENTEN
Password . . . . .

Peer username . . . . . 0012123456PARTNER1PC001
Peer password . . . . .

Connection timeout . . . . . 60      Number
Read timeout . . . . . 60      Number
Max. Retries . . . . . 10      Number
Retry delay . . . . . 300     Number
TCP/IP to X.25 gateway . . . . . *NO     *YES, *NO

More...
F3=Exit  F4=Prompt  F5=Refresh  F10=Additional parameters  F12=Cancel
F13=How to use this display  F24=More keys
  
```

If no communications profile was selected in the PROFILE() parameter, the communications parameters for communication with the remote system must be entered here.

The section consists of 10 parameters: The DNS name and port of the remote system, the user name and passwords, as well as timers.

DNS Name or IP:

TCP/IP address or DNS host name of the remote OFTP server.

TCP/IP Port:

The TCP/IP Port to which the remote OFTP server will answer. The default value is 3305.

User Name and Password:

User name and password that are used for authentication at the remote side.

Peer User Name and Peer Password:

Peer user name and peer password that the remote system uses for authentication on the local system.

The following special value is possible:

*ALL All (even empty) passwords are accepted.

Connection Timeout:

Timeout in seconds for connection setup.

Read-Timeout:

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

Maximum Send Retries:

Maximum number of connection attempts after connection failure or interruption.

Send Retry Pause:

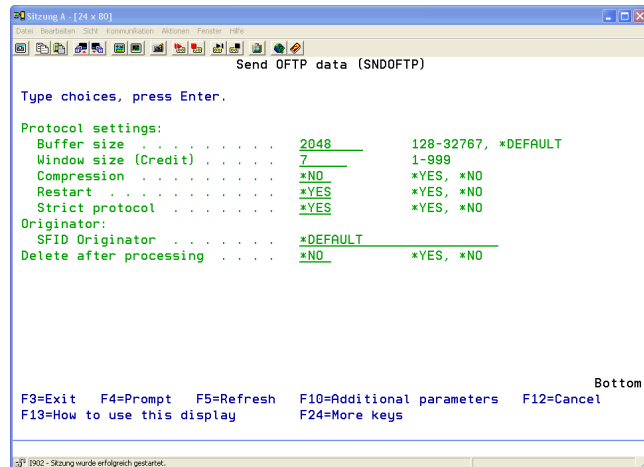
Time in seconds that the sever waits between transmission attempts.

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).

The following options are available:

- *YES A TCP/IP to X.25 Gateway will be used.
- *NO A direct TCP/IP connection will be used.

Section Protocol Settings:

If no communications profile was selected in the PROFILE() parameter, the parameters for communication with remote systems must be entered in this group of parameters.

This section consists of five parameters: The buffer size and window size compression, restart and protocol specifics.

Buffer Size:

The size of the buffer used for sending and receiving in bytes.

Window Size / Credit

This parameter determines the number of buffers that can be transmitted until the partner is requested to refill the credit.

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.

Originator

If no sender was selected in the parameter ORIGINATOR(), this parameter group should be used to determine sender specific settings.

SFID Originator:

The Odette code for the sender used in SFID.

Delete after Processing:

Determine if the source file should be deleted after it has been transmitted.

The following options are available:

- *YES The source file will be deleted after successful transmission.
- *NO The source file will not be deleted after successful transmission.

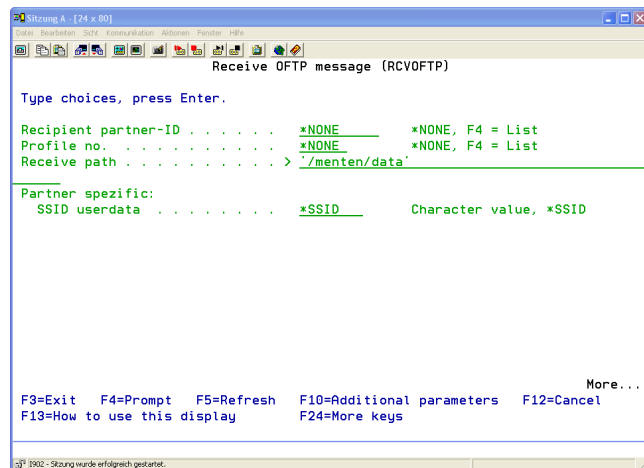
After an OFTP send profile has been created, authentication information can be added to it using menu 52 option 12.

OFTP: RCVOFTP Command

This chapter describes, in detail, reception of System i files using the data exchange protocol OFTP.

Select menu item 13 "i-effect Communications Tasks" from the main menu to open the "Communications Tasks."

Menu Item 61: Receive OFTP Data (RCVOFTP)



Communications parameters are determined with this dialogue. A partner or a profile can be entered, from which the parameter information will be taken. A reception profile can also be specified. The F4 key can be used to display a list of profiles for selection.

Recipient Partner ID:

Refer to a partner profile from the master data under menu item 50.

The following special values are available:

| | |
|-----------------|--|
| <i>*NONE</i> | No recipient partner ID will be assigned. All pertinent information for the recipient must be entered in the parameters of this command. |
| <i>*FRMFILE</i> | The partner-alias of the EDIFACT data (recipient in UNB segment) will be used. |
| <i>Text</i> | Enter a recipient partner ID. |

Profile No:

Refer to a communications profile from the master data under menu item 52.

The following special values are possible:

| | |
|--------------|--|
| <i>*NONE</i> | No communications profile will be assigned. All pertinent information for the recipient must be entered in the parameters of this command. |
| <i>Text</i> | Enter a communications profile number. |

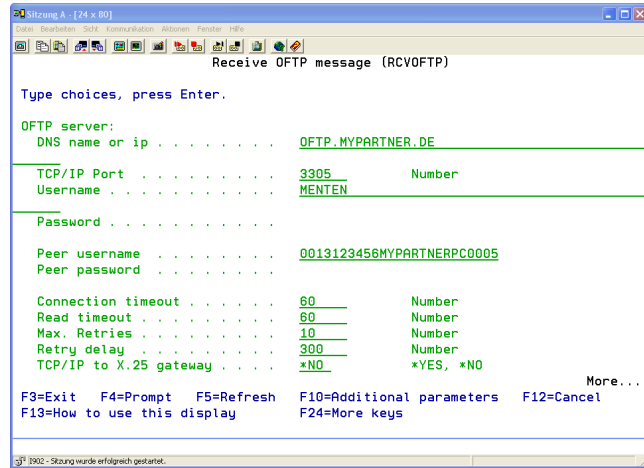
SSID User Data:

Depending on arrangements between partners, it may be necessary to enter specific data into the SSID user data field.

Section "OFTP Server":

If no communications profile was selected in the PROFILE() parameter, the communications parameters for communication with the remote system must be entered here.

The parameter consists of 10 elements: The DNS name and port of the remote system, the user name and passwords, as well as timers.



DNS Name or IP:

TCP/IP address or DNS host name of the remote OFTP server.

TCP/IP Port:

The TCP/IP Port to which the remote OFTP server will answer. The default value is 3305.

User Name and Password:

User name and password that are used for authentication at the remote side.

Peer User Name and Peer Password:

Peer user name and peer password that the remote system uses for authentication on the local system.

The following special value is possible:

*ALL All (even empty) passwords are accepted.

Connection Timeout:

Timeout in seconds for connection setup.

Read-Timeout:

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

Maximum Send Retries:

Maximum numbers of attempts to retransmit after connection failure or interruption.

Send Retry Pause:

Time in seconds that the server waits between transmission attempts.

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).

The following options are available:

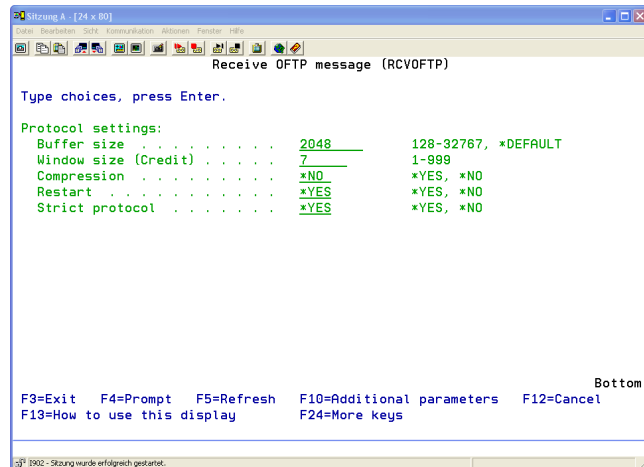
*YES A TCP/IP to X.25 Gateway will be used.

*NO A direct TCP/IP connection will be used.

Section Protocol "Settings":

If no communications profile was selected in the PROFILE() parameter, the parameters for communication with remote systems must be entered in this group of parameters.

The parameters consist of five elements: The buffer size and window size, compression, restart and protocol specifics.



Buffer Size:

The size of the buffer used for sending and receiving in bytes.

Window Size / Credit

This parameter determines the number of buffers that can be transmitted until the partner is requested to refill the credit.

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.

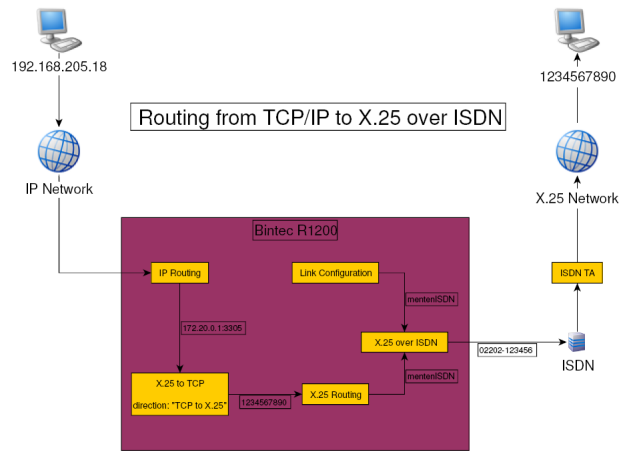
Bintec Router Configuration for OFTP Data Transmission Using the R1200

Introduction

Using the Bintec R1200 as an example, the following explains the necessary steps to set up a OFTP data transmission on a TCP/IP network with an ISDN connection (B-channel) to a host/server on X.25 network.

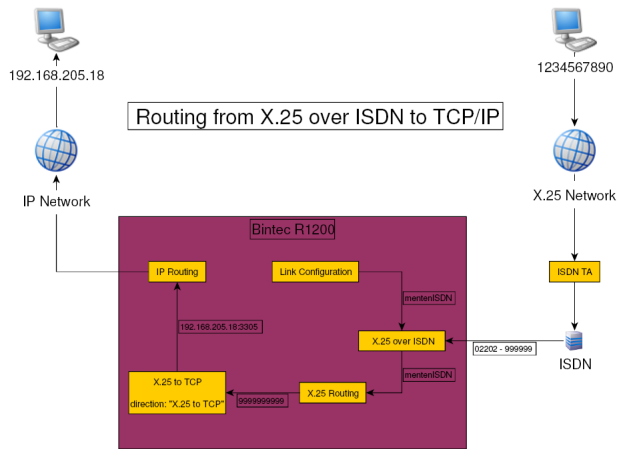
It is helpful to diagram the system setup, to better understand it's configuration. For the system in the TCP/IP network the remote system is accessible from an IP address, which makes both systems in the IP network.

Connection setup from the local system 192.168.205.18 to 172.20.0.1: 3305 (= X.25 address 1234567890):



The X.25 system views the receiving station as accessible with an X.25 address, which makes both systems in the X.25 network.

Connection setup from remote system 1234567890 with ISDN to the address 9999999999 (= local system 192.168.205.18: 3305):



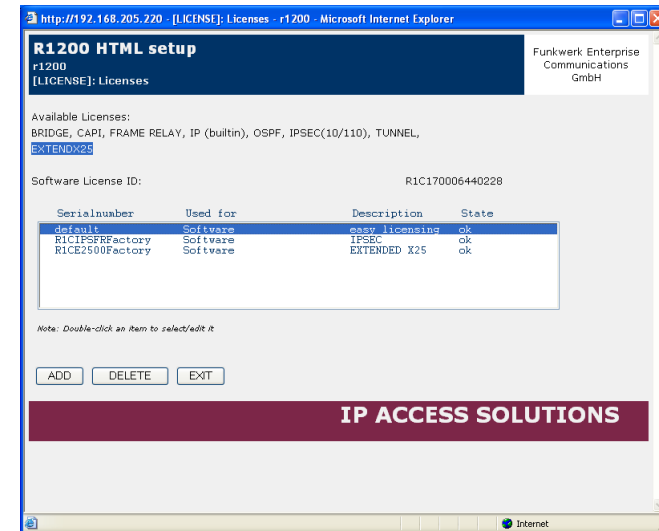
In both cases described above, the Bintec router translates between the IP world and the X.25 world. The following explains the necessary steps for configuration of this process.

The following parameters were take from the diagram above:

| | Local System | Remote System |
|-------------|----------------|---------------|
| TCP/IP | 192.168.205.18 | 172.20.0.1 |
| Subnet mask | 255.255.255.0 | 255.255.0.0 |
| X.25 | 9999999999 | 1234567890 |
| ISDN | 999999 | 02202-123456 |

Checking for the Required X.25 Licenses

Different Bintec products have different scopes of services. It may be necessary to purchase additional licenses (EXTENDX25) from Bintec. The R1200, which is used for this example, already contains the required license. To determine additional licenses if are required, the licenses already present can be viewed in the setup menu under "licenses:". Additional licenses can be added in this menu.



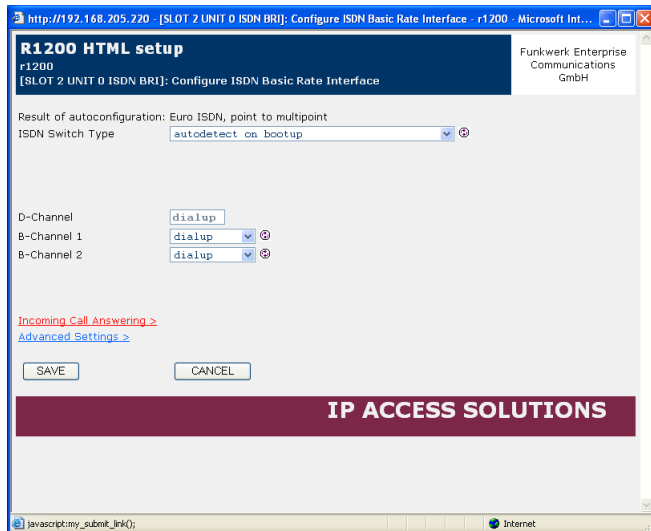
WAN Configuration (ISDN)

Follow the steps described here if incoming ISDN calls should be answered from X.25 remote stations.

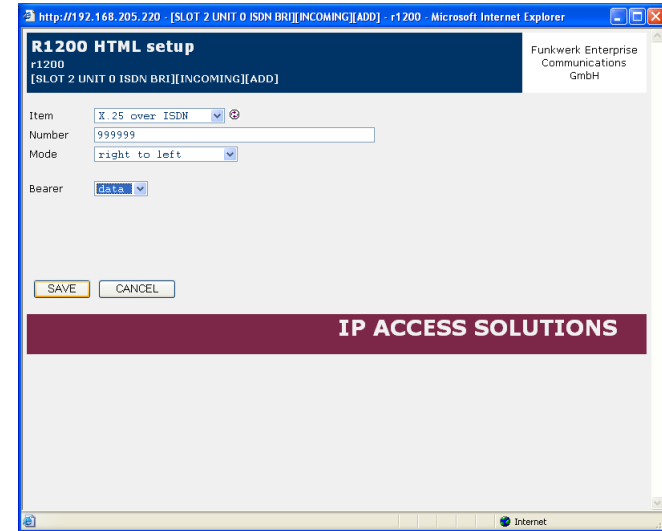
To configure the ISDN interface select "ISDN S0: 0" from the main menu:



Select "Incoming call answering >"



and then enter the following required values:



Click on "SAVE" to save the settings.

The values have the following meaning:

| | |
|---------------|--------------------------------------|
| <i>Item</i> | Protocol Used (here: X.25 over ISDN) |
| <i>Number</i> | MSN of the local ISDN |
| <i>Mode</i> | MSN detection mode |
| <i>Bearer</i> | Supported features (voice/data/both) |

IP Routing Configuration

[IP][ROUTING][ADD]

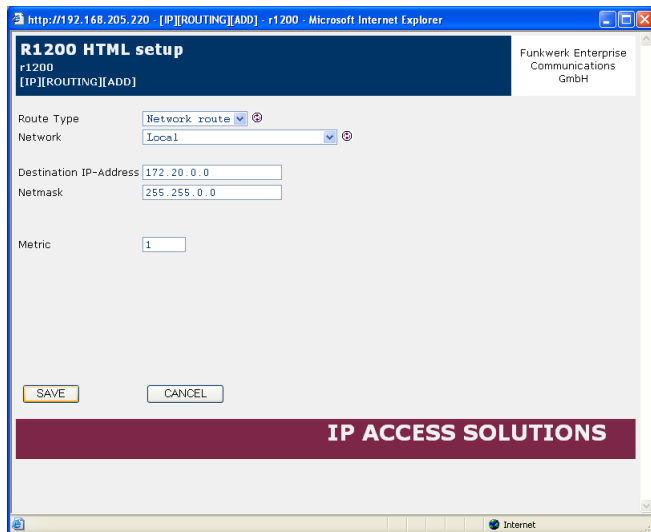
As described earlier, the local system is in the IP subnet 192.168.205.0 with the IP address 192.168.205.18. The remote system (the X.25 System which is virtually connected by ISDN) is in the IP subnet 172.20.0.0 with the IP address 172.20.0.1 (net mask 255.255.0.0)

For the local system, the Bintec router with the address 192.168.205.220 is the gateway to the IP subnet 172.20.0.0 (which represents the virtual X.25 address space: Each IP address in this subnet is assigned to a X.25 address).

IP routing must therefore be configured. This is accomplished by selecting "IP" from the main menu:



Select "Routing" and add a new route with "ADD":



X.25 Configuration

X.25 configuration consists of 4 steps: 1st. "X.25 to TCP conversion;" 2nd. "X.25 over ISDN;" 3rd. "X.25 link configuration;" and 4th. "X.25 Routing;". Configurations are made from the menu "X.25" of the main menu:

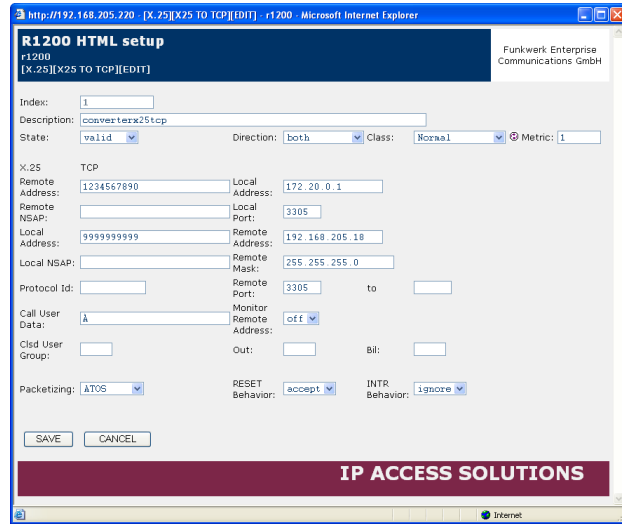


It is important to determine whether to connect with only one partner or with multiple partners. It is recommended that the system be configured for multiple partners.

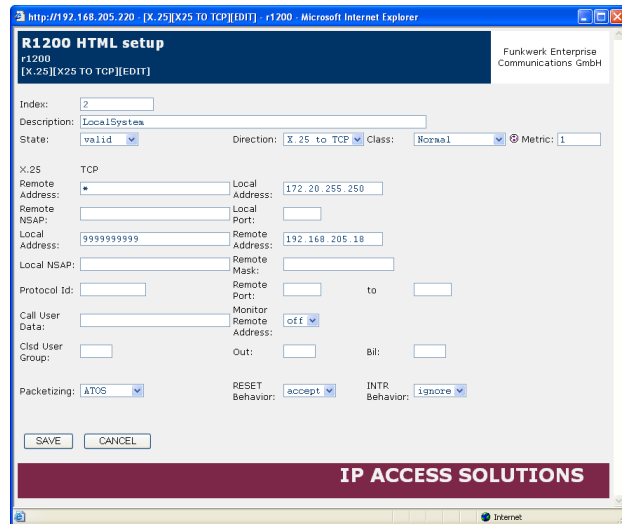
X.25 to TCP Conversion

[X.25][X.25 TO TCP][ADD]

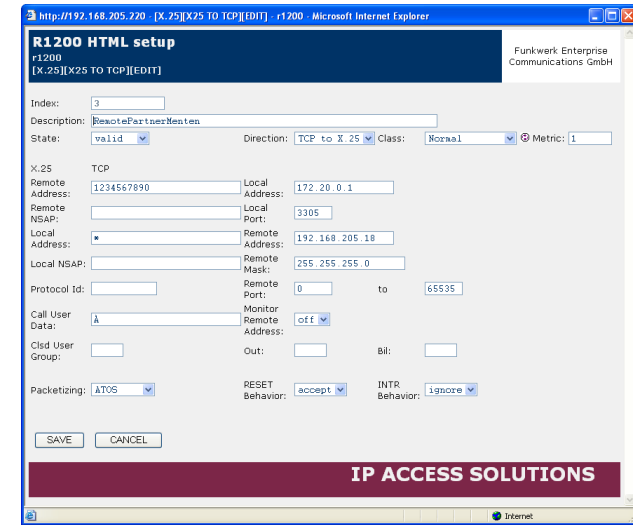
If communication with only one partner is desired select the option “X.25 to TCP conversion” and create a new entry with these values:



For multiple partners enter one entry for the local system and one for each remote system. For example, the local system:



and a remote system::



Explanation of the figures above:

Outgoing ISDN connection:

The IP address 172.20.0.1 at port 3305, which is requested by the local system (IP 192.168.205.18 assigned to the X.25 address 9999999999), is assigned to an ISDN call over the X.25 address. (See “X.25 over ISDN”)

Incoming ISDN call:

The requested X.25 address (9999999999) is assigned to the local system (IP address 192.168.205.18 listening on port 3305).

The values have the following meaning:

X.25:

| | Local System establishes a TCP/IP connection to a remote system (X.25 over ISDN) | Incoming ISDN connection from remote system |
|-----------------------|---|--|
| <i>Remote Address</i> | Unique X.25 partner address. | The unique X.25 address of the remote system can be used, or “*” if there is more than one remote system (partner). (see “Link configuration”) |
| <i>Local Address</i> | The unique X.25 address of the local system can be used, or “*” if there is more than one local system using TCP to X.25. | Unique X.25 address of the local system. |

Call User Data Must be coordinated with the remote party, e.g. 0xc0 (<STRG>+(NumPad)<192>) using IBM System i (depending upon software version)

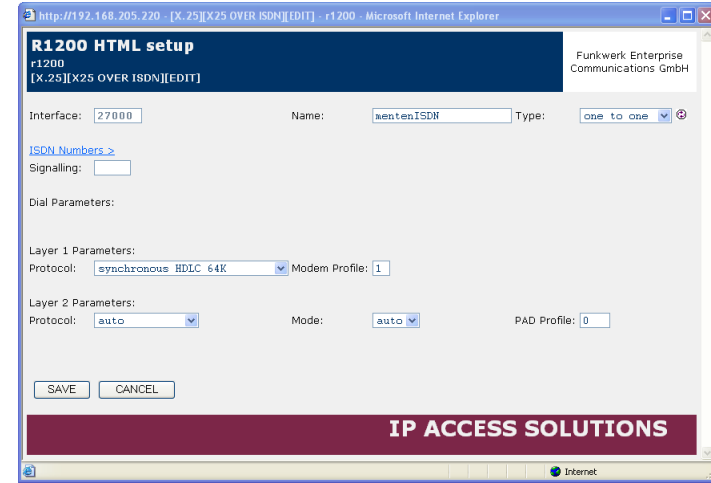
TCP:

| | Local System establishes a TCP/IP connection to a remote system (X.25 over ISDN) | Incoming ISDN connection from remote system |
|-----------------------|--|--|
| <i>Local Address</i> | IP assigned to the partner (Telephone book) | IP address assigned to the calling partner. |
| <i>Local Port</i> | Unique port assigned to IP | Not used |
| <i>Remote Address</i> | IP address of the local system: (0.0.0.0) for all local systems. | Unique IP of the receiving local system. |
| <i>Remote Mask</i> | Must be entered if an IP is entered for "Remote Address" | Not used |
| <i>Remote Port</i> | Valid port range. (0 to 65535) | The first value is the unique port of the called local system. |
| <i>Packetizing</i> | Must be set to "ATOS:" | Must be set to "ATOS:" |

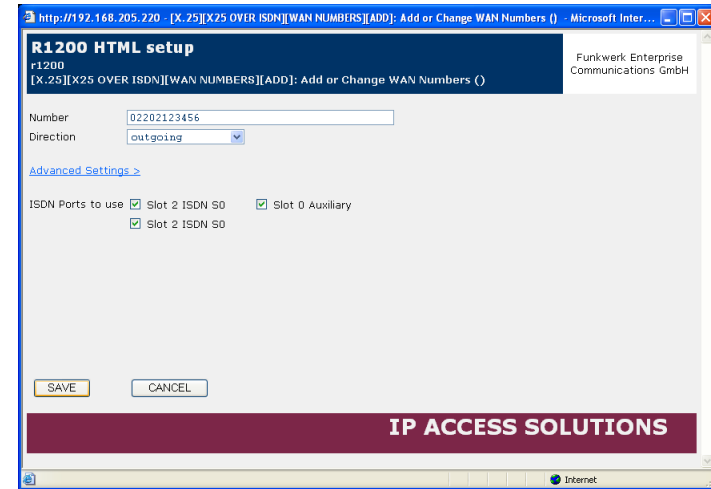
X.25 over ISDN

[X.25][X.25 OVER ISDN][ADD]

In order to dial up a partner with ISDN, partner(s) must be added in "X.25 over ISDN" configuration using "ADD". Each ISDN telephone number is assigned to a partner name (directory entry). First the name of the partner must be entered:



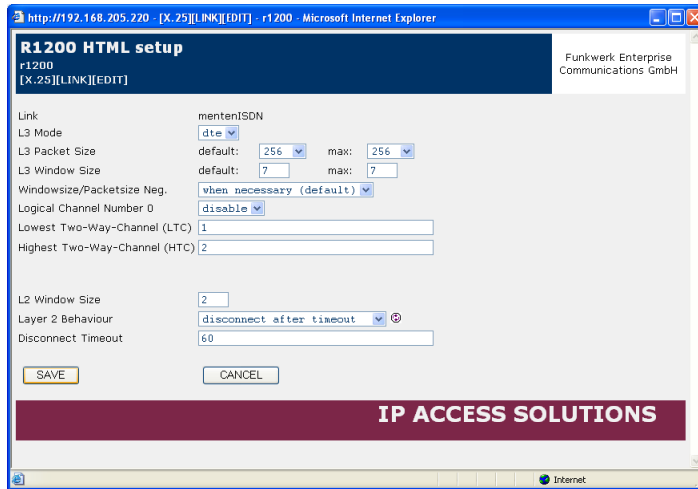
Enter the numbers under "ISDN Numbers"



To allow partners to dial into the system, change "Direction" to "both."

X.25 Link Configuration

For partners configured in "X.25 over ISDN" a link with an X.25 address must be related. This is done from the menu "X.25" option "Link configuration." Here is a sample configuration:



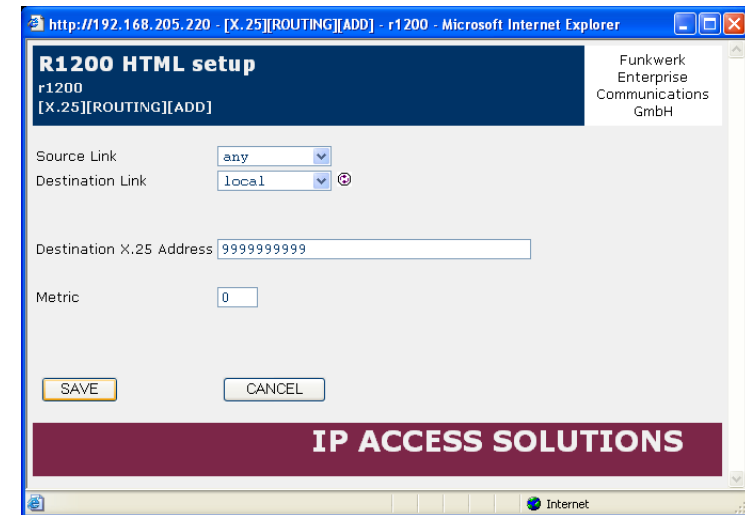
The X.25 address 1234567890 is linked with the telephone number 02202 - 123456 from the directory (see X.25 over ISDN), and the necessary parameters are defined:

| | |
|------------------------------------|--|
| <i>L3 Mode</i> | Determines which system sets the line clocking: |
| dce | The Bintec Router sets the line clocking. |
| dte | Remote system sets the line clocking. |
| <i>L3 Packet Size</i> | Defines standard and maximum packet size. Recommended: "256" |
| <i>L3 Window Size</i> | Defines standard and maximum window size. Recommended: "7" |
| <i>Window size/Packetsize Neg.</i> | Negotiation of packet/window size. Recommendation: "when necessary", negotiations will only be made if the requested values do not match the default values. |
| <i>Logical Channel 0</i> | Not supported by elder X.25 networks/hosts. Recommended: "disable" |
| <i>Lowest Two-Way-Channel</i> | Lowest virtual channel number. For most X.25 links „1“ is recommended. |

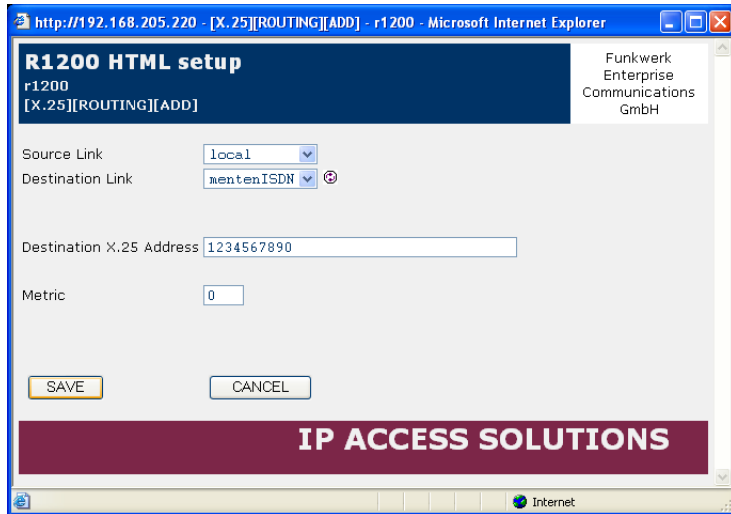
| | |
|--------------------------------|---|
| <i>Highest Two-Way-Channel</i> | Highest virtual circuit number |
| <i>L2 Window Size</i> | Recommended: "2" |
| <i>Layer 2 Behavior</i> | Recommended: "Disconnect after timeout" or "Disconnect when idle" |

X.25 Routing

Finally, routing must be configured. One entry is sufficient for the local system:



For each partner a link with (ISDN) routing must be specified:



Summary

If data is exchanged via X.25 with only one partner, the previously described steps must only be performed once.

When communicating with several partners with this gateway, the local system must be defined first: WAN configuration (ISDN), IP Routing configuration, X.25 to TCP conversion - local system, X.25 Routing - local system, and then the following configurations must be made for each partner: X.25 to TCP conversion - remote system, X.25 over ISDN, X.25 Link Configuration, X.25 Routing - remote system.

HTTP Communication

Note: To use the functions described here, licenses for the i-effect *BASE and *HTTP modules are required. To send and receive data via HTTPS a license for the *CRYPT module is also required.

The basic functions of the HTTP module can be found in Chapter 11 "Administration in i-effect". The section "Additional Parameters of the *HTTP Module" explains the general settings of *HTTP.

The *HTTP module enables the user to send and receive data via HTTP POST. This can be a standard HTTP connection or a secure SSL HTTPS connection.

To receive HTTP data, it is necessary to create an HTTP/S server be created on the system. Details about server configuration can be found in Chapter 10 "Master Data in i-effect" in the section "Create an HTTP Reception Profile".

What is HTTP ?

HTTP (Hypertext Transfer Protocol) is a protocol for data transmission with a network. It is mainly used, to load websites and other data from the World Wide Web (WWW) in web browsers.

HTTP belongs to the application layer of established network models. The application layer is called up by an application program; for HTTP this is usually a web browser. In the ISO/OSI security model it is the application layer of layer 7. TCP/IP, the reference model used on the Internet, sees the application layer in layer 4.

HTTP is basically a stateless protocol. This means that after data is transmitted, the connection between partners need not be maintained. If further data needs to be transmitted, a new connection must be made. Reliable logging of session data can be implemented by cookies, for example, in the application layer.

Due to expansion of request methods, header information, and status codes, HTTP is not restricted to Hypertext, but can also be used to exchange data. HTTP is a reliable transportation protocol for communication. In almost all cases TCP is used.

It was developed in 1989 by Tim Berners-Lee at CERN along with the URL and HTML, which was basically the birth of the World Wide Web (WWW).

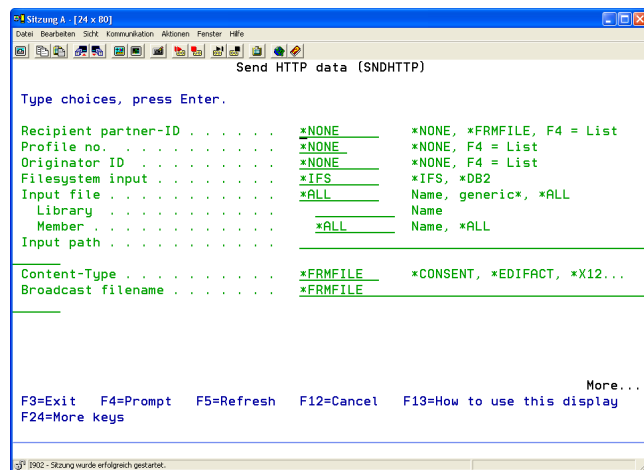
Menu Item 70: Send HTTP Data (SNDHTTP)

The command SNDHTTP is used to send data via HTTP or HTTPS (HyperText Transfer Protocol (Secure)). The HTTP POST method is used to transmit data.

If a user name and password are required to log onto the remote HTTP server, they can be assigned to a sending profile that describes the remote server. Chapter 9 “Master Data in i-effect”, section “User Authentication for HTTP Servers” contains information about storage of user data.

Select menu item 70 “Send HTTP Data” from the menu “i-effect Communications Tasks” or enter the command SNDHTTP followed by F4.

Enter the required parameters according to the following explanations.



The parameters for transmission are determined here. A partner or a profile can be assigned here, from which the parameter data will be taken. A sending profile can also be assigned. A list of profiles will be displayed when the F4 key is pressed.

The number of parameters that must be filled in, depends on whether or not a reception and/or sending profile, or communications profile was assigned for SNDHTTP.

Recipient Partner-ID (PARTNER)

A partner profile entered in the master data under menu item 50 can be referred to here.

The following special values are possible:

| | |
|----------|---|
| *NONE | No recipient partner ID will be assigned. The required specifications for the recipient must be entered manually in the parameters of this command. |
| *FRMFILE | The partner alias will be taken from the EDIFACT file (recipient in the UNB segment). |
| Text | Enter the recipient partner ID. |

Communications Profile No. (PROFILE)

A communications profile from menu item 52 of the master data can be referred to here.

The following special values are possible:

| | |
|-------|--|
| *NONE | No communications profile will be assigned. The specifications required by the remote system must be entered manually in the parameters of this command. |
| Text | Enter a communications profile ID. |

Originator ID (ORIGINATOR)

An originator profile from the master data in menu item 51 can be referred to here.

The following special values are possible:

| | |
|-------|--|
| *NONE | No originator profile will be assigned. Specifications regarding originator must be entered in the parameters of this command. |
| Text | Enter an originator profile ID. |

File System Input (IFS)

Enter the file system of the input file.

The following options are available:

| | |
|-------|--|
| *IFS | The input file is stored in the IFS (Integrated File System) |
| *DB2 | The input file is stored in the DB2 file system. |
| *NONE | No file system will be assigned. |

From File (FRMFILE)

The input file to be transmitted is entered here.

The following options are available:

| | |
|------|---|
| *ALL | All files in the source directory or library will be transmitted. |
|------|---|

Name Enter the name of the input file.
*generic** Use "*" as a wild card for generic input file selection.

The parameter consists of 2 elements:

Library

The library of the source file in the DB2 file system.

Member File

The source member file in the DB-2 file system.

Possible Special Value:

**ALL* All source member files in the DB-2 input file will be transmitted.

Input Path (FRMPATH)

Enter the path to the IFS input file. "*" can be used as a wild card for generic input.

Content Type (CONTENTT)

Determines the content type used for transmission.

**CONSENT* Data is marked as content type "application/EDI-Consent" and transmitted. This marking applies as long as EDIFACT, X.12, or XML data is not being used. This content type is used generally after bilateral agreement.

**EDIFACT* The data is marked as content type "application/EDIFACT" and transmitted. This marks EDIFACT messages, which can be sent to EDIFACT converter systems for automatic processing by the receiving system.

**X12* Data is marked as content type "application/EDI-X12" and transmitted. This marks ANSI X.12 messages, which can be sent to ANSI X.12 converter systems for automatic processing by the receiving system.

**XML* Data is marked as content type "application/XML" and transmitted. This marks data in the XML format.

**BINARY* Data is marked as content type "application/BINARY" and transmitted. This marks data in the binary format.

**FRMFILE* Data is marked with the content type specified by the file extension of the data that will be transmitted. A file with the extension ".txt" contains the content type "application/rtf". A file with the extension ".pdf" has the content type "application/pdf", and a file with the extension ".gif" has the content type "image/gif".

**DEFAULT* The defaults will be taken from the partner master data.

Virtual File Name (BROADCAST)

The virtual name of the transmitted file. This name will be sent to the recipient instead of the physical name, unless *FRMFILE is selected here.

Possible Special Value:

**FRMFILE* The virtual file name will be taken from the physical name of the transmitted file.

Proxy Settings (PROXY)

If a proxy is used for Internet access, the parameters for proxy access can be specified here.

This parameter consists of 4 elements:

The DNS name and the proxy port as well as user name and password (if required).

DNS Name or IP

Enter either the TCP/IP or DNS name of the proxy server.

TCP/IP Port:

Enter the TCP/IP port to which the proxy server will answer.

User Name/Password

Enter the user name and password for authentication on the proxy server.

HTTP Server (SERVER)

If no communications profile was specified in the parameter PROFILE (), the parameters for communication with the remote server must be entered in this parameter group.

This parameter consists of 10 elements:

The DNS name and port of the remote system, user name, password, SSL, certificate, keystore, as well as the timers to be used.

DNS Name or IP:

TCP/IP address or the DNS host name of the remote HTTP server.

TCP/IP Port:

TCP/IP port that the remote HTTP server answers. The default is 80.

User Name/Password:

User name and password (if required) for authentication on the sever.

SSL

The parameter determines the protocol. HTTP communication can either be SSL/HTTPS (Secure Socket Layer) or normal HTTP.

- *YES Yes, HTTPS will be used.
- *NO No, HTTPS will be used.

Import Certificates?

Specify here if certificates of the HTTP server should be automatically imported. The HTTP sever identifies to a client with a certificate by sending it to the client when the connection is established. If this certificate is not in the i-effect keystore, it will automatically be imported.

If *NO is selected, an error will occur if the server's certificate is not present in the i-effect keystore.

- *YES Server certificates will automatically be imported into the keystore.
- *NO Server certificates will not be imported into the keystore.

Connection Certificate

If the remote station asks for SSL client authentication, this parameter determines the alias of the key pair in the keystore that is used for authentication on the remote station. With the public key (certificate) of the key pair authentication is effected on the server as soon as an SSL connection is established. The certificate must exist in the keystore of the remote station's server before a connection establishment.

Connection Timeout

Timeout in seconds for establishing a connection.

Read Timeout

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

Maximum Send Retries

Number of retries for the transmission of a file. If a connection could not be established, or if the connection is aborted, the system will try to reach the system until the maximum number of tries has been reached.

Send Retry Pause

Pause in seconds between reties.

Sender (MISC)

The sender in the HTTP header.

This parameter consists of one element:**Originator Email:**

This email address will be entered in the header of an HTTP request as the sender's email address.

Delete after Transmission (DELETE)

Determine here if the transmitted file should be deleted after it is transmitted.

The following options are available:

- *NO The source file will not be deleted after transmission
- *YES The source file will be deleted after transmission.

i-effect Server (EFFSERVER)

It is possible, with i-effect, to remotely call up certain tasks from other IBM System i® in the network. It is also possible to call up this command remotely. The sever on which i-effect is installed and licensed must be specified in this case.

This parameter consists of 3 elements.

DNS Name or IP

Enter the DNS name or the IP address of the i-effect-Servers.

**LOCALHOST* This standard value specifies that the command is called up on the same system where i-effect is installed. It is required that a port be assigned in the next parameter.

TCP/IP-Port Enter the port from which the i-effect command will be called. This port is dependent on the area for TCP/IP ports, which are specified in the default settings of the *BASE module. (Menu item 80).

The following settings are possible:

- Command SNDAS2* Base port + 0
- Command SNDEMAIL* Base port + 1
- Command SNDFAX* Base port + 1
- Command SNDSMS* Base port + 1
- Command RCVEMAIL* Base port + 1
- Command RUNREPORT* Base port + 3
- Command SNDBACK* Base port + 4
- Command SNDHTTP* Base port + 6

Select the base i-effect TCP/IP port area and add a number that corresponds to the desired command.

Type of Call

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

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

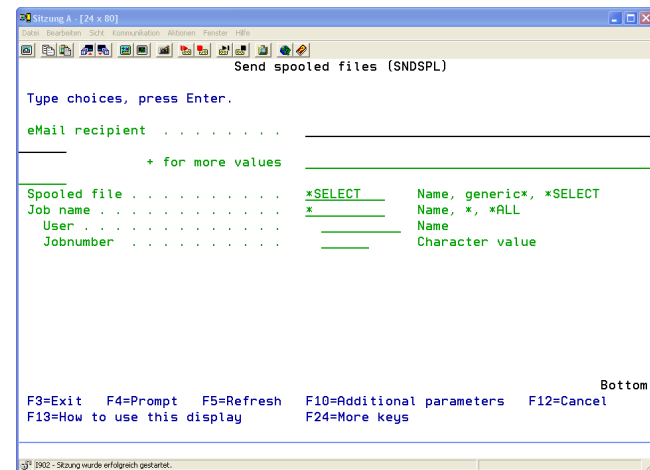
Old Commands

SNDSPL (Send Spooled Files)

The command SNDSPL is used to convert spooled files from the IBM System i format into other formats and send them as email. By entering selection criteria, the entries can be selected and then converted into another format. Parameters such as email address, attachments, and name of the attachments can be entered after this.

Enter SNDSPL in the i-effect menu and press F4.

The following display will appear:



Email Recipient (RECIPIENT)

Enter here the email addresses to which the attached files and/or text are sent. The email address must be entered thus: „name@domain.xy“. Up to 200 recipients can be entered.

The following variables are also possible:

- %USER%** The email address of the current user from the system's SMTP mailing list will be used during processing. The SMTP mailing list is maintained with WRKNAMSMTP TBLTYPE(*SYSTEM) and WRKDIRE (Network user ID).
- %SPLUSER%** The email address of the user who created the spooled file will be taken from the SMTP mailing list during processing and inserted in this variable. The SMTP mailing list is maintained in the system with WRKNAMSMPT TBLTYPE(*SYSTEM) and WRKDIRE (network user ID).

Spooled File

The file name of the spooled file, or one of the following special values.

- *SELECT** The files will be selected in other parameters.
- generic*** With an asterisk (*) part of the file name can be replaced. Enter only the first part of a name with (*) to receive a list of all files that begin with this word part. The following formats are possible for generic names:
 - ABC*** All files beginning with the characters ABC will be displayed, e.g. ABC, ABSD or ABCTEST.
 - a*** All files whose names are in quotation marks and begin with a are displayed, e.g. "a", "aB" or "aD".

Job Name

Spooled file selection can be restricted to all jobs, the current job, or a specific job. If a specific job is desired, then the qualified job name must be entered here.

- *** Only spooled files of the current job will be considered.
- *ALL** All spooled files on the system will be considered.

User

Spooled file(s) of the specified user will be sent.

Job Number

Spooled file(s) of the specified job will be sent.

The rest of this command's parameters can be found in Chapter 4 "Conversion"

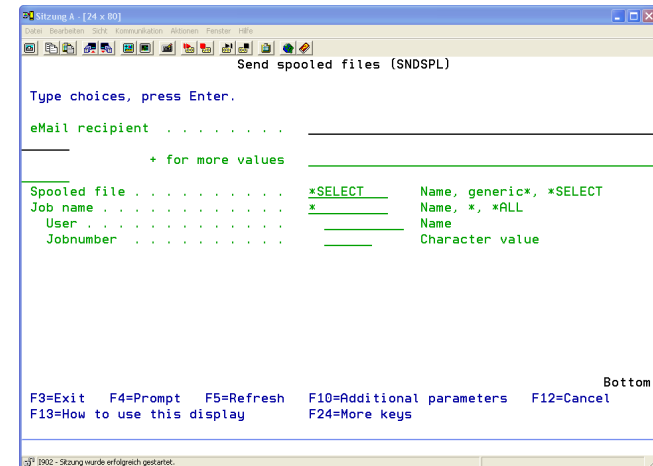
SNDSPLFAX (Send Spooled Files via Fax)

The command SNDSPLFAX converts spooled files from the IBM System i system into PDF and sends them via Telefax. One or more fax recipients can be specified. SNDSPLFAX sends PDF files as a MIME attachment and works with any standard SMTP mail sever.

Licenses for the *BASE, *SPOOL, *EMAIL, and *FAX moduels are required for SNDSPLFAX.

Enter SNDSPLFAX in the main menu and press F4.

The following display will appear:



Email Recipient (RECIPIENT)

Enter here the email addresses to which the attached files and/or text are sent. The email address must be entered thus: „name@domain.xy“. Up to 200 recipients can be entered.

The following variables are also possible:

| | |
|------------------------|--|
| <code>%USER%</code> | The email address of the current user from the system's SMTP mailing list will be used during processing. The SMTP mailing list is maintained with WRKNAMSMTP TBLTYPE(*SYSTEM) and WRKDIRE (Network user ID). |
| <code>%SPLUSER%</code> | The email address of the user who created the spooled file will be taken from the SMTP mailing list during processing and inserted in this variable. The SMTP mailing list is maintained in the system with WRKNAMSMTP TBLTYPE(*SYSTEM) and WRKDIRE (network user ID). |

Spoiled File

The file name of the spooled file, or one of the following special values.

| | |
|-----------------------|--|
| <code>*SELECT</code> | The files will be selected in other paramters. |
| <code>generic*</code> | With an asterisk (*) part of the file name can be replaced. Enter only the first part of a name with (*) to receive a list of all files, that begin with this word part. The following formats are possible for generic names: |
| <code>ABC*</code> | All files beginning with the characters ABC will be displayed, e.g. ABC, ABSD or ABCTEST. |
| <code>a*</code> | All files whose names are in quotation marks and begin with a are displayed, e.g. "a", "aB" or "aD". |

Job Name

Spoiled file selection can be restricted to all jobs, the current job, or a specific job. If a specific job is desired, then the qualified job name must be entered here.

| | |
|-------------------|---|
| <code>*</code> | Only spooled files of the current job will be considered. |
| <code>*ALL</code> | All spooled files on the system will be considered. |

User

Spoiled file(s) of the specified user will be sent.

Job Number

Spoiled file(s) of the specified job will be sent.

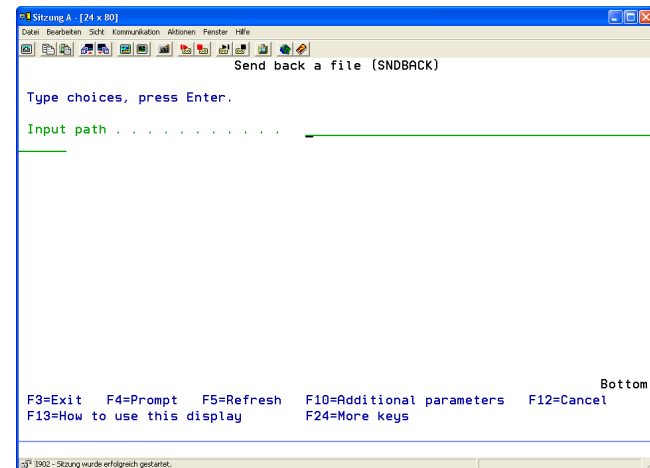
The rest of this command's parameters can be found in Chapter 4 "Conversion"

General Commands

SNDBACK (can only be called up from the command line)

SNDBACK is used to return incoming files. Use this command if several files but not all files were not received correctly. SNDBACK reconstructs the transmission path, and the origin from specifications. Data received with errors can be returned and the sender is then informed of the failed transaction.

Licenses for the *BASE module and the corresponding communications modules are required to use this command.

**Input Path**

Enter the directory here, in which the files that will be returned are stored.

What is SOA / SOAP ?

SOAP („Simple Object Access Protocol“) is a network protocol for data exchange between systems. RPCs (Remote Procedure Calls) can also be called up using this protocol.- Strictly speaking, RPCs are always run, but differ only in whether the files are returned or not.

SOAP uses the XML standard of data representation for data exchange and TCP/IP for transportation.

i-effect's SOAP clients provide essential functions to integrate data into an i-effect workflow .

Starting the SOAP Client (STRSOACTL)

The STRSOACTL command is used to run a SOAP client query at a SOAP web service. The web service is identified by the name of the service and the corresponding command.

In order to start the client, it is required that the IFFECT subsystem was successfully started. If this is not the case, the subsystem will attempt to start automatically, which can increase the time required to start the client.

Parameters must/can be passed on to the client, so that the query can be run.

In the following the “BLZService” SOA client with the command “GetBLZInfo” the parameter “BLZ” (German bank routing number) and the parameter value “10000000” to request information for the German routing number 100 000 00:

