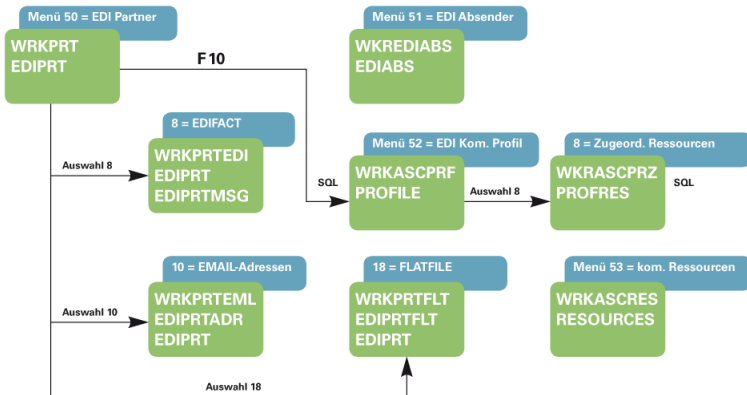


Kapitel 10

Stammdaten in i-effect

i-effect V1R4M0 Partnerstamm



An dieser Stelle können Sie alle für die Funktionalitäten in i-effect relevanten Stammdaten verwalten.

Dieses Kapitel umfasst dabei folgende i-effect Menüpunkte:

- o Menü 50 EDI-Partnerstammdaten (WRKPRT)
- o Menü 51 EDI-Absenderpartnerstamm (WKREDIABS)
- o Menü 52 EDI-Kommunikationsprofile (WRKASCPRF)
- o Menü 53 EDI-Kommunikationsressourcen (WRKASCRES)

Der Abschnitt

- o Benutzerauthentifizierung für Kommunikationsserver

informiert Sie darüber, wie Benutzeraccounts für die Anmeldung an i-effect Servern erstellt werden. Diese Accounts dienen zum einem der Zuordnung des Kommunikationspartners und zum anderen der Sicherheit für den von aussen erreichbaren Kommunikationsserver.

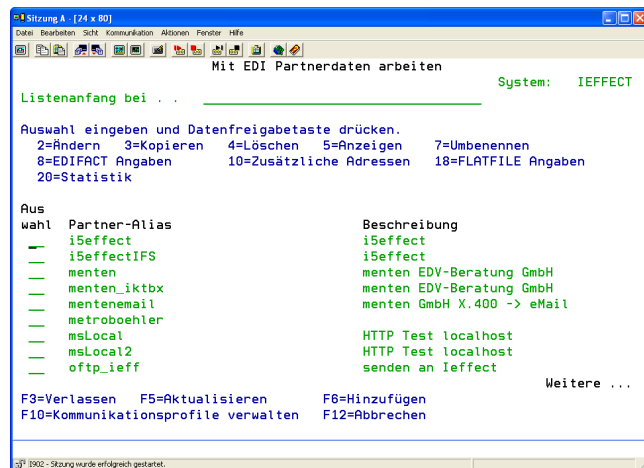
Stammdaten für die Kommunikation

Die Kommunikations-Stammdaten sind die zentrale Stelle in i-effect um Daten zu hinterlegen, die für wiederkehrende Aufgaben im Bereich der Kommunikation benötigt werden.

Menüpunkt 50: Mit EDI-Partnerstammdaten arbeiten

Mit Hilfe dieses Dialogprogramms verwalten Sie alle Stammdaten der Kommunikationspartner, mit denen Sie Daten austauschen möchten. Die hier vorgenommenen Einträge dienen zur Abwicklung der Datenkommunikation mit Geschäftspartnern. Rufen Sie das Dialogprogramm zur Verwaltung der Partnerstammdaten auf, indem Sie im i-effect Hauptmenü die Auswahl 50 treffen.

Sie erhalten folgende Anzeige:



Auswahlmöglichkeiten zum Dialogprogramm

Zur Bearbeitung der Einträge stehen Ihnen folgende Auswahlmöglichkeiten zur Verfügung. Diese können in das entsprechende Auswahlfeld vor der gewünschten Zeile eingegeben werden. Die nachfolgende Übersicht stellt die zur Verfügung stehenden Grundfunktionen dieses Dialogprogramms vor. Eine detaillierte Beschreibung der einzelnen Auswahlmöglichkeiten schließt sich an diese Übersicht an.

Hinzufügen (Auswahl F6)

Mit der Auswahl F6 legen Sie einen neuen Partner an. Legen Sie im nachfolgenden Dialogprogramm zunächst einen eindeutigen Alias für den anzulegenden Kommunikationspartner fest. Nach Angabe des Alias können Sie in weiteren Eingabemasken die zu diesem Alias gehörenden für die Kommunikation benötigten Daten eingeben.

Ändern (Auswahl 2)

Geben Sie die Auswahl 2 in der Auswahlspalte der gewünschten Zeile ein, um diesen bestehenden Eintrag zu ändern. Es werden Ihnen die Daten des Partners im Bezug auf die installierten Module angezeigt, die Sie hier bei Bedarf an neue Vorgaben anpassen können.

Kopieren (Auswahl 3)

Geben Sie die Auswahl 3 in der Auswahlspalte der gewünschten Zeile ein, um diesen bestehenden Eintrag auf einen neuen Alias zu übernehmen.

Löschen (Auswahl 4)

Geben Sie die Auswahl 4 in der Auswahlspalte der gewünschten Zeile ein, um diesen bestehenden Eintrag zu löschen.

Anzeigen (Auswahl 5)

Geben Sie die Auswahl 5 in der Auswahlspalte der gewünschten Zeile ein, um diesen bestehenden Eintrag anzeigen zu lassen.

Umbenennen (Auswahl 7)

Geben Sie die Auswahl 7 in der Auswahlspalte der gewünschten Zeile ein, um diesen bestehenden Eintrag umzubenennen.

EDIFACT-Angaben (Auswahl 8)

Geben Sie die Auswahl 8 in der Auswahlspalte der gewünschten Zeile ein, um für EDIFACT-Kommunikation benötigte Angaben zu diesem Eintrag zu pflegen. Zur Eingabe dieser Angaben gelangen Sie in ein neues Dialogprogramm.

Zusätzliche Adressen (Auswahl 10)

Geben Sie die Auswahl 10 in der Auswahlspalte der gewünschten Zeile ein, um eMail, Fax oder SMS Adressen für diesen Partner zu hinterlegen. Zur Eingabe dieser Angaben gelangen Sie in ein neues Dialogprogramm.

**FLATFILE Angaben
(Auswahl 18)**

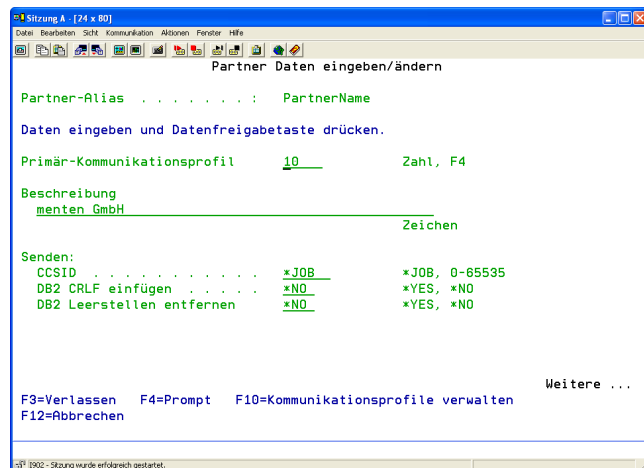
Geben Sie die Auswahl 18 in der Auswahlspalte der gewünschten Zeile ein, um für FLATFILE-Kommunikation benötigte Angaben zu diesem Eintrag zu pflegen. Zur Eingabe dieser Angaben gelangen Sie in ein neues Dialogprogramm.

Statistik (Auswahl 20)

Geben Sie die Auswahl 20 in der Auswahlspalte der gewünschten Zeile ein, um EDIFACT und FLATFILE spezifische Statistiken für diesen Partner anzuzeigen.

Details: F6=Hinzufügen, 2=Ändern, 5=Anzeigen

Bei Auswahl F6, Auswahlziffer 2 oder Auswahlziffer 5 (Anlage, Änderung oder Anzeige von Partnerstammdaten) erhalten Sie die nachstehenden Bildschirmanzeigen.

**Partner-Alias**

Der Partner-Alias ist eine Kurzreferenz der Partnerdefinition. Er kann in Befehlen verwendet werden, um auf Partnerstammdaten zu verweisen.

Primär-Kommunikationsprofil

Geben Sie hier ein zu diesem Eintrag gehöriges Kommunikationsprofil an. Das hier angegebene Profil wird NUR vom Befehl SNDFILE verwendet. Über dieses definierte Primär-Kommunikationsprofil werden von SNDFILE die EDIFACT Daten versendet. Mehr zum Befehl SNDFILE finden Sie in Kapitel 6 „Kommunikation“ in Abschnitt „EDI Kommunikation“.

Beschreibung

Dieser Parameter gibt Ihnen die Möglichkeit, eine Kurzbeschreibung für das angelegte Partnerprofil anzugeben. Diese kann frei gewählt werden. Es empfiehlt sich allerdings, als Beschreibung den offiziellen Namen / Bezeichnung Ihres Partners anzugeben. Im Gegensatz zu dem Alias, der als Schlüssel für den Partnerstamm dient, hat dieses Feld ausschließlich einen beschreibenden Charakter.

Senden**CCSID**

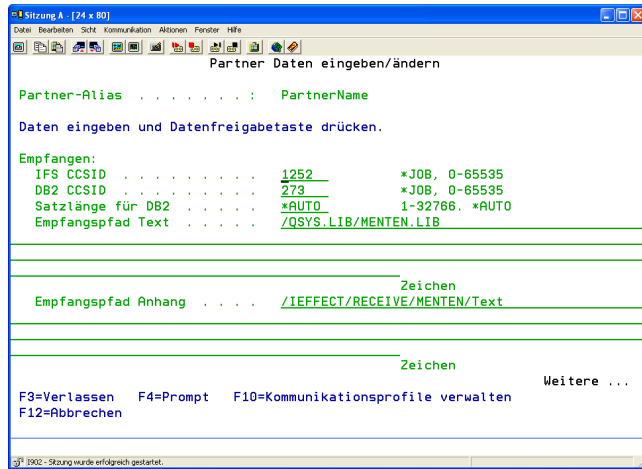
Tragen Sie hier die CCSID (Coded Character Set Identifier) für zu versendende Dateien ein. Wenn sich die Dateien nicht in der hier angegebenen CCSID befinden, werden sie automatisch konvertiert.

DB2 CRLF einfügen

Tragen Sie hier ein, ob für ausgehende DB2-Datenbankdateien jeweils am Datensatzende ein CRLF-Steuerzeichen (Zeilenende) angehängt werden soll.

DB2 Leerstellen entfernen

Tragen Sie hier ein, ob bei zu versendenden DB2-Datenbankdateien vor dem Versand die Leerzeichen am Ende jedes Datensatzes entfernt werden sollen.



Empfangen

IFS CCSID

Tragen Sie hier die CCSID (Coded Character Set Identifier) für empfangene Dateien ein. Die empfangenen Dateien werden unter dieser CCSID im IFS gespeichert, eine Konvertierung findet nicht statt.

DB2 CCSID

Tragen Sie hier die CCSID für empfangene Daten, die in der DB2 gespeichert werden sollen. Die Dateien werden vor der Speicherung von der hier angegebenen CCSID in die CCSID der Datenbank konvertiert.

Anmerkung zu IFS- und DB2-CCSID:

Zeichensatz

Der Standardwert ist *JOB. Bei der Angabe von *JOB erfolgt keine Zeichenumsetzung. Die Daten werden in der EBCDIC Codepage des aktuellen Jobs empfangen. (Auf einem deutschen System IBM iSeries also die Codepage 273). In diesem Feld kann eine beliebige, vom IBM iSeries System unterstützte Codepage ID eingetragen werden. Das System übersetzt die zu empfangenden Daten in die hier eingegebene Zielcodepage.

Typische CCSID-Werte sind:

273	(EBCDIC Deutschland)
273	(EBCDIC England/Amerika)
1252	(ASCII Windows)
850	(ASCII DOS)

Mögliche Sonderwerte:

*JOB Die CCSID des Jobs wird verwendet.

Satzlänge für DB2

Hier legen Sie die maximal Datensatzlänge für DB2 Datensätze fest. Bei Sonderwert *AUTO wird versucht anhand der Daten die Datensatzlänge automatisch zu bestimmen.

Empfangspfad Text

Tragen Sie hier ein, wo empfangene Dateien des Typs „Text“ standardmäßig gespeichert werden sollen.

Empfangspfad Anhang

Tragen Sie hier ein, wo empfangene Dateien des Typs „Anhang“ standardmäßig gespeichert werden sollen.

Daten, die als TEXT oder ANHANG empfangen wurden, werden in der Standardeinstellung in einem IFS Pfad abgelegt. Dieser Pfad ist nach der Installation des Produkts /i-effect/telebox/receive. Dieser Pfad kann überschrieben, und an eigene Bedürfnisse, z.B. Partner-individuelle Empfangsverzeichnisse angepasst werden.

Um empfangene Daten in einer physischen Datei innerhalb der DB/2 abzulegen, ist der Name der Empfangsbibliothek in der Form

/QSYS.LIB/<Name der Bibliothek>.LIB

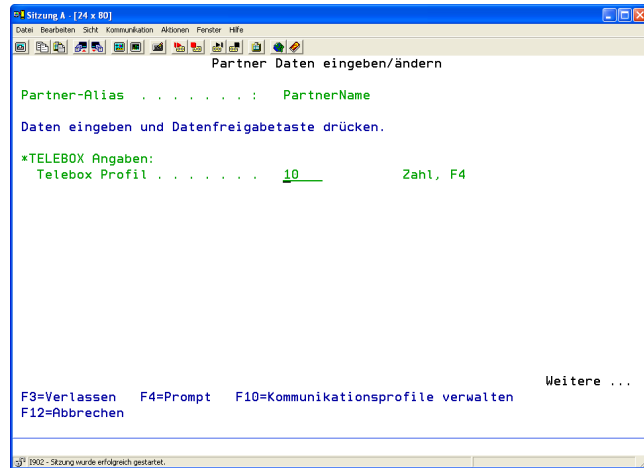
einzugeben. Durch Angabe des folgenden Formats kann der zu erstellenden physischen Datei in der Bibliothek noch ein individueller Prefix zugeordnet werden. Im nachfolgenden Beispiel sollen die Daten in der Bibliothek MYLIB abgelegt werden. Jede Datei soll den Prefix VK haben.

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

Wird also beispielsweise eine Datei mit dem Namen SALES.TXT empfangen, so erhält diese innerhalb der Bibliothek MYLIB den Namen VKSALES.

Hinweis: Bei der Bildung des Namens für die Empfangsdatei in einer Bibliothek wird der Name der Empfangsdatei auf maximal 10 Stellen gekürzt. Sollte eine Datei unter diesem Namen bereits in der Bibliothek vorhanden sein, so wird eine eindeutige laufende Nummer an den verkürzten Namen angehängt. Aus VKSALES wird also z.B. VKSALES1. Wird die Datei in einem IFS-Verzeichnis abgelegt und der Name der Datei existiert dort bereits, erzeugt i-effect durch Anhängen eines fortlaufenden numerischen Suffix einen eindeutigen neuen Dateinamen. Aus SALES.TXT wird so z. B. SALES_1.TXT.

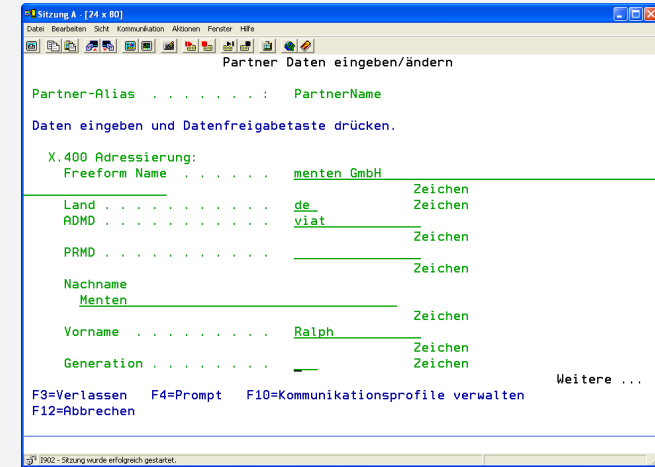
Zusätzlich zu den bereits beschriebenen Parametern, sehen Sie auf Ihren Anzeigen nur die Parameter der bei Ihnen installierten Module. Ein Beschreibung der spezifischen Parameter finden Sie hiernach.



Partnerstammdaten zum Modul *TELEBOX

Telebox Profil

Um Daten zu einem i-effect Profil zuzuordnen, (und damit zu dem Telebox-Partner zu dem eine Verbindung aufzubauen ist) ist hier die Nummer des i-effect Profils einzutragen, das diesen Telebox-Partner beschreibt. Mit der Funktionstaste F4 kann eine Liste der bereits im System definierten Profile zur Auswahl angezeigt werden.



X.400 Adressierung:

Freeform Name:

Name des Adressaten. Geben Sie hier einen beschreibenden Namen für den X.400 Partner an

Land:

Länderschlüssel. Bei Compuserve Teilnehmern z.B. „US“. Die X.400 übliche Abkürzung für dieses Feld lautet „C“.

ADMD:

Das Kürzel für den ADMD (Administration management domaine) Bei Compuserve Teilnehmern z.B. „Compuserve“. Die X.400 übliche Abkürzung für dieses Feld lautet „A“.

PRMD:

Kürzel des PRMD (Private management domaine). Bei Compuserve Teilnehmern z.B. „CSMAIL“. Die X.400 übliche Abkürzung für dieses Feld lautet „P“.

Nachname:

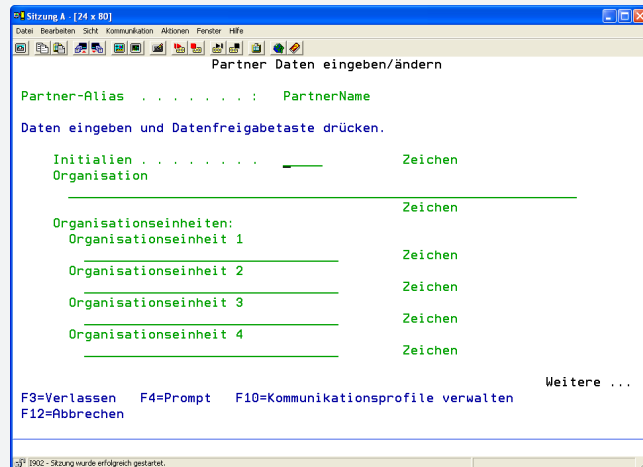
Geben Sie hier den Nachnamen ein. Die X.400 übliche Abkürzung für dieses Feld lautet „S“:

Vorname:

Geben Sie hier den Vornamen ein. Die X.400 übliche Abkürzung für dieses Feld lautet „G“:

Generation:

Kürzel für die Generation. Die X.400 übliche Abkürzung für dieses Feld lautet „GN“:


Initialien:

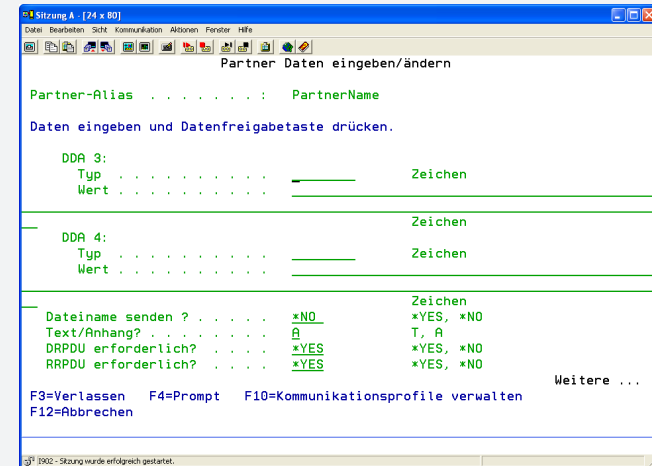
Geben Sie hier die Initialien ein. Die X.400 übliche Abkürzung für dieses Feld lautet „I“:

Organisation:

Angaben zur Organisation. Die X.400 übliche Abkürzung für dieses Feld lautet „O“:

Organisationseinheit 1 bis 4:

Geben Sie hier die Organisationseinheiten ein. Die X.400 übliche Abkürzung für diese Felder lautet „OU“:


DDA 1 bis 4:**Typ:**

Eine von 4 möglichen Angaben zum DDA (Direct distribution attribute). Die X.400 übliche Abkürzung für die DDA Angaben lautet „DDA“. Bei Comuserve Teilnehmern steht hier z.B. „ID“. Mit diesem Eintrag wird der im DDA-Wertefeld eingetragene Wert als Comuserve Identifikationsnummer bekanntgegeben.

Wert:

Wertangabe zur vorherigen Eintragung. Diese Angabe ist in Verbindung mit dem Eintrag DDA Typ zu sehen. Sie sind beide erforderlich und müssen zusammen angegeben werden. Bei Comuserve Teilnehmern kann hier z.B. die Teilnehmernummer erscheinen, wenn im DDA Typ der Eintrag „ID“ eingetragen wurde.

Dateiname senden?

Beim Versenden von Anhängen über diese Schnittstelle kann es je nach Empfänger wünschenswert sein, die Übermittlung des Dateinamens zu unterdrücken. In bestimmten Fällen generiert der weiterleitende ADMD für diesen Dateinamen einen zusätzlichen Text-Bodypart, der beim Empfänger zu Verarbeitungsproblemen führen kann. Mit diesem Parameter kann die Übermittlung des Dateinamens unterdrückt werden.

Mögliche Eingaben sind

- *YES Ja, der Dateiname wird übermittelt.
- *NO Nein, der Dateiname wird nicht übermittelt

Text/Anhang?

Geben Sie an, ob Text oder Anhang verarbeitet werden sollen.

DRPDU erforderlich?

Geben Sie an, ob eine DRPDU Versandbestätigung (delivery report data unit) erforderlich ist.

RRPDU erforderlich?

Geben Sie an, ob eine RRPDU Empfangsbestätigung (receipt report data unit) erforderlich ist.

Partner Daten eingeben/ändern

Partner-Alias PartnerName

Daten eingeben und Datenfreigabetaste drücken.

Priority *NORMAL *NORMAL, *URGENT

*OFTP Angaben:
OFTP Kommunikationsprofil 820 Zahl, F4

*FTP Angaben:
FTP Kommunikationsprofil . . . 41 Zahl, F4

*ZIP Angaben:
Kompressions-Parameter:
Komprimieren ? *NO *YES, *NO
Zip Archiv erzeugen *NO *YES, *NO
Dekompressions-Parameter:
Dekomprimieren ? *NO *YES, *NO

Weitere ...

F3=Verlassen F4=Prompt F10=Kommunikationsprofile verwalten
F12=Abbrechen

1002 - Sitzung wurde erfolgreich gestartet.

Priority:

Legen Sie hier die Dringlichkeit der Kommunikation für diesen Eintrag fest. Möglich sind hier *URGENT (eilig) und *NORMAL.

Partnerstammdaten zum Modul *OFTP**OFTP Kommunikationsprofil:**

Um Daten zu einem i-effect Profil zuzuordnen, (und damit zu dem OFTP-Partner zu dem eine Verbindung aufzubauen ist) ist hier die Nummer des i-effect Profils einzutragen, das diesen entfernten OFTP-Partner beschreibt. Mit der Funktionstaste F4 kann eine Liste der bereits im System definierten Profile zur Auswahl angezeigt werden.

Partnerstammdaten zum Modul *FTP**FTP Kommunikationsprofil:**

Um Daten zu einem i-effect Profil zuzuordnen, (und damit zu dem FTP-Partner zu dem eine Verbindung aufzubauen ist) ist hier die Nummer des i-effect Profils einzutragen, das diesen entfernten FTP-Server beschreibt. Mit der Funktionstaste F4 kann eine Liste der bereits im System definierten Profile zur Auswahl angezeigt werden.

Partnerstammdaten zum Modul *AS2**Empfangspfad Anhang**

Hier werden die Daten der von einem Partner an Sie gesendeten AS2 Nachricht abgespeichert. Das in Parameter „Empfangspfad Text“ definierte Verzeichnis/Bibliothek wird von AS2 nicht verwendet.

Partner Daten eingeben/ändern

Partner-Alias menten

Daten eingeben und Datenfreigabetaste drücken.

Empfangen:
IFS CCSID 1252 *JOB, 0-65535
DB2 CCSID 1252 *JOB, 0-65535
Satzlänge für DB2 *AUTO 1-32766. *AUTO
Empfangspfad Text /qsus.lib/menten

Empfangspfad Anhang /AS2/inbound/partnerDir_

Weitere ...

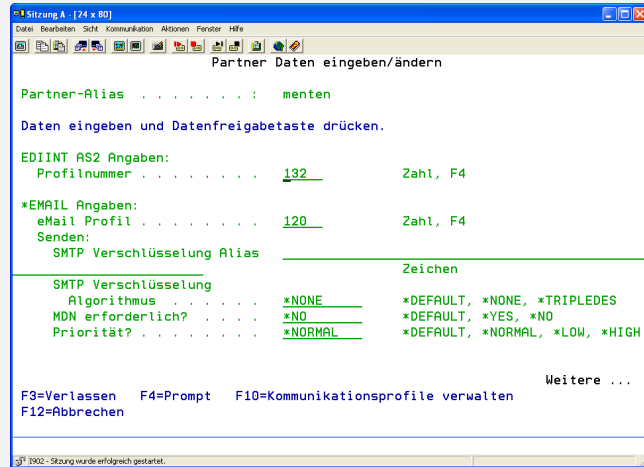
F3=Verlassen F4=Prompt F10=Kommunikationsprofile verwalten
F12=Abbrechen

1002 - Sitzung wurde erfolgreich gestartet.

Profilnummer:

Geben Sie hier ein zu diesem Eintrag gehöriges AS2 Kommunikationsprofil (Sendeprofil) an.

Um Daten zu einem i-effect Profil zuzuordnen, (und damit zu dem AS2-Partner zu dem eine Verbindung aufzubauen ist) ist hier die Nummer des i-effect Profils einzutragen, das diesen entfernten AS2-Server beschreibt. Mit der Funktionstaste F4 kann eine Liste der bereits im System definierten Profile zur Auswahl angezeigt werden.



Bitte achten Sie darauf, dass ein AS2 Kommunikationsprofil NIEMALS gleichzeitig mehreren Partnern zugeordnet ist. Die Verknüpfung von Partner und Sendeprofil stellt eine 1 zu 1 Beziehung dar. Beim Empfang von AS2 Nachrichten erfolgt die Zuordnung des Partners dann über den „umgekehrten“ Weg. Es wird überprüft, welcher Partner einem bestimmten AS2 Sendeprofil zugeordnet ist. Wird ein AS2 Sendeprofil mehreren Partnern zugeordnet, so kann beim AS2 Empfang keine eindeutige Ermittlung des Partners mehr erfolgen.

Partnerstammdaten zum Modul *EMAIL**E-Mail Profil:**

Um Daten einem i-effect Profil zuzuordnen, (und damit zu dem EMAIL-Partner zu dem eine Verbindung aufzubauen ist) ist hier die Nummer des i-effect Profils einzutragen, das diesen EMAIL-Partner beschreibt. Mit der Funktionstaste F4 kann eine Liste der bereits im System definierten Profile zur Auswahl angezeigt werden.

SMTP Verschlüsselung Alias

Name des Alias, unter dem im Keystore der Schlüssel abgelegt ist.

SMTP Verschlüsselungs Algorithmus:

Algorithmus, mit dem die Nachricht verschlüsselt werden soll.

- *DEFAULT* Der Algorithmus wird den Standardeinstellungen des Email-Moduls entnommen (Menü 80).
- *NONE* Die Email wird nicht verschlüsselt.
- *TRIPLEDES* Die EMAIL wird mit dem Triple-DES-Algorithmus (3 x 56 Bit) verschlüsselt.

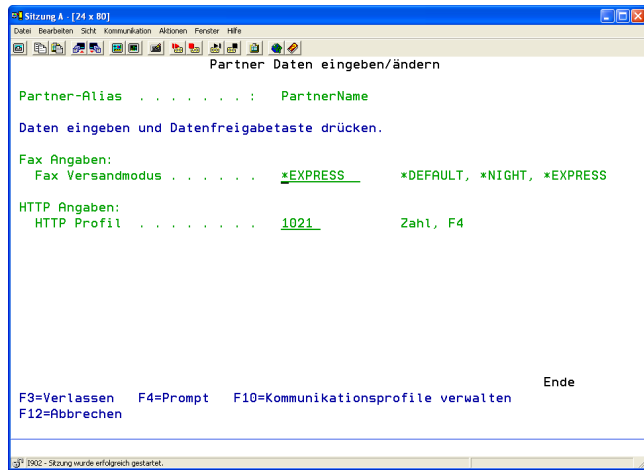
MDN erforderlich?:

Geben Sie hier an, ob Sie eine Email-Versandbestätigung (MDN = Message Delivery Notification) benötigen.

Priorität:

Geben Sie hier die Priorität an mit der die Email versendet werden soll.

- *DEFAULT* Die Priorität wird den Standardeinstellungen des Email-Moduls entnommen (Menü 80).
- *NORMAL* Die Email wird mit normaler Priorität versendet.
- *HIGH* Die Email wird mit hoher Priorität versendet.
- *LOW* Die Email wird mit niedriger Priorität versendet.



Für eine variable Steuerung der Empfänger-, CC-, und BCC Adressen haben Sie Möglichkeit, diese Adressen für jeden Partner zu hinterlegen. Wenn Sie im Befehl SNDEMAIL (alternativ: i-effect Hauptmenü 13, dann 30) einen Partner bei Parameter „Empfänger Partner-ID“ angeben, wird die eMail automatisch an alle für den Partner definierten Adressen versendet.

In gleicher Weise können eMails auch partnergesteuert empfangen und abgespeichert werden. Dies geschieht indem Sie eMailabsenderadressen für einen Partner hinterlegen. Beim Empfang von eMails mittels des Befehls RCVEMAIL (alternativ: i-effect Hauptmenü 13, dann 31) wird die Absenderadresse jeder eMail überprüft und mit den im Partnerstamm hinterlegten Absenderadressen verglichen. Stimmen die Adressen überein, wird die eMail dem jeweiligen Partner zugeordnet und die Partneinstellungen (Pfade, CCSID, etc.) werden für den Empfang verwendet.

Partnerstammdaten zum Modul *FAX

Fax Versandmodus

Geben Sie hier die Priorität an mit der ein Fax versendet werden soll.

- **DEFAULT* Die Priorität wird den Standardeinstellungen des Fax-Moduls entnommen.
- **NIGHT* Das Fax wird kostengünstig mit niedriger Priorität versendet. (Nachtтарif)
- **EXPRESS* Das Fax wird unverzüglich mit hoher Priorität versendet. (Tagtarif)

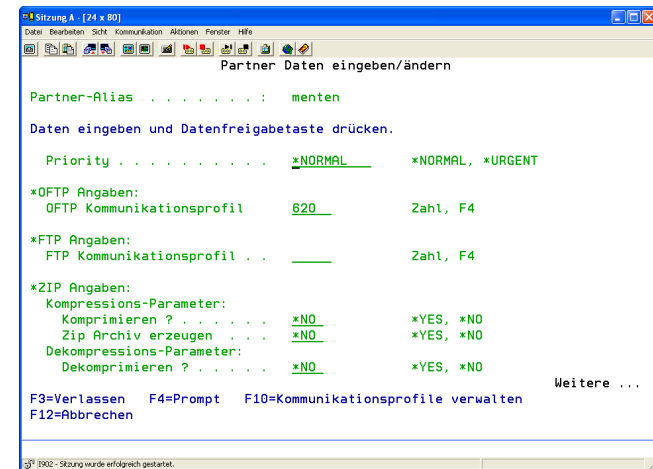
Partnerstammdaten zum Modul *HTTP

HTTP Profil:

Um Daten einem i-effect Profil zuzuordnen, (und damit zu dem HTTP-Partner zu dem eine Verbindung aufzubauen ist) ist hier die Nummer des i-effect Profils einzutragen, das diesen entfernten HTTP-Server beschreibt. Mit der Funktionstaste F4 kann eine Liste der bereits im System definierten Profile zur Auswahl angezeigt werden.

Partnerstammdaten zum Modul *FTP

Die nachfolgenden Angaben beschreiben die Parameter, die bei installiertem *FTP Modul sichtbar sind.

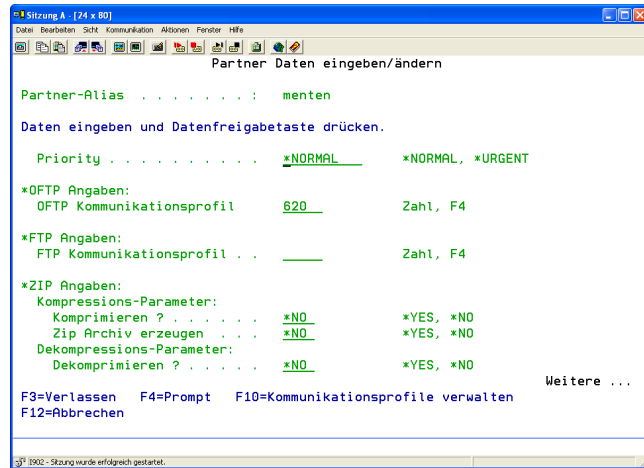


Kommunikationsprofil

Um Daten einem i-effect Profil zuzuordnen, (und damit zu dem FTP-Partner zu dem eine Verbindung aufzubauen ist) ist hier die Nummer des i-effect Profils einzutragen, das diesen entfernten FTP-Server beschreibt. Mit der Funktionstaste F4 kann eine Liste der bereits im System definierten Profil zur Auswahl angezeigt werden.

Partnerstammdaten zum Modul *ZIP

Die nachfolgenden Angaben beschreiben die Parameter, die bei installiertem *ZIP Modul sichtbar sind.



Kompressions-Parameter:

Komprimieren?

Legt fest, ob bei diesem Partner automatisch eine Komprimierung der Sendedaten mit i-effect erfolgen soll.

- | | |
|------|---|
| *YES | Ja, eine Komprimierung der Daten soll erfolgen. |
| *NO | Nein, zu sendenden Daten werden nicht komprimiert |

ZIP Archiv erzeugen:

Bei der Komprimierung kann entweder eine gzip Datei oder ein ZIP Archiv erzeugt werden.

- | | |
|------|---|
| *YES | Ja, es wird ein ZIP Archiv erzeugt. |
| *NO | Nein, es wird eine einfache gzip Datei erzeugt. |

Dekompressions-Parameter:

Dekomprimieren ?

Legt fest, ob bei diesem Partner automatisch eine Dekomprimierung der empfangenen Daten mit i-effect erfolgen soll.

Mögliche Werte:

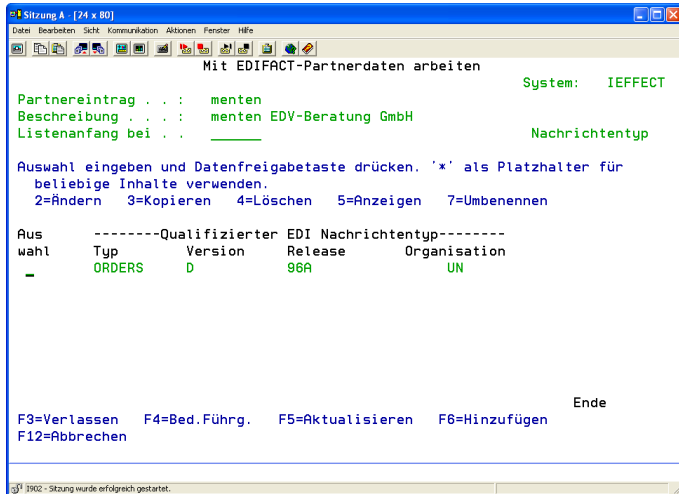
- | | |
|------|--|
| *YES | Ja, eine Dekomprimierung der Daten soll erfolgen. |
| *NO | Nein, zu empfangene Daten werden nicht dekomprimiert |

Hinweis für die Module *AS2, *EMAIL, *HTTP, *FTP und *TELEBOX im Zusammenhang mit GZIP Kompression

Wenn für das Senden/Empfangen ein Partner angegeben/erkannt wurde, so werden die hier hinterlegten ZIP-Einstellungen auf die Sende/Empfangsdateie(n) angewendet. Sofern eingestellt, wird jede Eingabedatei GZIP gepackt, jede empfangene GZIP Datei automatisch entpackt.

Details: 8=EDIFACT Angaben

Durch die Auswahl 8 wird Ihnen eine Übersicht über alle diesem Partner zugeordneten Nachrichtentypen angezeigt. Hier können Sie auch definieren, welche Nachrichtentypen für diesen Partner verarbeitet werden dürfen. Jede eingehende oder zu versendende Nachricht wird von i-effect zunächst dahingehend geprüft, ob dieser Nachrichtentyp für diesen Partner freigegeben ist. Andernfalls wird keine Konvertierung durchgeführt.



Hinzufügen (Auswahl F6)

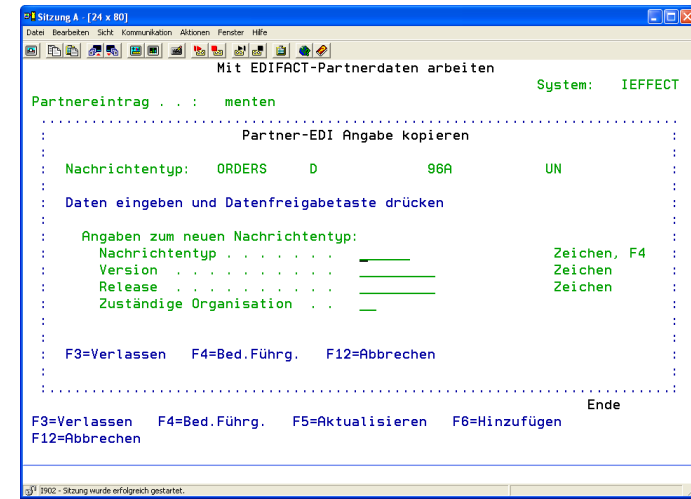
Mit der Auswahl F6 legen Sie einen neuen Eintrag an. Sie erhalten daraufhin eine Anzeige, in der Sie die erforderlichen Daten eingeben können.

Ändern (Auswahl 2)

Geben Sie die Auswahl 2 in der Auswahlspalte der gewünschten Zeile ein, um diesen bestehenden Eintrag zu ändern. Es werden Ihnen die Daten des Partners im Bezug auf den gewählten Nachrichtentyp zur Änderung angezeigt.

Kopieren (Auswahl 3)

Geben Sie die Auswahl 3 in der Auswahlspalte der gewünschten Zeile ein, um diesen bestehenden Eintrag zu kopieren.



In der folgenden Anzeige können die Schlüsselfelder des zu erstellenden neuen Eintrags eingetragen werden. Nach Betätigen der Datenfreigabetaste wird der gewählte Eintrag kopiert und unter dem neuen Nachrichtentyp abgelegt.

Löschen (Auswahl 4)

Geben Sie die Auswahl 4 in der Auswahlspalte der gewünschten Zeile ein, um diesen bestehenden Eintrag zu löschen.

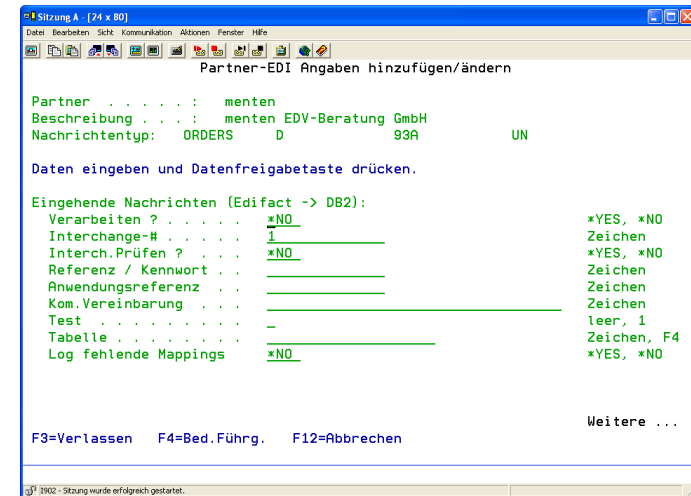
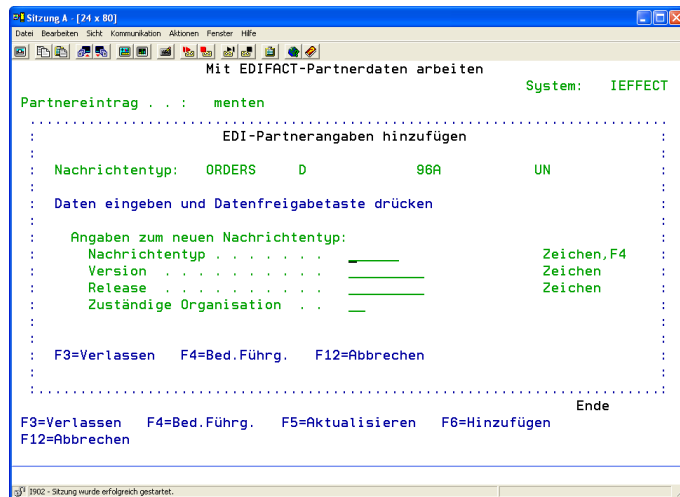
Anzeigen (Auswahl 5)

Geben Sie die Auswahl 5 in der Auswahlspalte der gewünschten Zeile ein, um diesen bestehenden Eintrag anzeigen zu lassen.

Umbenennen (Auswahl 7)

Geben Sie die Auswahl 7 in der Auswahlspalte der gewünschten Zeile ein, um diesen bestehenden Eintrag umbenennen.

Details zu: F6=Hinzufügen, 5=Anzeigen, 2=Ändern



Hier werden die Parameter zum Bearbeiten von EDIFACT-Partnerdaten beschrieben.

Nachrichtentyp - Nachrichtentyp für EDI-Angaben.

Der qualifizierte Nachrichtentyp, für den EDI-Angaben hinterlegt werden sollen. Mit F4 kann eine Liste der derzeit geladenen EDIFACT Directories zur Auswahl eines Nachrichtentyps angefordert werden.

Version - Versionsnummer des Nachrichtentyps.

Die Versionsnummer des EDIFACT Standards, mit dem dieser Nachrichtentyps definiert wurde.

Release - Releasenummer des Nachrichtentyps

Die Releasenummer des EDIFACT Standards, mit dem dieser Nachrichtentyp definiert wurde.

Zuständige Organisation

Das hier einzutragende Kürzel steht für die zuständige Organisation, die diesen EDIFACT-Standard definiert hat.

Eingehende Nachrichten (EDIFACT --> DB/2)

Hier können Sie die Partnerstammdaten für eingehende EDIFACT-Nachrichten hinterlegen.

Verarbeiten

Legt fest, ob für den angezeigten Nachrichtentyp und Partner die EDIFACT Dateien konvertiert werden.

- *YES EDIFACT Dateien werden verarbeitet.
- *NO EDIFACT Dateien werden NICHT verarbeitet.

Interchange # - Die nächste erwartete Interchange Nummer

Ist beim folgenden Parameter (Interchange prüfen) die Prüfung dieser Folge Nummer im UNB-Segment aktiviert, so MUSS die nächste zu verarbeitende Datei dieses Partners mit diesem Nachrichtentyp die hier verzeichnete Folge Nummer aufweisen. Ist dies nicht der Fall wird die Konvertierung abgebrochen. i-effect erhöht diese Nummer bei jeder erfolgreichen Konvertierung automatisch um 1.

Interchange prüfen

Schaltet die Überprüfung der UNB Zählnummer an oder aus.

- *YES Die Interchange Nummer wird geprüft. Bei Abweichung zu der im vorherigen Feld eingetragenen Nummer wird die Konvertierung abgebrochen.
- *NO Die Interchange Nummer wird NICHT geprüft.

Referenz / Kennwort

Ist in diesem Feld ein Wert eingetragen, so wird das entsprechende Feld im UNB Segment (Service-Segment, Header) der zu verarbeitenden EDIFACT Datei geprüft. Nur bei Übereinstimmung wird die Verarbeitung fortgesetzt.

Anwendungsreferenz

Ist in diesem Feld ein Wert eingetragen, so wird das entsprechende Feld im UNB Segment der zu verarbeitenden EDIFACT Datei geprüft. Nur bei Übereinstimmung wird die Verarbeitung fortgesetzt.

Kommunikationsvereinbarung

Ist in diesem Feld ein Wert eingetragen, so wird das entsprechende Feld im UNB Segment der zu verarbeitenden EDIFACT Datei geprüft. Nur bei Übereinstimmung wird die Verarbeitung fortgesetzt.

Test

Ist in diesem Feld ein Wert eingetragen, so wird das entsprechende Feld im UNB Segment der zu verarbeitenden EDIFACT Datei geprüft. Nur bei Übereinstimmung wird die Verarbeitung fortgesetzt.

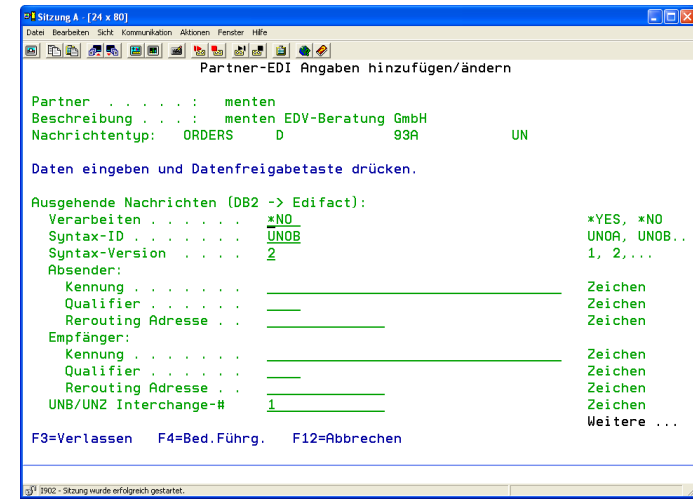
Tabelle

Der Name der i-effect Konvertertabelle, die für diese Konvertierung verwendet werden soll. Die Tabelle muss die Konvertierung des hier festgelegten Nachrichtentyp beschreiben. Durch Drücken der Funktionstaste F4 kann eine Liste der geladenen Mappingtabellen zur Auswahl angezeigt werden.

LOG fehlende Mappings

Auf Wunsch werden im Logbuch während einer Konvertierung alle EDIFACT Datenelemente aufgezeichnet, für die keine Zuordnung zu einem DB/2 Feld festgelegt wurde. Im Testbetrieb lassen sich so fehlende Zuordnungen leicht aufspüren.

- *YES Nicht zugeordnete Datenelemente werden im Logbuch aufgezeichnet.
- *NO Es erfolgt keine Aufzeichnung.



Ausgehende Nachrichten (DB/2 --> EDIFACT)

Hier können Sie die Partnerstammdaten für ausgehende EDIFACT-Nachrichten hinterlegen.

Verarbeiten

Legt fest, ob für den angezeigten Nachrichtentyp und Partner EDIFACT Dateien erzeugt werden.

- *YES EDIFACT Dateien werden erzeugt.
- *NO EDIFACT Dateien werden NICHT erzeugt.

Syntax-ID

Ist in diesem Feld ein Wert eingetragen, so wird das Feld S001-0001 im UNB Segment mit diesem Wert gefüllt, sobald die Funktion *SYNID beim Mapping verwendet wird.

Syntax-Version

Ist in diesem Feld ein Wert eingetragen, so wird das Feld S001-0002 im UNB Segment mit diesem Wert gefüllt, sobald die Funktion *SYNVER beim Mapping verwendet wird.

Absender**Absender Kennung**

Ist in diesem Feld ein Wert eingetragen, so wird das Feld S002-0004 im UNB Segment mit diesem Wert gefüllt, sobald die Funktion *SNDID beim Mapping verwendet wird.

Absender Qualifier

Ist in diesem Feld ein Wert eingetragen, so wird das Feld S002-0007 im UNB Segment mit diesem Wert gefüllt, sobald die Funktion *SNDQUAL beim Mapping verwendet wird.

Absender Rerouting Adresse

Ist in diesem Feld ein Wert eingetragen, so wird das Feld S002-0008 im UNB Segment mit diesem Wert gefüllt, sobald die Funktion *SNDREROUTE beim Mapping verwendet wird.

Empfänger**Empfänger Kennung**

Ist in diesem Feld ein Wert eingetragen, so wird das Feld S003-0010 im UNB Segment mit diesem Wert gefüllt, sobald die Funktion *RCPID beim Mapping verwendet wird.

Empfänger Qualifier

Ist in diesem Feld ein Wert eingetragen, so wird das Feld S003-0007 im UNB Segment mit diesem Wert gefüllt, sobald die Funktion *RCPQUAL im Mapping verwendet wird.

Empfänger Rerouting Adresse

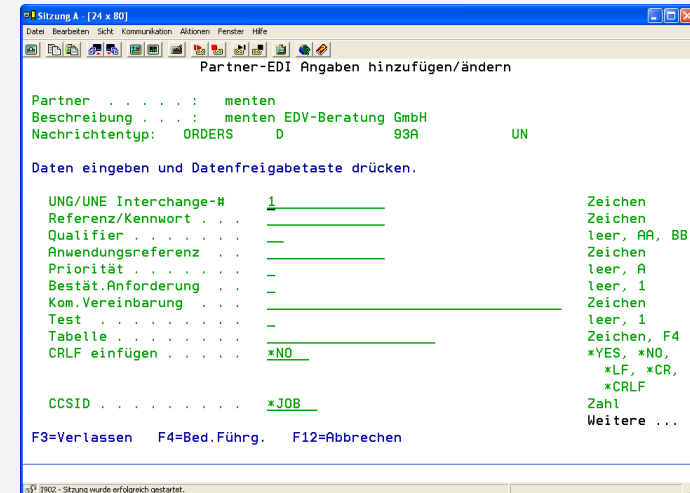
Ist in diesem Feld ein Wert eingetragen, so wird das Feld S003-0014 im UNB Segment mit diesem Wert gefüllt, sobald die Funktion *RCPROUTE im Mapping verwendet wird.

UNB/UNZ Interchange #

Ist in diesem Feld ein Wert eingetragen, so wird das Feld 0020 im UNB Segment mit diesem Wert gefüllt, sobald die Funktion *INTREF im Mapping verwendet wird. Nach jeder erzeugten EDIFACT Datei für diesen Partner wird der hier angezeigte Wert automatisch um „1“ erhöht.

UNG/UNE Interchange #

Ist in diesem Feld ein Wert eingetragen, so wird das Feld 0048 im UNG Segment mit diesem Wert gefüllt, sobald die Funktion *GRPREF im Mapping verwendet wird. Nach jeder erzeugten Gruppe für diesen Partner wird der hier angezeigte Wert automatisch um „1“ erhöht.


Referenz / Kennwort

Ist in diesem Feld ein Wert eingetragen, so wird das Feld S005-0022 im UNB Segment mit diesem Wert gefüllt, sobald die Funktion *REFPW im Mapping verwendet wird.

Qualifier

Ist in diesem Feld ein Wert eingetragen, so wird das Feld S005-0025 im UNB Segment mit diesem Wert gefüllt, sobald die Funktion *REFQUA im Mapping verwendet wird.

Anwendungsreferenz

Ist in diesem Feld ein Wert eingetragen, so wird das Feld 0026 im UNB Segment mit diesem Wert gefüllt, sobald die Funktion *APPREF im Mapping verwendet wird.

Priorität

Ist in diesem Feld ein Wert eingetragen, so wird das Feld 0029 im UNB Segment mit diesem Wert gefüllt, sobald die Funktion *PRIO im Mapping verwendet wird.

Bestätigungsanforderung

Ist in diesem Feld ein Wert eingetragen, so wird das Feld 0031 im UNB Segment mit diesem Wert gefüllt, sobald die Funktion *ACQREQ im Mapping verwendet wird.

Kommunikations Vereinbarung

Ist in diesem Feld ein Wert eingetragen, so wird das Feld 0032 im UNB Segment mit diesem Wert gefüllt, sobald die Funktion *COMREQ im Mapping verwendet wird.

Test

Ist in diesem Feld ein Wert eingetragen, so wird das Feld 0035 im UNB Segment mit diesem Wert gefüllt, sobald die Funktion *TEST im Mapping verwendet wird.

Tabelle

Der Name der i-effect Konvertertabelle, die für diese Konvertierung verwendet werden soll. Die Tabelle muss die Konvertierung des hier festgelegten Nachrichtentyp beschreiben. Durch Drücken der Funktionstaste F4 kann eine Liste der geladenen Mappingtabellen zur Auswahl angezeigt werden.

CRLF einfügen

Legt fest, ob am Ende eines jeden erzeugten EDIFACT-Segments die Steuerzeichen für CRLF eingefügt werden sollen.

*YES	Die Steuerzeichen werden eingefügt.
*NO	Es werden keine Steuerzeichen eingefügt.

CCSID

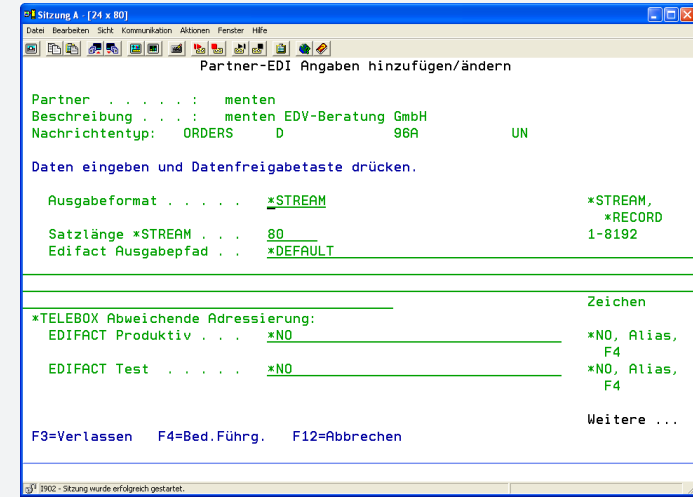
Durch die Angabe einer CCSID (Coded character set identification) werden die EDIFACT Daten während der Verarbeitung in den jeweiligen Zeichensatz umgesetzt. Hierbei können sowohl EBCDIC als auch ASCII Zeichensätze angegeben werden. Sind Quell- und Ziel CCSID identisch erfolgt keine Umsetzung.

Typische CCSID-Werte sind:

273	(EBCDIC Deutschland)
037	(EBCDIC England/Amerika)
1252	(ASCII Windows)
850	(ASCII DOS)

Mögliche Sonderwerte:

*JOB	Die CCSID des Jobs wird verwendet.
------	------------------------------------



Ausgabeformat

Nur gültig bei Wahl des Ausgabedateisystems *DB2. Bestimmt das Ausgabeformat der physischen Datei, in die EDIFACT-Daten geschrieben werden.

*STREAM	Alle EDIFACT Segmente werden hintereinander ausgegeben. Das Satzende der Datei ist nicht das Ende eines Segments.
*RECORD	Jedes EDIFACT Segment wird in einen eigenen Datensatz ausgegeben.

Satzlänge *STREAM

Nur gültig bei Wahl des Ausgabedateisystems *DB2 und Angabe des Ausgabeformats *STREAM. Die erzeugte EDIFACT Datei wird mit der hier angegebenen Satzlänge erstellt.

EDIFACT Ausgabepfad

Ausgabepfad, welcher für den momentan bearbeiteten Partner und EDIFACT Nachrichtentyp zu verwenden ist. In diesen Ausgabepfad werden die erzeugten EDIFACT Dateien abgelegt.

Folgende Sonderwerte stehen zur Verfügung

*DEFAULT	Der Ausgabepfad wird den Standard-Moduleinstellungen des EDIFACT-Moduls entnommen.
----------	--

Benennung EDIFACT-Datei

Der Name der erzeugten EDIFACT Datei. Der Dateiname kann dynamisch nach dem hier eingetragenen Muster bestimmt werden. Dafür stehen folgende Variablen zur Verfügung:

%MSGTYPE%	Nachrichtentyp
%APPREF%	Anwendungsreferenz
%SENDER%	Absender-Kennung
%RECIPIENT%	Empfänger-Kennung
%YEAR%	Jahr YYYY
%MONTH%	Monat MM
%DAY%	Tag DD
%INTREF%	Datenaustauschreferenz (interchange number)
%PARTNER%	Zugeordnete Partnereintrag
%TIMESTAMP%	Zeitpunkt bei Erzeugung der EDI-Datei

Abweichende *TELEBOX Adressierung - EDIFACT Produktiv

Ermöglicht es, für den Versand von Daten über das *TELEBOX Modul abweichende Adressierungen in Abhängigkeit vom Testkennzeichen zu wählen. Sollen die hier selektierten EDIFACT Nachrichtentypen an den hier ausgewählten Partner übermittelt werden und ist die Datei OHNE Testkennzeichen erstellt worden, so gilt die hier eingetragene Adresse (der Eintrag unter diesem Alias) als die Datenquelle zur Bestimmung der Adressierung.

Mit Hilfe dieser Parameter kann also ohne Änderung des UNB Empfängeralias eine zwischen Test und Produktivbetrieb abweichende Adressierung realisiert werden.

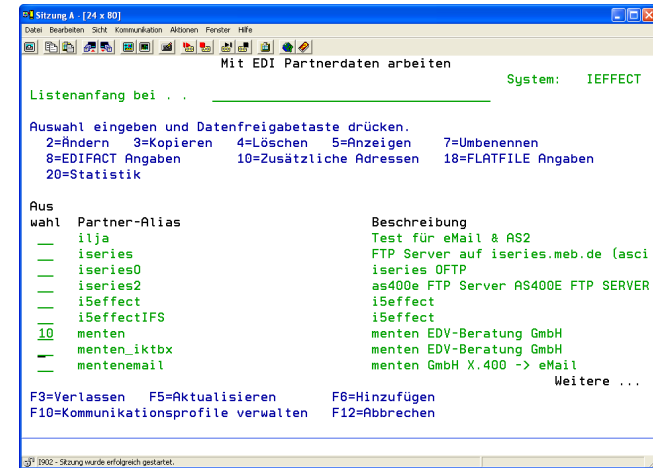
Abweichende *TELEBOX Adressierung - EDIFACT Test

Ermöglicht es, für den Versand von Daten über das *TELEBOX Modul abweichende Adressierungen in Abhängigkeit vom Testkennzeichen zu wählen. Sollen die hier selektierten EDIFACT Nachrichtentypen an den hier ausgewählten Partner übermittelt werden und ist die Datei MIT Testkennzeichen erstellt worden, so gilt die hier eingetragene Adresse (der Eintrag unter diesem Alias) als die Datenquelle zur Bestimmung der Adressierung.

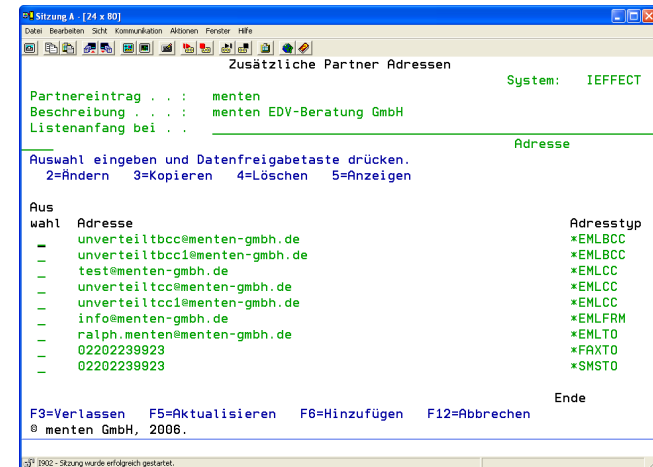
Mit Hilfe dieser Parameter kann also ohne Änderung des UNB Empfängeralias eine zwischen Test und Produktivbetrieb abweichende Adressierung realisiert werden.

Details: 10=Additional Addresses

In das Menü zum Anlegen der Adressen gelangen Sie über Menüpunkt 50 und dann mit Auswahl 10 „Zusätzliche Adressen“ vor den gewünschten Eintrag.



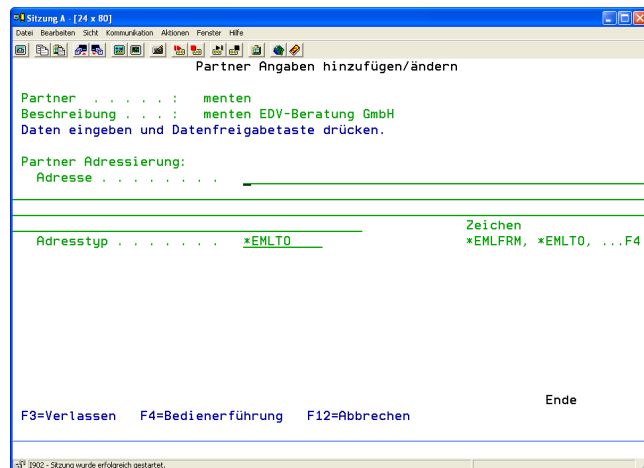
Sie erhalten folgende Anzeige:



Die nachfolgende Übersicht stellt die zur Verfügung stehenden Grundfunktionen dieses Dialogprogramms vor.

- Hinzufügen (Auswahl F6)** Mit der Auswahl F6 legen Sie eine neue Adresse an. Legen Sie im nachfolgenden Dialogprogramm den Adressname sowie Adresstyp fest.
- Ändern (Auswahl 2)** Geben Sie die Auswahl 2 in der Auswahlspalte der gewünschten Zeile ein um diesen bestehenden Eintrag zu ändern.
- Kopieren (Auswahl 3)** Geben Sie die Auswahl 3 in der Auswahlspalte der gewünschten Zeile ein um diese bestehende Adresse auf einen neuen Eintrag zu übernehmen.
- Löschen (Auswahl 4)** Geben Sie die Auswahl 4 in der Auswahlspalte der gewünschten Zeile ein um diesen bestehenden Eintrag zu löschen.
- Anzeigen (Auswahl 5)** Geben Sie die Auswahl 5 in der Auswahlspalte der gewünschten Zeile ein um diesen bestehenden Eintrag anzeigen zu lassen.

Drücken Sie nun F6 um eine neue Adresse anzulegen. Sie erhalten folgende Anzeige:



Adresse

Geben Sie hier die zusätzliche Adresse ein, die mit dem ausgewählten Partner verwendet werden soll. Diese muss entweder eine gültige Email-Adresse, Telefaxnummer oder Handy-Nummer sein, je nach gewünschter Anwendung.

Adresstyp

Geben Sie hier den Typ der zuvor angegebenen Adresse an.

Mögliche Werte sind:

**EMLFRM* Die zuvor eingegebene Adresse wird als Email-Absenderadresse behandelt.

Bei Adresstyp **EMLFRM* haben Sie die Möglichkeit Wildcards im Adressnamen anzugeben. Zulässig sind * und ?. Somit können beim eMailempfang z.B. alle eMails aus den USA einem Standard-Partner zugeordnet und entsprechend gespeichert werden.

Beispiele:

**@*.com* – für alle eMails aus den USA

@myCompany. – für alle eMails von myCompany

vertrieb@.de* – für alle eMails aus Deutschland mit dem Absender „Vertrieb“

**EMLT0* Die zuvor eingegebene Adresse wird als Email-Adressat behandelt.

**EMLCC* Die zuvor eingegebene Adresse wird als Email-Verteileradresse behandelt.

**EMLBCC* Die eingegebene Adresse wird als Email-Blindkopieadresse behandelt.

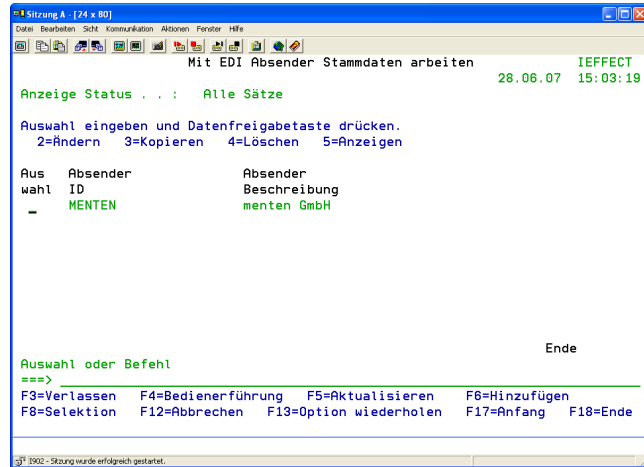
**FAXT0* Die eingegebene Adresse wird als Telefax-Adressatennummer behandelt.

**SMST0* Die eingegebene Adresse wird als SMS-Adressatennummer behandelt.

Menüpunkt 51: Mit EDI Absender Stammdaten arbeiten

Das Anlegen von Absender Stammdaten erfolgt über das Dialogprogramm 51 (Mit EDI Absender Stammdaten arbeiten). Geben Sie hierzu die Auswahl 52 im i-effect Hauptmenü ein.

Folgendes Dialogprogramm kommt zur Anzeige:



In diesem Menü können Sie Absenderinformationen für die Module *AS2, *EMAIL, *OFTP und für *HTTP erstellen und bearbeiten.

Zur Bearbeitung der Einträge stehen Ihnen folgende Auswahlmöglichkeiten zur Verfügung. Diese können in das entsprechende Auswahlfeld vor der gewünschten Zeile eingegeben werden. Die nachfolgende Übersicht stellt die zur Verfügung stehenden Grundfunktionen dieses Dialogprogramms vor.

Anlegen einer neuen Adresse (Option F6)

Mit der Auswahl F6 legen Sie einen neuen Absendereintrag an. Danach haben Sie dann die Möglichkeit den Absendereintrag mit Auswahl 2 zu konfigurieren.

Ändern einer Adresse (Option 2)

Zeigt Ihnen die Definition einer Adresse zur Änderung an. Die Auswahl kann zusammen mit einem Alias in der ersten Zeile der Adressübersicht oder vor der gewünschten Zeile angegeben werden. Nach Drücken der Datenfreigabetaste wird der Änderungsbildschirm angezeigt.

Kopieren einer Adresse (Option 3)

Kopiert eine vorhandene Adresseintragung in eine neue Adresseintragung. Die Auswahl kann zusammen mit einem Alias in der ersten Zeile der Profilübersicht oder vor der gewünschten Zeile angegeben werden. Nach Drücken der Datenfreigabetaste werden Sie zu Eingabe der Ziel Adresse aufgefordert.

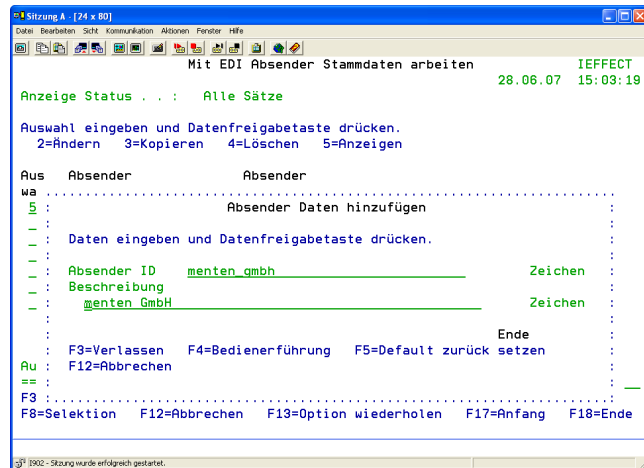
Löschen einer Adresse (Option 4)

Löscht eine vorhandene Adresseintragung. Die Auswahl kann zusammen mit einem Alias in der ersten Zeile der Adressübersicht oder vor der gewünschten Zeile angegeben werden. Nach Drücken der Datenfreigabetaste werden Sie zur Bestätigung der Löschung der Adresse aufgefordert.

Anzeigen einer Adresse (Option 5)

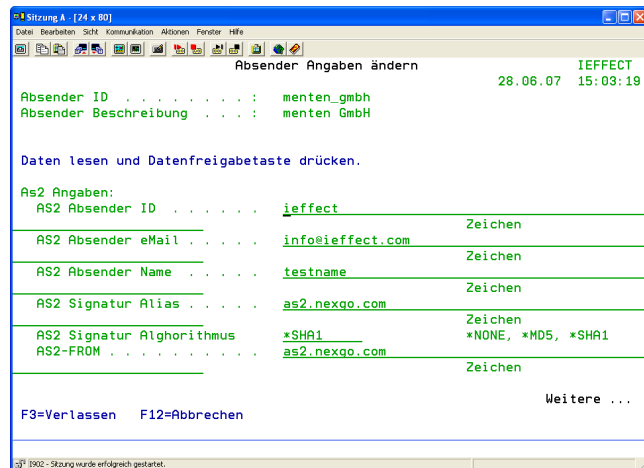
Zeigt eine vorhandene Adresseintragung an. Die Auswahl kann zusammen mit einem Alias in der ersten Zeile der Adressübersicht oder vor der gewünschten Zeile angegeben werden. Nach Drücken der Datenfreigabetaste werden die Daten zu dieser Adresse angezeigt.

Details zu: F6=Hinzufügen, 2=Ändern, 5=Anzeigen



Beim Anlegen eines neuen Absendereintrags können Sie eine eindeutige ID/Namen und eine Beschreibung des Eintrags vornehmen. Der Eintrag steht dann später unter der angegebenen ID zur Auswahl zur Verfügung. Die Beschreibung kann einen detaillierteren Text aufnehmen und findet keine weitere Verwendung, ist aber nützlich um den Eintrag besser zu dokumentieren.

Nachdem Sie einen Eintrag zur Änderung ausgewählt haben, können Sie folgende Absenderangaben konfigurieren:

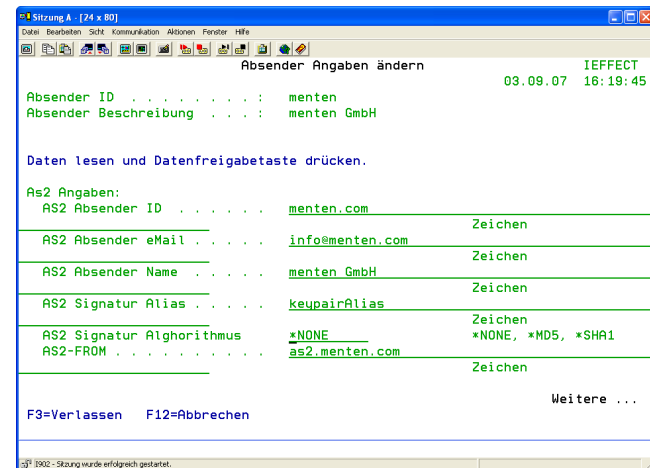


Absenderangaben zum Modul *AS2

Im Abschnitt „AS2 Angaben“ können Sie Ihre absenderspezifischen AS2 Daten für die Kommunikation hinterlegen. Damit haben Sie z.B. die Möglichkeit, falls dies erforderlich ist, bei der Kommunikation mit unterschiedlichen Partnern jeweils andere AS2 Absenderdaten zu verwenden. Auf alle in diesem Eintrag hinterlegten AS2 Daten kann später referenziert werden, indem im Befehl SDNAS2 beim Parameter „Absender ID“ der Name dieses Eintrags angegeben wird. Dies erspart die unnötige Wiederholung der Eingabe von gleich bleibenden Daten.

In das Menü zum Anlegen eines AS2 Absenderpartners gelangen Sie, indem Sie im i-effect Hauptmenü den Menüpunkt 51 auswählen. Im darauf folgenden Menü sehen Sie eine Liste der, falls schon Partner angelegt wurden, bereits vorhandenen Absenderpartner. Rufen Sie nun durch Drücken von F6 das Menü zum Anlegen eines Absenderpartners auf und geben diesem einen eindeutigen Namen sowie eine Beschreibung. Nach dem Drücken der Datenfreigabetaste sehen Sie wieder die Liste der Absenderpartner inklusive dem neu angelegten Partner. Gehen Sie nun mit Auswahl 2 vor den neu erstellten Partner.

Sie erhalten folgende Anzeige:



AS2 Absender ID

Die Absender ID wird dazu verwendet eine eindeutige Nachrichten ID (in der Form: <i-effect AS2Client-30092005092214+0200-0438@ieffect.com>) für Ihre zu versendende AS2-Nachricht zu erstellen. Es empfiehlt sich als Absender ID Ihren Domainnamen zu verwenden, da dieser im Internet ebenfalls eindeutig ist. Diese ID wird für in den Headern der AS2 Nachricht mit übertragen.

AS2 Absender eMail

Hier haben Sie die Möglichkeit eine eMail Adresse anzugeben, unter der Sie ggf. über misslungene AS2-Transaktionen oder generell erreichbar sein wollen. Üblicherweise ist dies die Adresse der EDI-Abteilung oder die des Ansprechpartners für AS2.

AS2 Absender Name

In dem Parameter "Absender name" können Sie entweder den offiziellen Namen Ihrer Organisation, Ihres Unternehmens angeben oder den Namen der i-effect AS2 Software (Default Wert). Allerdings besitzt dieser Parameter ausschließlich einen beschreibenden Charakter und spielt keine tragende Rolle bei dem Empfangs- sowie Sendeprozess und kann somit frei von Ihnen gewählt werden. Dieser Name wird in den Headern der AS2 Nachricht mit übertragen.

AS2 Signatur Alias

Geben Sie hier den Aliasnamen Ihres Schlüsselpaars im Keystore an. Mit diesem Schlüsselpaar (genauer: mit dem privaten Schlüssel) wird die AS2 Nachricht digital signiert. Es ist zwingend erforderlich, dass der hier eingetragene Aliasname identisch zu dem Aliasnamen ist, unter dem Ihr Schlüsselpaar im Keystore abgespeichert wurde.

AS2 Signatur Algorithmus

In diesem Parameter wird festgelegt, mit welchem Algorithmus die *AS2 Nachricht signiert wird. Dabei stehen folgende Werte zur Auswahl:

- *NONE Die Nachricht wird nicht signiert
- *MD5 Die Nachricht wird mit einer MD5 (Message Digest 5) Signatur versehen.
- *SHA1 Die Nachricht wird mit einer SHA1 (Secure Hash Algorithm 1) Signatur versehen.

AS2-FROM

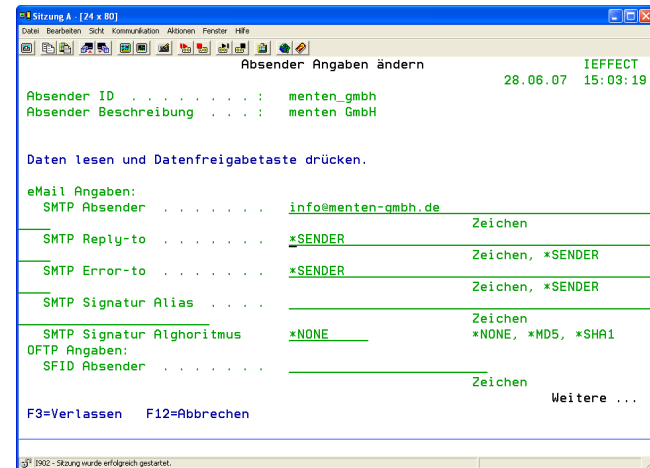
Dies ist die eindeutige AS2 Absender ID. Sie wird als „Absender“ in der gesendeten Nachricht eingetragen. Mittels dieser ID erfolgt beim Empfänger die eindeutige Zuordnung Ihrer gesendeten AS2 Nachricht.

Absenderangaben zum Modul *EMAIL

In einem EMAIL Absenderpartner können Sie Ihre absenderspezifischen EMAIL Daten für die Kommunikation hinterlegen. Damit haben Sie z.B. die Möglichkeit, falls dies erforderlich ist, bei der Kommunikation mit unterschiedlichen Partnern jeweils andere EMAIL Absenderdaten zu verwenden. Darüber hinaus hat ein EMAIL Absenderpartner den Vorteil, dass dort alle Ihre absenderspezifischen AS2 Daten hinterlegt werden können und später einfach im Befehl SDNAS2 dieser Partner beim Parameter „Absender ID“ angegeben werden kann. Dies erspart die unnötige Wiederholung der Eingabe von gleich bleibenden Daten.

In das Menü zum Anlegen eines EMAIL Absenderpartners gelangen Sie, indem Sie im i-effect Hauptmenü den Menüpunkt „51“ auswählen. Im darauf folgenden Menü sehen Sie eine Liste der, falls schon Partner angelegt wurden, bereits vorhandenen Absenderpartner. Rufen Sie nun durch Drücken von F6 das Menü zum Anlegen eines Absenderpartners auf und geben diesem einen eindeutigen Namen sowie eine Beschreibung. Nach dem Drücken der Datenfreigabetaste sehen Sie wieder die Liste der Absenderpartner inklusive dem neu angelegten Partner. Gehen Sie nun mit Auswahl „2“ vor den neu erstellten Partner und blättern dann bis zu den EMAIL Einstellungen.

Sie erhalten folgende Anzeige:



SMTP Absender

Diese eMail-Adresse wird in der eMail als Absenderadresse eingetragen. Wird kein „SMTP Reply-to“ eingetragen und jemand antwortet auf eine von Ihnen gesendete eMail, so wird diese automatisch an die hier eingetragene Adresse adressiert.

SMTP Reply-to

Diese eMail-Adresse wird in der eMail als Rückantwortadresse eingetragen. Antwortet jemand auf Ihre eMail, so wird die Rückantwort automatisch an die hier hinterlegte Adresse adressiert.

SMTP Error-to

Im Fehlerfalle senden eMail-Server eine Benachrichtigung an die in diesem Feld angegebene Adresse. Ist diese Adresse nicht angegeben, so werden Fehlermeldungen an die im Feld „SMTP Absender“ oder „SMTP Reply-to“ angegebene Adresse gesendet.

SMTP Signatur Alias

Geben Sie in diesem Parameter an unter welchem Alias Ihr privater Schlüssel im Keystore eingetragen ist. Mit diesem privaten Schlüssel wird die eMail signiert. Es ist zwingend erforderlich, dass der hier eingetragene Aliasname identisch zu dem Aliasnamen ist, unter dem Ihr Schlüsselpaar im Keystore abgespeichert wurde.

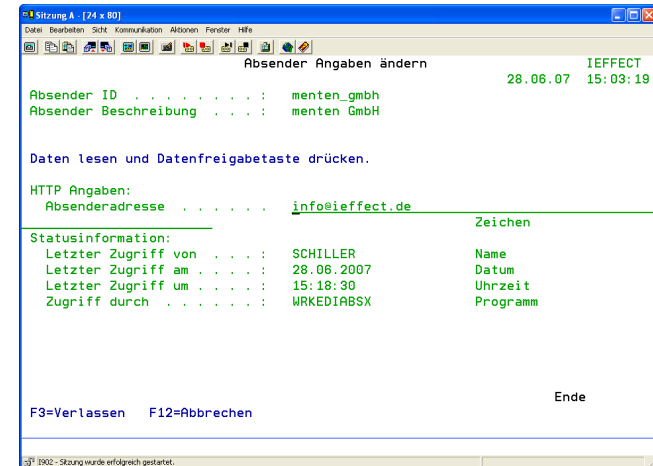
SMTP Signatur Algorithmus

In diesem Parameter wird festgelegt, mit welchem Algorithmus die *EMAIL Nachricht signiert wird. Dabei stehen folgende Werte zur Auswahl:

- *NONE Die eMail wird nicht signiert
- *MD5 Die eMail wird mit einer MD5 (Message Digest 5) Signatur versehen.
- *SHA1 Die eMail wird mit einer SHA1 (Secure Hash Algorithm 1) Signatur versehen.

Absenderangaben zum Modul *OFTP**SFID Absender**

Der SFID Absender (start file identification) gibt an, von welchem Partner die ursprüngliche Datei gesendet wurde. Dabei wird eine bis zu 25-stellige Odette-ID angegeben wie z.B.: O0013012345MENTEN01PC0001

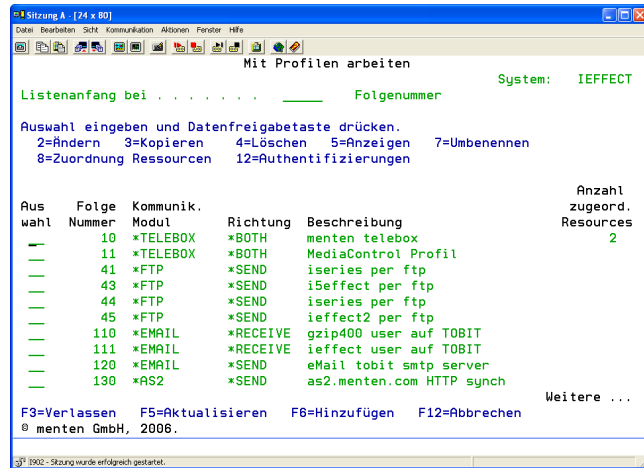
Absenderangaben zum Modul *HTTP**Absenderadresse**

Absender eMail-Adresse die in den HTTP-Header als Absenderadresse eingefügt wird.

Menüpunkt 52: Anlegen von Kommunikationsprofilen

Das Anlegen von Kommunikationsprofilen erfolgt über das Dialogprogramm „52“ (Mit EDI Kommunikationsressourcen arbeiten). Geben Sie hierzu die Auswahl „52“ im i-effect Hauptmenü ein.

Folgendes Dialogprogramm kommt zur Anzeige:



Zur Bearbeitung der Einträge stehen Ihnen folgende Auswahlmöglichkeiten zur Verfügung. Diese können in das entsprechende Auswahlfeld vor der gewünschten Zeile eingegeben werden. Die nachfolgende Übersicht stellt die zur Verfügung stehenden Grundfunktionen dieses Dialogprogramms vor. Eine detaillierte Beschreibung der einzelnen Auswahlmöglichkeiten schließt sich an diese Übersicht an.

Hinzufügen (Auswahl F6)

Mit der Auswahl F6 legen Sie eine neue Kommunikationsressource an. Im nachfolgenden Dialogprogramm haben Sie dann die Möglichkeit die Kommunikationsressourcen der installierten i-effect Module auszuwählen.

Ändern (Auswahl 2)

Geben Sie die Auswahl 2 in der Auswahlspalte der gewünschten Zeile ein, um diesen bestehenden Eintrag zu ändern. Es werden Ihnen die Daten der Kommunikationsressource angezeigt, die Sie hier bei Bedarf an neue Vorgaben anpassen können.

Kopieren (Auswahl 3)

Geben Sie die Auswahl 3 in der Auswahlspalte der gewünschten Zeile ein, um diesen bestehenden Eintrag auf einen neuen Eintrag zu übernehmen.

Löschen (Auswahl 4)

Geben Sie die Auswahl 4 in der Auswahlspalte der gewünschten Zeile ein, um diesen bestehenden Eintrag zu löschen.

Anzeigen (Auswahl 5)

Geben Sie die Auswahl 5 in der Auswahlspalte der gewünschten Zeile ein, um diesen bestehenden Eintrag anzeigen zu lassen.

Umbenennen (Auswahl 7)

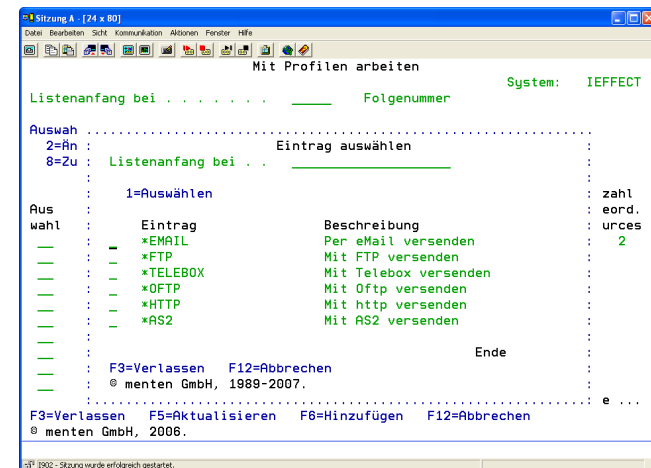
Geben Sie die Auswahl 7 in der Auswahlspalte der gewünschten Zeile ein, um diesen bestehenden Eintrag umbenennen.

Zuordnung Ressourcen (Auswahl 8)

Geben Sie die Auswahl 8 in der Auswahlspalte der gewünschten Zeile ein, um diesem bestehenden Eintrag eine Kommunikationsressource zuzuordnen.

Details zu: F6=Hinzufügen

Durch die Auswahl F6 erhalten Sie im nachfolgenden Dialogprogramm die Möglichkeit, eine Kommunikationsressource für eines der installierten i-effect Module anzulegen. Der unten abgebildete Bildschirm zeigt Ihnen die Auswahlmöglichkeiten die Ihnen zur Verfügung stehen, wenn alle Module von i-effect erfolgreich installiert wurden. Um einen Eintrag auszuwählen, tragen Sie bitte die Auswahlziffer "1" in die Spalte der gewünschten Zeile ein.



Anlegen von AS2 Kommunikationsprofilen

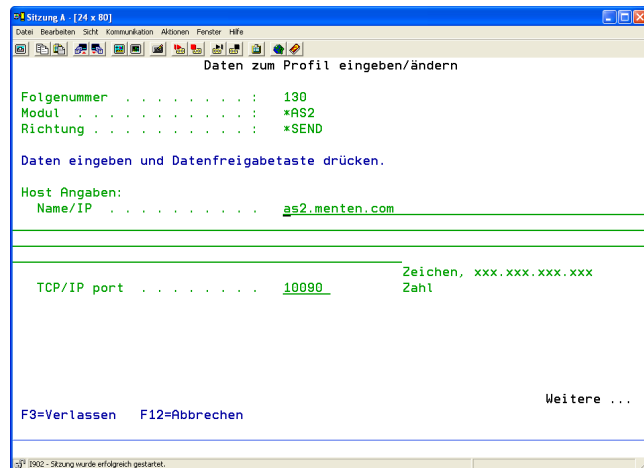
Anlegen eines *AS2-Sendeprofiles

Um AS2 Nachrichten an Ihre Partner versenden zu können, benötigen Sie für jeden Partner ein AS2 Sendeprofil. In diesen Profilen werden die sendespezifischen AS2 Einstellungen hinterlegt, die für die AS2 Kommunikation in Richtung Ihres Partners notwendig sind.

In das Menü zum Anlegen eines AS2 Sendeprofiles gelangen Sie, indem Sie im i-effect Hauptmenü den Menüpunkt „52“ auswählen. Im darauf folgenden Menü sehen Sie eine Liste der, falls schon Profile angelegt wurden, bereits vorhandenen Kommunikationsprofile.

Rufen Sie nun durch Drücken von F6 das Menü zum Anlegen eines Kommunikationsprofils auf und wählen anschließend mit Auswahl „1“ den AS2 Kommunikationsweg aus. Im darauf folgenden Menü wählen Sie bitte dann den Eintrag „*SEND“ aus.

Sie erhalten die folgende Anzeige:



Nun können Sie die benötigten Parameter konfigurieren:

Name/IP:

Geben Sie hier die IP Nummer oder den per DNS auflösbaren Hostnamen des AS2 Servers Ihres Kommunikationspartners an.

TCP/IP port:

Geben Sie hier die Portnummer des AS2 Servers Ihres Kommunikationspartners an.

Pfad für empfangene MDN

Geben Sie in diesem Parameter bei Bedarf ein anderes IFS Verzeichnis an, in dem die MDN-Dateien von erfolgreich empfangenen MDNs abgelegt werden.

Hinweis: In diesem Parameter dürfen ausschließlich IFS Verzeichnisse angegeben werden.

Pfad für gesendete Header

Der Standard IFS Pfad, in dem die Header Daten gesendeter AS2-Nachrichten abgelegt werden. Geben Sie in diesem Parameter bei Bedarf ein anderes IFS Verzeichnis an.

Hinweis: In diesem Parameter dürfen ausschließlich IFS Verzeichnisse angegeben werden.

AS2-TO (Empfängeridentifikation)

Tragen Sie hier die AS2 ID Ihres Kommunikationspartners ein. Diese ID ist für jeden Partner eindeutig und muss Ihnen von Ihrem Partner mitgeteilt werden. Häufig ist diese ID die GLN (Global Location Number) des Partners. Mittels der hier eingetragenen ID erfolgt in i-effect auch die eindeutige Zuordnung des Kommunikationspartner bei Empfang von AS2 Nachrichten dieses Partners.

AS2 Verschlüsselung Alias

Der Name benennt den Eintrag des Partnerzertifikats im Keystore. Das Zertifikat ist der öffentliche Schlüssel Ihres Kommunikationspartners und muss Ihnen von Ihrem Partner zugesendet werden. Hiermit wird die Nachricht digital verschlüsselt. Der Empfänger kann die Nachricht dann nur mit dem (seinem) passenden privaten Schlüssel wieder entschlüsseln. Wie Sie ein Zertifikat in den Keystore importieren, entnehmen Sie bitte Kapitel 12 „Graphische Zusatzanwendungen“.

AS2 Verschlüsselungsalgorithmus

Mit diesem Parameter kann angegeben werden, ob die AS2 Nachricht elektronisch verschlüsselt werden soll. Es stehen zwei Sonderwerte zur Auswahl:

*NONE Keine Verschlüsselung

Die AS2-Nachricht wird NICHT verschlüsselt.

***TRIPLEDES** 3DES Verschlüsselung

Der Data Encryption Standard (Abkürzung:DES) ist ein weit verbreiteter symmetrischer Verschlüsselungsalgorithmus. Die Schlüssellänge von 3DES ist mit 168 Bit drei mal so groß wie bei DES (56 Bit).

MDN erforderlich

Mit diesem Parameter geben Sie an, ob und wie eine MDN von Ihrem Partner angefordert werden soll. Häufig bekommen Sie Ihrem Partner mitgeteilt, welche Einstellung erwartet wird.

Es stehen drei Sonderwerte zur Auswahl:

- *SYNCH** Zeitgleich zum Versand der AS2-Nachricht wird eine MDN angefordert, die unmittelbar nach Übertragung der Nachricht eintreffen sollte. Sie wird vom Empfänger in der BESTEHENDEN Verbindung zurückgesendet.
- *ASYNCH** Es wird eine MDN angefordert, die jedoch zeitversetzt nach der AS2-Übertragung empfangen wird. Sie wird vom Empfänger in einer NEUEN Verbindung zurückgesendet.
- *NONE** Es wird keine MDN angefordert.

MDN Signatur

Der Parameter „MDN Signatur“ gibt an welchen Algorithmus der Empfänger der AS2-Nachricht benutzen muss, um die MDN zu signieren. Dabei gilt allerdings, wenn die versendete AS2-Nachricht mit dem Algorithmus SHA1 signiert ist, wird der Empfänger automatisch dazu gezwungen die MDN auch mit dem Algorithmus SHA1 zu signieren. Die Auswahl *MD5 in diesem Parameter wird in diesem Fall ignoriert. Nur wenn Sie eine AS2-Nachricht unsigniert versenden, greift die Auswahl dieses Parameters.

- *MD5** Die angeforderte MDN soll nach dem MD5-Algorithmus signiert sein.
- *SHA1** Die angeforderte MDN soll nach dem SHA1-Algorithmus signiert sein.

MDN Protokoll

Geben Sie in diesem Parameter an, über welches Protokoll eine asynchrone MDN an Sie zurückgesendet werden soll. Dieser Wert ist deshalb nur für asynchrone MDNs relevant, da bei synchronen MDNs die von Ihnen aufgebaute Verbindung und somit auch das zur Übertragung der AS2-Nachricht verwendete Protokoll benutzt wird.

Mögliche Sonderwerte sind:

- *SERVER** Dies ist der Standard.Die MDN wird an den in Ihrem System für den Empfang von asynchronen MND's definierten AS2 Server gesendet, Dieser Server muss vorher angelegt werden. Wie Sie eine AS2 Server anlegen, entnehmen Sie bitte dem Abschnitt „Anlegen eines AS2-Empfangsprofils“ in diesem Kapitel.

***SMTP**

Die MDN wird per SMPT (eMail) an die in Menü 80 eintragene „AS2 Absender Mailadresse“ zurückgesendet. Bitte beachten Sie, dass dieser Weg der MDN Übermittlung so gut wie nie verwendet wird.

Verbindungstimeout

Die hier angegebene Zeit wartet der AS2Client ab, um eine Verbindung zu einem entfernten Host (zum Server Ihres Partners) aufzubauen. Wenn nach der hier, in Sekunden, definierten Zeit der Verbindungsaufbau zu dem Server Ihres Partners nicht zustande kommt wird der Sendevorgang abgebrochen. Nach der in Parameter „Send Retry pause“ definierten Zeit erfolgt dann die Sendewiederholung.

Empfohlener Wert: 120 Sekunden.

Empfangstimeout

Nachdem die Verbindung zu dem Server Ihres Partners aufgebaut und die Daten übertragen wurden, wartet der AS2Client die hier definierte Zeit ab um ein OK (Http Statuscode 200) vom Server ihres Partners zu empfangen. Wenn das erforderliche OK nicht innerhalb der hier definierten Zeit empfangen wird, wird das *AS2 Modul einen Timeout-Fehler für die Übertragung melden. Leider lässt sich für die hier einzutragende Zeit keine Faustregel definieren. Lediglich Erfahrungswerte können Sie bei der Vergabe dieser Zeit mit einfließen lassen.

Empfohlener Wert: 120 Sekunden.

Content-Type

Hier können Sie die Art des Inhalts der AS2 Nachricht festlegen.

Es stehen folgende Sonderwerte zur Auswahl:

- *CONSENT** Die AS2-Nachricht enthält EDI Daten in keinem der nachfolgenden Formate (application/edi-consent).
- *EDIFACT** Die AS2-Nachricht enthält Daten im EDIFACT-Format (application/EDIFACT).
- *X12** Die AS2-Nachricht enthält Daten im X12-Format (application/EDI-X12).
- *XML** Die AS2-Nachricht enthält Daten im XML-Format (text/xml)..
- *BINARY** Die AS2-Nachricht enthält Binärdaten (application/octet-stream).
- *FRMFILE** Der Typ wird anhand der Dateieindung der Eingabedatei ermittelt. (.edi = application/EDIFACT). Bei *FRMFILE für DB2 Dateien ergibt sich als Content-Typ immer *BINARY (application/octet-stream), da in der DB2 keine Dateieendungen im herkömmlichen Sinn existieren.

Bodypart Typ

Hier können Sie festlegen, ob mit der AS2 Nachricht eine oder mehrere Dateien versendet werden.

Es stehen folgende Sonderwerte zur Auswahl:

<i>*SINGLE</i>	Der Standardwert. Mit der AS2-Übertragung wird eine Datei übermittelt.
<i>*MULTI</i>	Mit der AS2-Übertragung werden mehrere Dateien übermittelt.

Die Übertragung von mehreren Dateien wird in der aktuellen AS2 Version nicht unterstützt. Verwenden Sie bitte daher hier immer den Wert **SINGLE*.

Proxy Server

Wenn Sie einen Proxy Server für die AS2 Kommunikation einsetzen möchten, können Sie hier die zu verwendenden Parameter hinterlegen.

Folgende Parameter stehen zur Auswahl:

<i>Host name/IP</i>	Geben Sie hier die IP-Adresse oder DNS-Namen an.
<i>TCP/IP Port</i>	Geben Sie hier den TCP/IP-Port an.
<i>Benutzername</i>	Geben Sie (falls erforderlich) hier einen autorisierten Benutzer dafür an.
<i>Kennwort</i>	Geben Sie (falls erforderlich) hier das Passwort des zuvor angegebenen autorisierten Benutzers dafür an.

SSL

Dieser Parameter steuert das zu verwendene Protokoll. Geben Sie hier an, ob die AS2-Kommunikation über SSL/HTTPS (Secure Socket Layer) oder über normales HTTP erfolgen soll.

<i>*YES</i>	Ja, die Verbindung erfolgt über SSL/HTTPS
<i>*NO</i>	Nein, die Verbindung erfolgt über standard HTTP

Import nicht vertrauenswürdiger Zertifikate

Tragen Sie in diesem Parameter den Wert **YES* ein um bei Verbindungen über https (SSL/TLS) die Server Zertifikate, die nicht in Ihrem Keystore vorhanden sind, automatisch zu importieren. Jedoch sollten Sie sich in diesem Fall darüber bewusst sein, dass Sie automatisch auch jedem Server, zu dem Sie eine Verbindung über https aufbauen und dessen Zertifikat NICHT in Ihrem Keystore enthalten ist, Ihr Vertrauen schenken.

Ist dieser Parameter mit dem Wert **NO* gesetzt und das Zertifikat von dem Server zu dem Sie versuchen eine Verbindung aufzubauen nicht in Ihrem Keystore enthalten, so wird die Verbindung automatisch geschlossen. Der Verbindungsabbruch ist in diesem Falle korrekt, da das Zertifikat nicht in Ihrem Keystore enthalten ist und somit die Identität des Servers nicht geprüft werden kann.

<i>*YES</i>	Ja, nicht vertrauenswürdige Zertifikate werden automatisch importiert.
<i>*NO</i>	Nein, nicht vertrauenswürdige Zertifikate werden nicht automatisch importiert.

Client Authentifizierung verwenden

Bei der Auswahl **YES* für den Parameter „SSL“ können Sie in diesem Parameter angeben ob sich der AS2 Client beim Verbindungsaufbau zum Server Ihres Partners mit Ihrem X509 Zertifikat authentifizieren muss. Nur wenn diese Prüfung des vom Client gesendeten Zertifikates gegen das Zertifikat im Keystore des Servers erfolgreich ist, akzeptiert der AS2 Server Ihres Partners die eingehende Verbindung. Andernfalls schließt er die vom Client aufgebaute Verbindung, da nicht sichergestellt ist, dass Sie wirklich ein autorisierter Partner sind, der versucht eine AS2-Nachricht an den Server zu senden.

Sie sollten von Ihrem Partner explizit mitgeteilt bekommen, wenn diese Form der SSL Authentifizierung verlangt wird,

<i>*AUTO</i>	Die Standardeinstellung. Beim Verbindungsaufbau (SSL Handshake) wird automatisch ermittelt ob Client Authentifizierung vom Server verlangt wird. Ist dies der Fall, so wird versucht das passende Zertifikat zum Server zu übermitteln.
<i>*YES</i>	Ja, es wird Client Authentifizierung verlangt. Der Verbindungsaufbau wird explizit mit dieser Einstellung durchgeführt. Bei Servern die dies nicht verlangen, führt dies zum Fehler und dem Abbruch der Verbindung.

Bitte beachten Sie, dass diese Form der SSL Authentifizierung nicht von sehr vielen Servern verlangt wird und im Internet im allgemeinen nicht üblich ist.

SSL Verbindungszertifikat

Wenn Sie den Wert **YES* beim Parameter „SSL Client Authentifizierung“ verwenden, können Sie hier den Namen des Schlüsselpaars im Keystore eintragen, der Ihren öffentlichen Schlüssel (das Zertifikat) für die Authentifizierung enthält. Diese Zertifikat wird beim Senden der AS2 Nachricht an den Server übermittelt. Es muss sich natürlich vor Verbindungsaufbau im Keystore des AS2 Servers Ihres Partners befinden.

Beschreibung

Bei Bedarf können Sie hier eine Kurzbeschreibung des angelegten AS2 Sendeprofiles angeben. Der hier eingetragene Text besitzt rein informellen Charakter und ist somit frei wählbar.

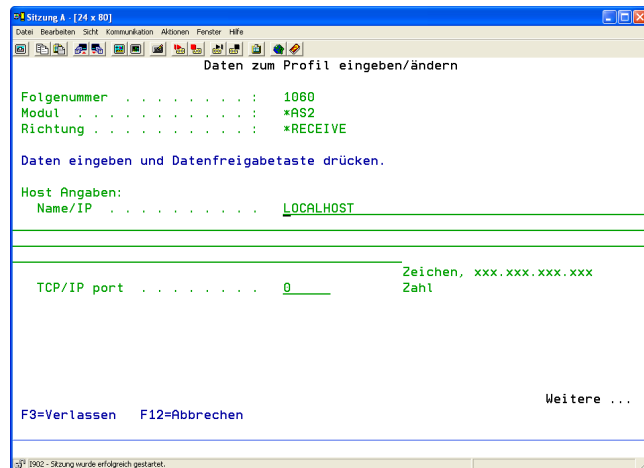
Anlegen eines AS2-Empfangsprofils (AS2 Server)

Um AS2 Nachrichten und MDNs von Ihren Partner empfangen zu können, müssen Sie einen AS2 Server anlegen. Sie können mehrere AS2 Server Instanzen im System anlegen. Jeder AS2 Server der von Ihnen angelegt wird, muss allerdings auf einer noch nicht verwendeten Adresse/Port gesetzt werden. So ist es beispielsweise möglich, für jeden Ihrer Partner einen AS2 Server anzulegen. Der AS2 Server wartet auf einer von Ihnen definierten Adresse/Port auf eingehende AS2-Nachrichten. Weiterhin müssen Sie, wenn Sie AS2-Nachrichten mit asynchroner MDN Anforderung versenden wollen, einen dieser AS2 Server als Empfangsserver für die asynchron angeforderten MDNs definieren. In der Parameterbeschreibung „Asynch MDN server?“ finden Sie dazu weiterführende Informationen.

In das Menü zum Anlegen eines AS2 Empfangsprofils gelangen Sie, indem Sie im i-effect Hauptmenü den Menüpunkt 52 auswählen. Im darauf folgenden Menü sehen Sie eine Liste der, falls schon Profile angelegt wurden, bereits vorhandenen Kommunikationsprofile.

Rufen Sie nun durch Drücken von F6 das Menü zum Anlegen eines Kommunikationsprofils auf und wählen anschließend mit Auswahl 1 den AS2 Kommunikationsweg aus. Im darauf folgenden Menü wählen Sie bitte dann den Eintrag „*RECEIVE“ aus.

Sie erhalten die folgende Anzeige:



Nun können Sie die benötigten Parameter konfigurieren:

Name/IP

Der Hostname/die IP-Adresse an den der AS2 Server gebunden wird.

TCP/IP port

Der Port auf dem der AS2 Server auf eingehende Verbindungen wartet.

Pfad für empfangene Daten

Hier können Sie ein IFS Verzeichnis für die Speicherung der empfangenen Daten angeben.

Dieser Parameter wird in einer der nächsten Versionen entfallen. Da bei AS2 immer partnerbezogen empfangen wird, ist die Angabe eines „allgemeinen“ Empfangspfades überflüssig.

Pfad für empfangene Header

Geben Sie in diesem Parameter bei Bedarf ein anderes IFS Verzeichnis an, indem die Header-Dateien von erfolgreich empfangenen AS2 Nachrichten abgelegt werden.

Hinweis: In diesem Parameter dürfen ausschließlich IFS Verzeichnisse angegeben werden.

Pfad für empfangene MDN

Geben Sie in diesem Parameter bei Bedarf ein anderes IFS Verzeichnis an, in dem die erfolgreich empfangenen MDNs abgelegt werden.

Hinweis: In diesem Parameter dürfen ausschließlich IFS Verzeichnisse angegeben werden.

Pfad für gesendete MDN

Geben Sie in diesem Parameter bei Bedarf ein anderes IFS Verzeichnis an, indem die erfolgreich gesendeten MDNs abgelegt werden.

Hinweis: In diesem Parameter dürfen ausschließlich IFS Verzeichnisse angegeben werden.

Pfad für offene MDN (asynchron)

Geben Sie in diesem Parameter bei Bedarf ein anderes IFS Verzeichnis an, in dem empfangene AS2 Nachrichten mit asynchroner MDN Anforderung temporär abgelegt werden, bis die angeforderte MDN erfolgreich übertragen werden konnte.

Hinweis: In diesem Parameter dürfen ausschließlich IFS Verzeichnisse angegeben werden.

Async MDN Server

AS2 bietet Ihnen die Möglichkeit, Empfangsbestätigungen für Ihre versendeten AS2-Nachrichten anzufordern. Die Empfangsbestätigungen, sogenannte MDNs (Message Disposition Notification) können synchron oder asynchron angefordert werden.

Synchron heißt bei AS2: Die von Ihnen angeforderte MDN muss über die zu Ihrem Partner aufgebaute Verbindung zurückgesendet werden. Findet die Übertragung einer synchron angeforderten MDN nicht über die von Ihnen aufgebaute Verbindung statt, wird der Sendevorgang als nicht erfolgreich beendet, auch wenn das Senden der AS2-Nachricht erfolgreich abgeschlossen wurde. Dies ist notwendig, da durch das Ausbleiben der MDN nicht sicher gestellt werden kann, ob die gesendete AS2-Nachricht wirklich von Ihrem Partner empfangen und erfolgreich verarbeitet wurde. Dieser Sachverhalt kann u.U. beim Versand großer Datenmengen mit synchroner MDN Anfrage auftreten, da das Zielsystem die Daten nicht in der im AS2 Sendeprofil als „Empfangstimeout“ definierten Zeit verarbeiten kann. Der AS2 Client bricht dann die aufgebaute Verbindung ab, bevor die MDN von Ihrem Partner an Sie übertragen werden konnte. Um solche Situationen beim Versand großer Datenmengen präventiv zu vermeiden, können Sie für diese AS2-Nachrichten auch eine asynchrone MDN anfordern. Allerdings sollten Sie vorher mit Ihren Partnern absprechen, ob deren AS2 Systeme in der Lage sind, asynchron angeforderte MDNs zu versenden.

Asynchron bedeutet im AS2 System: Die Verbindung wird geschlossen, nachdem die AS2-Nachricht an Ihren Partner übertragen wurde. Nachdem die Verarbeitung auf dem Empfangssystem abgeschlossen ist, baut Ihr Partner eine neue Verbindung zu Ihnen auf, um über diese die angeforderte MDN zu versenden. Gerade bei großen Datenmengen ist diese Option sehr hilfreich, da die Verarbeitung von großen Datenmengen sehr schnell den eingestellten Empfangstimeout auf der Sendeseite übersteigt. Leider kann schlecht angegeben werden, ab welcher Datengröße es sinnvoll ist, eine asynchrone MDN anzufordern, da viele Faktoren (Verarbeitungszeit auf dem Zielsystem, Länge des Übertragungsweges etc) auf diesen Prozess einwirken. Um asynchrone MDN's für Ihre versendeten AS2-Nachrichten empfangen zu können, müssen Sie einen der angelegten AS2 Server als den Empfangsserver für asynchron zurückgesendete MDNs definieren. Wenn Sie nur einen AS2 Server angelegt haben, sollte dieser gleichzeitig auch durch Setzen der Auswahl *YES in diesem Parameter als MDN Empfangsserver definiert werden, damit Sie die Möglichkeit haben asynchrone MDNs über diesen Server zu empfangen.

*YES Dieser AS2 Server empfängt alle asynchronen MDNs, die von Ihren Partnern an Sie zurückgesendet werden.

*NO Dieser AS2 Server soll keine asynchron zurückgesendete MDN's empfangen. (Standard)

In der aktuellen AS2 Version besteht nur die Möglichkeit EINEN Server für den Empfang von asynchronen MDN's zu definieren. Mehrere MDN Server im System sind nicht möglich

Maximale Server Threads

Mit Hilfe dieses Parameters geben Sie an, wie viele Verbindungen der AS2 Server maximal gleichzeitig verarbeiten soll. Ist diese Anzahl der gleichzeitigen Verbindungen erreicht, werden die anstehenden Verbindungen in eine Warteschlange gestellt und verarbeitet, sobald eine freie Verbindung verfügbar ist.

Empfangstimeout

Geben Sie in diesem Parameter die Zeit (in Sekunden) an, die der AS2 Server maximal auf Daten einer eingegangenen Verbindung warten soll. Ist diese Zeit abgelaufen, wird ein Timeout-Fehler gemeldet und die Verbindung wird abgebrochen.

Scan-Intervall offene MDN

In dem im Parameter „Pfad für offene MDN (asynchron)“ angegebenen IFS-Verzeichnis werden die empfangenen AS2 Nachrichten mit asynchroner MDN Anforderung, nachdem Sie entschlüsselt und verifiziert worden sind, als AS2-Objektdatei (.as2) abgelegt. Somit muss dieses Verzeichnis in regelmäßigen Zeitintervallen auf neue AS2-Objektdateien geprüft werden, um für diese empfangenen AS2-Nachrichten die MDN's zurückzusenden. Die Zeit für dieses Intervall, in Sekunden, können Sie in diesem Parameter angeben.

MDN.Anz.Sendewiederholungen

Geben Sie in diesem Parameter an, wieviele Versuche maximal unternommen werden sollen, um eine asynchron angeforderte MDN zurückzusenden.

Externe IP, DNS-Name

In diesem Parameter geben Sie die URL/IP für asynchron angeforderte MDNs an. Diese Adresse wird dem Partnersystem beim Senden einer AS2 Nachricht mit asynchroner MDN Anforderung mit übermittelt. An diese Adresse sendet Ihre Partner dann die angeforderten MDN. Bei Übertragung via HTTP/HTTPS ist dies der externe DNS-Name bzw. die externe IP-Adresse Ihres AS2 Servers, Diese Adresse muss von außen erreichbar sein.

Externer TCP/IP port

Geben Sie hier den externen TCP/IP Port des AS2 Servers an. Auf diesem Port werden die MDN's von Ihrem AS2 Server entgegengenommen. Dieser Port muss von außen erreichbar sein.

SSL

Dieser Parameter steuert das vom AS2 Server zu verwendene Protokoll, welches der AS2 Server verwenden soll. Als Auswahlmöglichkeiten stehen Ihnen *YES und *NO zur Verfügung. Bei der Auswahl *NO verwendet der AS2 Server das HTTP-Protokoll und ist somit über "normale" HTTP-Verbindungen erreichbar. Durch Setzen des Wertes *YES geben Sie an, dass der AS2 Server SSL (TLS) verwenden soll und somit nur über HTTPS-Verbindungen erreichbar ist. Bei Verwendung von *YES können Sie in den drei folgenden Parametern "Client Auth. erforderlich?"; "Import nicht vertrauter Zertifikate" sowie „SSL Verbindungszertifikat“ das Verhalten des AS2 Servers weiter spezifizieren.

- *NO Der AS2 Server verwendet das HTTP-Protokoll (Standard).
- *YES Der AS2 Server verwendet das HTTPS-Protokoll.

Import nicht vertrauenswürdiger Zertifikate

Bei der Auswahl *YES im Parameter „SSL“ haben Sie mittels des hier eingetragenen Wertes die Möglichkeit anzugeben, ob Client Zertifikate, die NICHT in Ihrem Keystore enthalten sind, automatisch vom AS2 Server in Ihren Keystore importiert werden sollen. Dies erreichen Sie, indem Sie in diesem Parameter den Wert *YES eingeben. Allerdings stellt der Wert *YES für diesen Parameter auch ein gewisses Sicherheitsrisiko dar. Durch die automatische Importierung des vom Clients beim Verbindungsaufbau gesendeten Zertifikates in den Keystore, wird jeder Client als vertrauenswürdig eingestuft. Ist dieser Parameter mit dem Wert *NO gesetzt und das Zertifikat beim Aufbau einer Verbindung nicht in Ihrem Keystore enthalten, so wird die Verbindung automatisch geschlossen. Der Verbindungsabbruch ist in diesem Falle korrekt, da das Zertifikat nicht in Ihrem Keystore enthalten ist und somit die Identität des Clients nicht sichergestellt werden kann.

Die automatische Importierung in den Keystore greift jedoch nur, wenn der Parameter „Client Auth. erforderlich?“ mit dem Wert *YES gesetzt ist.

- *YES Ja, unbekannte Client Zertifikate werden automatisch importiert.
- *NO Nein, unbekannte Client Zertifikate werden NICHT automatisch importiert.

Client Authentifizierung erforderlich

Bei der Auswahl *YES für den Parameter „SSL“ können Sie in diesem Parameter angeben ob der Client, der eine AS2 Nachricht an Sie sendet, sich gegenüber (Ihrem) AS2 Server mit seinem X509 Zertifikat authentifizieren muss.

Wenn Sie hier die Auswahl *YES treffen und im vorhergehenden Parameter „Import nicht vertrauter Zertifikate“ den Wert *NO angeben, muss das Zertifikat Ihres Partners schon vor dem Verbindungsaufbau in Ihrem Keystore vorhanden sein. Somit ist gewährleistet, dass das über die aufgebaute HTTPS-Verbindung automatisch gesendete Zertifikat Ihres Partners, vom AS2 Server geprüft werden kann. Nur wenn diese Prüfung des vom Client gesendeten Zertifikates gegen das Zertifikat aus Ihrem Keystore erfolgreich ist, akzeptiert der AS2 Server die eingehende Verbindung. Andernfalls schließt er die vom Client aufgebaute Verbindung, da nicht sichergestellt ist, dass es wirklich Ihr Partner ist, der versucht eine AS2-Nachricht an sie zu senden. Geben Sie in diesem Parameter den Wert *NO an, findet die Prüfung des Zertifikats während des Verbindungsaufbaus nicht statt.

- *YES Ja, es wird Client Authentifizierung verlangt.
- *NO Nein, es wird keine Client Authentifizierung verlangt.

Bitte beachten Sie, dass diese Form der SSL Authentifizierung nicht von sehr vielen Clients unterstützt wird und im Internet im allgemeinen nicht üblich ist.

SSL Verbindungszertifikat

Hier können Sie den Namen des Schlüsselpaares im Keystore eintragen, der Ihren öffentlichen Schlüssel (das Zertifikat) enthält. Dieses Zertifikat wird an jeden Client der eine SSL Verbindung zu Ihrem AS2 Server aufbaut übermittelt. Hiermit authentifiziert sich Ihr Server gegenüber dem Client. Diese Zertifikat sollte sich natürlich vor Verbindungsaufbau im Keystore des Clients Ihres Partners befinden.

Diese Form der HTTPS Authentifizierung ist das Standardverfahren im Internet.

Beschreibung

In diesem Parameter können Sie eine Kurzbeschreibung für den angelegten AS2 Server angeben. Diese Beschreibung hat rein informellen Charakter und kann somit von Ihnen frei gewählt werden.

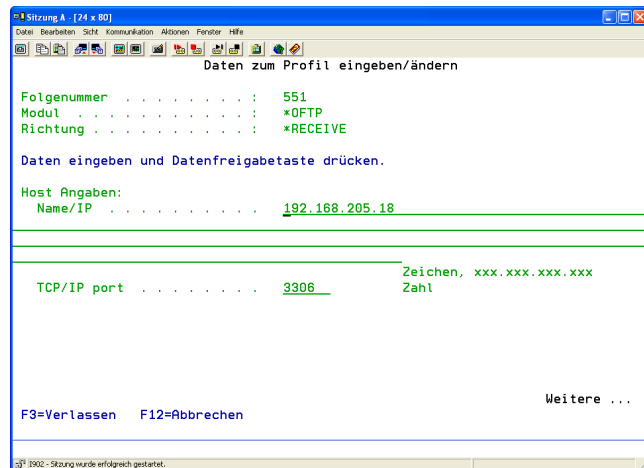
Anlegen von OFTP Kommunikationsprofilen

Anlegen eines *OFTP Empfangsprofils (OFTP-Server)

In das Menü zum Anlegen eines OFTP Empfangsprofils gelangen Sie, indem Sie im i-effect Hauptmenü den Menüpunkt „52“ auswählen.

Rufen Sie nun durch Drücken von F6 das Menü zum Anlegen eines Kommunikationsprofils auf und wählen anschließend mit Auswahl „1“ den OFTP Kommunikationsweg aus. Im darauffolgenden Menü wählen Sie bitte dann den Eintrag „*RECEIVE“ aus.

Nun können Sie die benötigten Parameter konfigurieren:



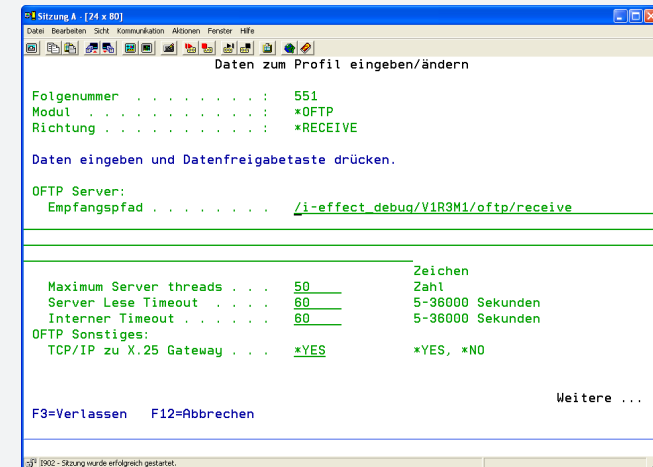
Host Angaben:

Name/IP:

Geben Sie hier bitte den Host-Namen oder die IP-Adresse an, unter der Ihr Server erreichbar sein soll. Beachten Sie dabei, dass diese Parameter mit Ihren „System i“-Einstellungen bzw. denen ihres Netzwerkes übereinstimmen (siehe WRKTCPS -> Auswahl 1). Sollten Sie sich nicht sicher sein, so kontaktieren Sie bitte Ihren Systemadministrator.

TCP/IP port:

Geben Sie hier die Portnummer an, unter der Ihr Server erreichbar sein soll. Der Standard OFTP port ist 3305, aber prinzipiell ist er frei wählbar (>1023). Er sollte jedoch nicht im Konflikt mit anderen Programmen stehen, die auf einem Port lauschen. Dies können Sie mittels WRKTCPS -> Auswahl 3 -> F14 (Port Adressen anzeigen) überprüfen. Sollten Sie sich nicht sicher sein, so kontaktieren Sie bitte Ihren Systemadministrator.



OFTP Server:

Empfangspfad:

Hier können Sie den Standard-Empfangspfad für empfangene Dateien angeben. Um die Performance zu verbessern, empfehlen wir Ihnen einen IFS-Pfad anzugeben, da das primäre Ablegen von empfangenen Daten in DB2-Pfade mehr Rechenleistung erfordert. Wenn Sie für Ihre Kommunikationspartner Profile angelegt haben, werden die hier empfangenen Daten in die für den Partner konfigurierten Empfangsverzeichnisse übertragen.

Maximum Server threads:

Mit dieser Einstellung legen Sie fest, wie viele gleichzeitige OFTP-Server-Instanzen erstellt werden dürfen. Wird dieser Wert erreicht, so werden weitere OFTP-Verbindungen nicht angenommen. Ein typischer Wert für die maximale Anzahl ist 50.

Server Lese Timeout:

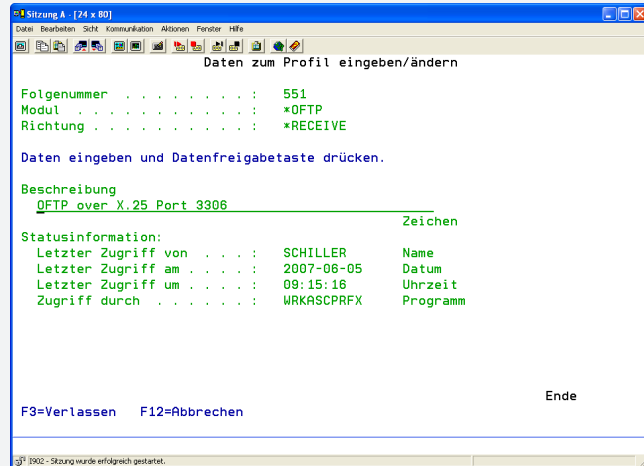
Legt die Zeit in Sekunden fest, nach denen die Verbindung als gescheitert betrachtet wird. Entsteht während einer Verbindung eine Leerlaufzeit, die diese Zeit übersteigt, so wird die Verbindung abgebrochen.

Interner Timeout:

Diese Zeit bestimmt, wann eine Serverinstanz für nicht mehr reaktionsfähig erklärt wird, etwa weil es bei einem Speichervorgang zu lange dauert, eine Datei zu bearbeiten.

OFTP Sonstiges:**TCP/IP zu X.25 Gateway:**

Wenn Sie nicht über TCP/IP mit dem OFTP Server kommunizieren, sondern, sondern über einen Bintec Router zu X.25 Netzen eine Verbindung aufbauen, so müssen Sie hier den Wert „*YES“ eintragen (siehe auch Konfiguration Bintec Router). Andernfalls belassen Sie diesen Parameter auf „*NO“; wenn Sie per TCP/IP kommunizieren.

**Beschreibung**

Hier können Sie eine Beschreibung der Serverinstanz angeben. Hilfreich ist es hier in Kurzform anzugeben auf welche IP/Hostname Port Kombination der Server lauscht. Z. B.: OFTPMENTEN.DE:3305

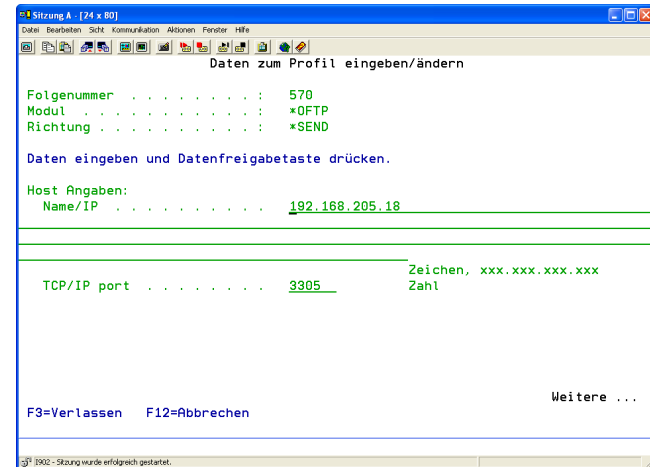
Nachdem Sie nun einen Server-Eintrag angelegt haben, können Sie für Ihre Partner Benutzer-Authentifizierungen hinterlegen.

Anlegen eines *OFTP Sendeprofiles

In das Menü zum Anlegen eines OFTP Empfangsprozils gelangen Sie, indem Sie im i-effect Hauptmenü den Menüpunkt „52“ auswählen.

Rufen Sie nun durch Drücken von F6 das Menü zum Anlegen eines Kommunikationsprozils auf und wählen anschließend mit Auswahl „1“ den OFTP Kommunikationsweg aus. Im darauffolgenden Menü wählen Sie bitte dann den Eintrag „*SEND“ aus.

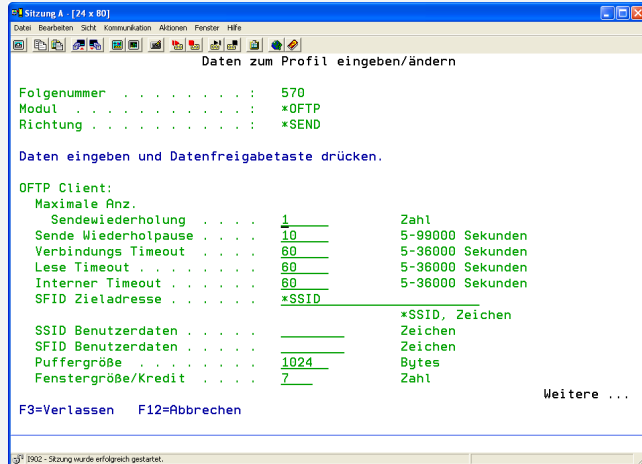
Nun können Sie die benötigten Parameter konfigurieren:

**Host Angaben:****Name/IP:**

Geben Sie hier die IP Nummer oder den per DNS auflösbaren Hostnamen des Servers Ihres Kommunikationspartners an.

TCP/IP port:

Geben Sie hier die Portnummer des Servers Ihres Kommunikationspartners an. Der Standardport für das OFTP Protokoll ist 3305. Er kann jedoch auch davon abweichen. Dieser Parameter ist dann bei Ihrem Kommunikationspartner zu erfragen.



OFTP Client:

Maximale Anz. Sendewiederholungen:

Hier legen Sie fest, wie oft nach einem gescheiterten Verbindungsversuch ein erneuter Versuch gestartet wird.

Sende Wiederholpause

Hier bestimmen Sie die Pause in Sekunden, die zwischen 2 Versuchen gewartet wird.

Verbindungs Timeout

Timeout in Sekunden für den Aufbau einer Verbindung.

Lese Timeout

Timeout in Sekunden für das Lesen von Daten auf einer offenen Datenverbindung.

Interner Timeout

Dieser Parameter definiert den internen Verarbeitungstimeout des *OFTP-Clients. Die hier angegebene Zeit (in Sekunden) wartet der *OFTP-Client beispielsweise bei Verarbeitungsengpässen ab, um die vom System / User delegierten Aufgaben (Vorbereiten / Senden OFTP-Daten) zu verarbeiten.

SFID Zieladresse

OdetteID des Empfängers. Diese ist in der Regel identisch mit der OdetteID des Partner. Sie kann jedoch von dieser abweichen, wenn die Daten über ein OFTP-Gateway übertragen werden.

SSID Benutzerdaten

Dieser Parameter wird in der Regel nicht benötigt, außer wenn dies bilateral zwischen den Partnern vereinbart wurde.

SFID Benutzerdaten

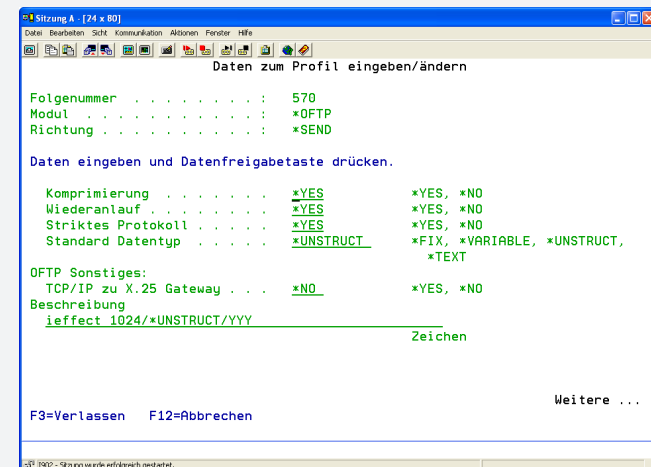
Dieser Parameter wird in der Regel nicht benötigt, außer wenn dies bilateral zwischen den Partnern vereinbart wurde.

Puffergröße

Maximale Größe des Puffers der bei der Datenübertragung verwendet wird. Bei einer TCP/IP-Verbindung ist hier eine Größe von 2048 oder 4096 ein normaler Wert. Bei Verbindungen mit „X.25 über ISDN“ sollte er mit 256 bis maximal 512 festgelegt werden.

Fenstergröße/Kredit

Dieser Parameter bestimmt nach wie vielen Datenpaketen der Sendekredit verbraucht ist und wieder aufgefrischt werden muss. Dieser Parameter ist vergleichbar der in TCP gebräuchlichen „Window size“. 7 ist ein üblicher Wert.



Komprimierung

Legt fest, ob eine einfache Kompression auf Dateien des Formats *TEXT (siehe „Fix, Variable, Unstr., Text“) angewandt werden soll. Dies muss jedoch auch von der Gegenstelle unterstützt werden.

Wiederanlauf

Falls während einer vorhergehenden Datenübertragung die Übertragung unterbrochen wurde, so kann versucht werden die Übertragung der Datei fortzusetzen. Dies muss jedoch auch von der Gegenstelle unterstützt werden.

Striktes Protokoll

Bestimmt, ob die Datenübertragung ohne Abweichungen zu dem Standardprotokoll erfolgt. Eine Änderung auf *NO kann notwendig sein, wenn auf der Gegenseite ein ODEX-System eingesetzt wird, oder es bei einem Partner regelmäßig zu Protokollfehlern kommt.

Standard Datentyp

Bei der Übertragung von Daten mittels *OFTP ist es möglich, diese in einer von 4 verschiedenen Übertragungsarten zu senden/empfangen: *FIX, *VARIABLE, *TEXT und *UNSTRUCT. Dies bedeutet im einzelnen folgendes:

<i>*UNSTRUCT</i>	Die Daten werden so wie sie sind – also als binäre Datei – versendet. Es findet keinerlei Konvertierung statt.
<i>*TEXT</i>	Die Datei wird vor dem Senden in die partnerspezifische CCSID konvertiert. Befindet sich die zu übertragende Datei in der Datenbank, so wird jeweils am Ende eines Datenbank-Records ein Zeilenumbruch (CR LF) eingefügt.
<i>*FIX</i>	Die Daten werden vor dem Senden in Sätze gleicher Länge aufgeteilt – nötigenfalls mit Leerzeichen aufgefüllt – und in die partnerspezifische CCSID konvertiert.
<i>*VARIABLE</i>	Es wird vor dem Senden der Daten der längste Datensatz ermittelt und es findet eine Konvertierung in die partnerspezifische CCSID statt. Eine Auffüllung der Datensätze mit Leerzeichen findet nicht statt.

OFTP Sonstiges:**TCP/IP zu X.25 Gateway**

Legt fest, ob die OFTP Verbindung über ein TCP/X.25 Gateway aufgebaut wird, oder ob es sich um eine native TCP/IP Verbindung handelt. Bei einer Gateway/X.25 Lösung wird ein X.25 fähiger Router via TCP/IP an das lokale Netz angeschlossen und leitet die OFTP Übertragungsanforderung an ein natives X.25 oder an ein ISDN Netzwerk weiter (X.25 via ISDN B-Kanal).

Folgende Optionen stehen zur Auswahl:

<i>*YES</i>	Es wird ein TCP/IP to X.25 gateway verwendet.
<i>*NO</i>	Es wird eine direkte TCP/IP Verbindung verwendet.

Beschreibung

Hier können Sie eine Beschreibung des Sendeprofiles angeben. Hilfreich ist es hier in Kurzform anzugeben über welche IP/Hostname Port Kombination oder eventuell X.25 Adresse eine Verbindung zum Partner aufgebaut wird. Z. B. OFTPMENTEN.DE:3305

Nachdem Sie einen Partner-Eintrag angelegt haben, können Sie mit Auswahl "12" vor einem Partner-Eintrag Authentifizierungs-Informationen hinterlegen.

Anlegen von FTP Kommunikationsprofilen

Anlegen eines FTP Sende/Empfangsprofils

Im Partnerstamm Menü „52“ des i-effect Hauptmenüs können Sie durch Drücken von F6 und dann Auswahl 1 vor *FTP ein Kommunikationsprofil anlegen, welches für die Sende- und Empfangsrichtung verwendet werden kann (Richtung *BOTH).

Nun können Sie die benötigten Parameter konfigurieren:

Screenshot of the i-effect software interface showing the 'Daten zum Profil eingeben/ändern' dialog box. The dialog contains the following fields and values:

- Folgenummer: 410
- Modul: *FTP
- Richtung: *BOTH
- Host Angaben: Name/IP: i5effect
- TCP/IP port: 21
- Benutzername: QSECOFR
- Kennwort: xxxxxxxx

Additional text in the dialog includes: 'Daten eingeben und Datenfreigabetaste drücken.', 'F3=Verlassen F12=Abbrechen', and 'Weitere ...'.

Host Angaben

Name/IP

Geben Sie hier die IP Nummer oder den per DNS auflösbaren Hostnamen des FTP Servers Ihres Kommunikationspartners an.

TCP/IP port

Geben Sie hier die Portnummer des FTP Servers Ihres Kommunikationspartners an. Der Standardport für das FTP Protokoll ist 21

Benutzer Angaben

Benutzername

Der Benutzername, der zur Anmeldung am FTP Server verwendet wird.

Kennwort

Das Kennwort zur Anmeldung für den angegebenen Benutzer.

FTP Angaben

Std. Übertragungsart

Die Art der Übertragung, die normalerweise mit diesem FTP-Server vorgenommen wird. Diese Voreinstellung lässt sich per jeder einzelnen Übertragung überschreiben.

Folgende Werte stehen zur Auswahl:

- *ASCII Diese Einstellung wird beim Austausch von Daten von und zu ASCII Maschinen benötigt, die keine EBCDIC Darstellung unterstützen.
- *EBCDIC Diese Einstellung wird beim Austausch von Daten von und zu EBCDIC Maschinen benötigt. Hiermit wird eine unnötige Übersetzung zwischen ASCII und EBCDIC auf beiden Maschinen vermieden.
- *BINARY Zum Austausch von Binärdaten (z.B. SaveFiles) wird diese Einstellung gewählt. Die Daten werden einzu-eins übertragen.

Std. Modus

Geben Sie hier ein, welcher FTP-Modus standardmäßig verwendet werden soll.

Mögliche Sonderwerte:

- *ACTIVE Der FTP Modus „ACTIVE“ wird verwendet.
- *PASSIVE Der FTP Modus „PASSIVE“ wird verwendet.

Beschreibung

In diesem Parameter können Sie eine Kurzbeschreibung für das angelegte FTP Profil angeben. Diese Beschreibung hat rein informellen Charakter und kann somit von Ihnen frei gewählt werden.

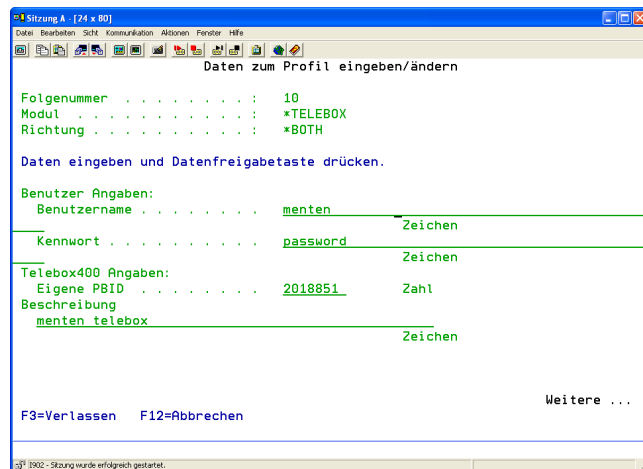
Anlegen von TELEBOX Kommunikationsprofilen

In Abschnitt „Menüpunkt 53 EDI- Kommunikationsressourcen“ in diesem Kapitel wird erklärt, wie Sie die Telebox-Hardwareressource in i-effect konfigurieren können. Diese Ressource können Sie dann einem Telebox-Kommunikationsprofil (*RECEIVE oder *SEND) zuweisen.

Anlegen eines TELEBOX Sende/Empfangprofils

Im Partnerstamm Menü „52“ des i-effect Hauptmenüs können Sie durch Drücken von F6 und dann Auswahl 1 vor *TELEBOX ein Kommunikationsprofil anlegen, welches für die Sende- und Empfangsrichtung verwendet werden kann (Richtung *BOTH).

Nun können Sie die benötigten Parameter konfigurieren:



Benutzer Angaben

Benutzername

Der Benutzername, der zur Anmeldung an der X.400 Telebox verwendet wird.

Kennwort

Das Kennwort zur Anmeldung für den angegebenen Benutzer.

Telebox Angaben

Eigene PBID

Die persönliche Identifikation PBID (personal box ID) für dieses Profil auf dem Telebox System.

Beschreibung

In diesem Parameter können Sie eine Kurzbeschreibung für das angelegte FTP Profil angeben. Diese Beschreibung hat rein informellen Charakter und kann somit von Ihnen frei gewählt werden.

Anlegen von HTTP Kommunikationsprofilen

Dieser Abschnitt beschreibt, wie Sie HTTP Sende-Kommunikationsprofile einrichten können und wie ein HTTP Server (Empfangsprofil) im System zu konfigurieren ist.

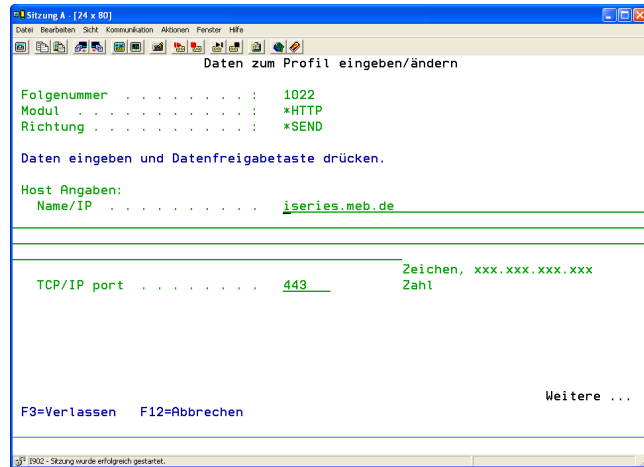
Anlegen eines HTTP-Sendeprofls

Um Daten per HTTP POST an Ihre Partner versenden zu können, benötigen Sie für jeden Partner ein HTTP Sendeprofil. In diesen Profilen werden die sendespezifischen HTTP Einstellungen hinterlegt, die für die Kommunikation in Richtung Ihres Partners notwendig sind.

In das Menü zum Anlegen eines HTTP Sendeprofls gelangen Sie, indem Sie im i-effect Hauptmenü den Menüpunkt „52“ auswählen. Im darauf folgenden Menü sehen Sie eine Liste der, falls schon Profile angelegt wurden, bereits vorhandenen Kommunikationsprofile.

Rufen Sie nun durch Drücken von F6 das Menü zum Anlegen eines Kommunikationsprofils auf und wählen anschließend mit Auswahl „1“ den HTTP Kommunikationsweg aus. Im darauf folgenden Menü wählen Sie bitte dann den Eintrag „*SEND“ aus.

Sie erhalten die folgende Anzeige:



Nun können Sie die benötigten Parameter konfigurieren:

Host Angaben

Name/IP:

Geben Sie hier die IP Nummer oder den per DNS auflösbaren Hostnamen des HTTP Servers Ihres Kommunikationspartners an.

TCP/IP port:

Geben Sie hier die Portnummer des HTTP Servers Ihres Kommunikationspartners an.

HTTP Angaben

Verbindung Timeout

Die hier angegebene Zeit wartet der HTTP Client ab, um eine Verbindung zu einem entfernten Host (zum Server Ihres Partners) aufzubauen. Wenn nach der hier, in Sekunden, definierten Zeit der Verbindungsaufbau zu dem Server Ihres Partners nicht zustande kommt wird der Sendevorgang abgebrochen. Nach der in Parameter „Send Retry pause“ definierten Zeit erfolgt dann die Sendewiederholung.

Empfohlener Wert: 120 Sekunden.

Lese Timeout

Timeout in Sekunden für das Lesen von Daten auf einer offenen Datenverbindung.

Empfohlener Wert: 120 Sekunden.

Interner Timeout

Timeout in Sekunden bevor ein interner Timeout gemeldet wird.

Maximale Anz. Sendewiederholung

Anzahl an Wiederholungen, die für den Versand einer Datei vorgenommen werden. Kommt keine Verbindung zu Stande, oder wird eine Verbindung abgebrochen, so versucht das System, bis zu der hier eingestellten Maximalanzahl, die Versendung zu wiederholen.

Sende Wiederholpause

Pause in Sekunden, die zwischen zwei Sendeversuchen gewartet wird.

Content Typ

Hier können Sie die Art des Inhalts der HTTP Daten festlegen.

Es stehen folgende Sonderwerte zur Auswahl:

<i>*CONSENT</i>	Die Daten haben keines der nachfolgenden Formate (application/edi-consent).
<i>*EDIFACT</i>	Die Daten sind im EDIFACT-Format (application/EDIFACT).
<i>*X12</i>	Die Daten sind im X12-Format (application/EDIX12).
<i>*XML</i>	Die Daten sind im XML-Format (text/xml)..
<i>*BINARY</i>	Die Daten sind Binärdaten (application/octet-stream).
<i>*FRMFILE</i>	Der Typ wird anhand der Dateieindung der Eingabedatei ermittelt. (.edi = application/EDIFACT). Bei *FRMFILE für DB2 Dateien ergibt sich als Content-Typ immer *BINARY (application/octet-stream), da in der DB2 keine Dateieindungen im herkömmlichen Sinn existieren.

Proxy Server

Wenn Sie einen Proxy Server für die HTTP Kommunikation einsetzen möchten, können Sie hier die zu verwendenden Parameter hinterlegen.

Folgende Parameter stehen zur Auswahl:

<i>Host name/IP</i>	Geben Sie hier die IP-Adresse oder DNS-Namen an.
<i>TCP/IP Port</i>	Geben Sie hier den TCP/IP-Port an.
<i>Benutzername</i>	Geben Sie (falls erforderlich) hier einen autorisierten Benutzer dafür an.
<i>Kennwort</i>	Geben Sie (falls erforderlich) hier das Passwort des zuvor angegebenen autorisierten Benutzers dafür an.

SSL

Dieser Parameter steuert das zu verwendene Protokoll. Geben Sie hier an, ob die HTTP-Kommunikation über SSL/HTTPS (Secure Socket Layer) oder über normales HTTP erfolgen soll.

<i>*YES</i>	Ja, die Verbindung erfolgt über SSL/HTTPS
<i>*NO</i>	Nein, die Verbindung erfolgt über standard HTTP.

Import nicht vertrauenswürdiger Zertifikate

Tragen Sie in diesem Parameter den Wert **YES* ein um bei Verbindungen über https (SSL/TLS) die Server Zertifikate, die nicht in Ihrem Keystore vorhanden sind, automatisch zu importieren. Jedoch sollten Sie sich in diesem Fall darüber bewusst sein, dass Sie automatisch auch jedem Server, zu dem Sie eine Verbindung über https aufbauen und dessen Zertifikat NICHT in Ihrem Keystore enthalten ist, Ihr Vertrauen schenken.

Ist dieser Parameter mit dem Wert **NO* gesetzt und das Zertifikat von dem Server zu dem Sie versuchen eine Verbindung aufzubauen nicht in Ihrem Keystore enthalten, so wird die Verbindung automatisch geschlossen. Der Verbindungsabbruch ist in diesem Falle korrekt, da das Zertifikat nicht in Ihrem Keystore enthalten ist und somit die Identität des Servers nicht geprüft werden kann.

<i>*YES</i>	Ja, unbestätigte Zertifikate werden automatisch importiert.
<i>*NO</i>	Nein, unbestätigte Zertifikate werden nicht automatisch importiert.

Client Authentifizierung verwenden

Bei der Auswahl **YES* für den Parameter „SSL“ können Sie in diesem Parameter angeben ob sich der HTTP Client beim Verbindungsaufbau zum Server Ihres Partners mit Ihrem X509 Zertifikat authentifizieren muss. Nur wenn diese Prüfung des vom Client gesendeten Zertifikates gegen das Zertifikat im Keystore des Servers erfolgreich ist, akzeptiert der HTTP Server Ihres Partners die eingehende Verbindung. Andernfalls schließt er die vom Client aufgebaute Verbindung, da nicht sichergestellt ist, dass Sie wirklich ein autorisierter Partner sind, der versucht Daten an den Server zu senden.

Sie sollten von Ihrem Partner explizit mitgeteilt bekommen, wenn diese Form der SSL Authentifizierung verlangt wird,

<i>*AUTO</i>	Die Standardeinstellung. Beim Verbindungsaufbau (SSL Handshake) wird automatisch ermittelt ob Client Authentifizierung vom Server verlangt wird. Ist dies der Fall, so wird versucht das passende Zertifikat zum Server zu übermitteln.
<i>*YES</i>	Ja, es wird Client Authentifizierung verlangt. Der Verbindungsaufbau wird explizit mit dieser Einstellung durchgeführt. Bei Servern die dies nicht verlangen, führt dies zum Fehler und dem Abbruch der Verbindung.

Bitte beachten Sie, dass diese Form der SSL Authentifizierung nicht von sehr vielen Server verlangt wird und im Internet im allgemeinen nicht üblich ist.

SSL Verbindungszertifikat

Wenn Sie den Wert **YES* beim Parameter „SSL Client Authentifizierung“ verwenden, können Sie hier den Namen des Schlüsselpaars im Keystore eintragen, der Ihren öffentlichen Schlüssel (das Zertifikat) für die Authentifizierung enthält. Dieses Zertifikat wird beim Verbindungsaufbau an den Server übermittelt. Es muss sich daher natürlich vor Verbindungsaufbau im Keystore des HTTP Servers Ihres Partners befinden.

Beschreibung

Bei Bedarf können Sie hier eine Kurzbeschreibung des angelegten HTTP Sendeprofiles angeben. Der hier eingetragene Text besitzt rein informellen Charakter und ist somit frei wählbar.

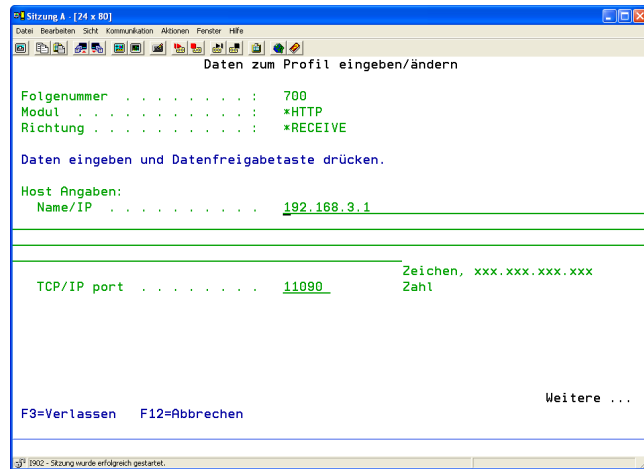
Anlegen eines HTTP-Empfangsprofils (HTTP Server)

Um HTTP POST Daten Ihrer Partner empfangen zu können, müssen Sie einen HTTP Server anlegen. Sie können mehrere HTTP Server Instanzen im System anlegen. Jeder HTTP Server der von Ihnen angelegt wird, muss allerdings auf einer noch nicht verwendeten Adresse/Port gesetzt werden. Der HTTP Server wartet auf einer von Ihnen definierten Adresse/Port auf eingehende Daten.

Um in das Menü zum Anlegen eines HTTP Empfangsprofils gelangen Sie, indem Sie im i-effect Hauptmenü den Menüpunkt „52“ auswählen. Im darauf folgenden Menü sehen Sie eine Liste der, falls schon Profile angelegt wurden, bereits vorhandenen Kommunikationsprofile.

Rufen Sie nun durch Drücken von F6 das Menü zum Anlegen eines Kommunikationsprofils auf und wählen anschließend mit Auswahl „1“ den HTTP Kommunikationsweg aus. Im darauf folgenden Menü wählen Sie bitte dann den Eintrag „*RECEIVE“ aus.

Sie erhalten die folgende Anzeige:



Nun können Sie die benötigten Parameter konfigurieren:

Host Angaben:

Name/IP

Der Hostname/die IP-Adresse an den der HTTP Server gebunden wird.

TCP/IP port

Der Port auf dem der HTTP Server auf eingehende Verbindungen wartet.

HTTP Angaben:

Verbindung Timeout

Timeout in Sekunden für eine inaktive Verbindung.

Empfohlener Wert: 120 Sekunden.

Lese Timeout

Geben Sie in diesem Parameter die Zeit (in Sekunden) an, die der HTTP Server maximal auf Daten einer eingegangenen Verbindung warten soll. Ist diese Zeit abgelaufen, wird ein Timeout-Fehler gemeldet und die Verbindung wird abgebrochen.

Empfohlener Wert: 120 Sekunden.

Interner Timeout

Timeout in Sekunden bevor ein interner Timeout gemeldet wird.

HTTP Server

Maximale Server Threads

Mit Hilfe dieses Parameters geben Sie an, wie viele Verbindungen der HTTP Server maximal gleichzeitig verarbeiten soll. Ist diese Anzahl der gleichzeitigen Verbindungen erreicht, werden die anstehenden Verbindungen in eine Warteschlange gestellt und verarbeitet, sobald eine freie Verbindung verfügbar ist.

Pfad für empfangene Daten

Hier können Sie ein IFS Verzeichnis für die Speicherung der empfangenen Daten angeben.

Hinweis: In diesem Parameter dürfen ausschließlich IFS Verzeichnisse angegeben werden.

Authentifizierung erforderlich?

Hier können Sie angeben, ob für Verbindungen zum Server eine Authentifizierung mittels Benutzername und Passwort benötigt wird. Diese geschieht über die HTTP „Basic Authentication“ (RFC 2617)

Wie Sie diese Authentifizierungsdaten für einen Server sowie für einen Partner einrichten können, erfahren Sie in Abschnitt „Benutzerauthentifizierung für Kommunikationsserver“ in diesem Kapitel.

Es wird empfohlen, die Benutzerauthentifizierung für den Server zu aktivieren. NUR mittels Benutzername und Passwort ist eine partnerbezogene Verarbeitung der empfangenen Daten des Servers möglich. Hierzu kann jedem Benutzernamen ein Partneralias aus Menü 50 zugeordnet werden kann.

*YES	Ja, es werden Name und Passwort für eine Anmeldung am Server verlangt.
*NO	Nein, es wird KEINE Authentifizierung verlangt.

Maximale Dateigröße

Legen Sie hier maximale Größe der Daten (in Kb) fest, die per HTTP POST in einer Verbindung auf den Server übertragen werden können.

SSL

Dieser Parameter steuert das vom HTTP Server zu verwendene Protokoll. Als Auswahlmöglichkeiten stehen Ihnen *YES und *NO zur Verfügung. Bei der Auswahl *NO wird das Standard HTTP-Protokoll verwendet. Durch Setzen des Wertes *YES geben Sie an, dass der HTTP Server SSL/TLS verwenden soll und somit nur über HTTPS-Verbindungen erreichbar ist. Bei Verwendung von *YES können Sie in den drei folgenden Parametern "Client Authentifizierung?" "Import nicht vertrauenswürdiger Zertifikate" sowie "SSL Verbindungszertifikat" das Verhalten des HTTPS Servers weiter spezifizieren.

*NO	Es wird das HTTP-Protokoll verwendet (Standard).
*YES	Es wird das HTTPS-Protokoll verwendet.

Import nicht vertrauenswürdiger Zertifikate?

Bei der Auswahl *YES im Parameter „SSL“ haben Sie mittels des hier eingetragenen Wertes die Möglichkeit anzugeben, ob Client Zertifikate, die NICHT in Ihrem Keystore enthalten sind, automatisch vom HTTP Server in Ihren Keystore importiert werden sollen. Dies erreichen Sie indem Sie in diesem Parameter den Wert *YES eingeben. Allerdings stellt der Wert *YES für diesen Parameter auch ein gewisses Sicherheitsrisiko dar. Durch die automatische Importierung des vom Clients beim Verbindungsaufbau gesendeten Zertifikates in den Keystore, wird jeder Client als vertrauenswürdig eingestuft.

Ist dieser Parameter mit dem Wert *NO gesetzt und das Zertifikat beim Aufbau einer Verbindung nicht in Ihrem Keystore enthalten, so wird die Verbindung automatisch geschlossen. Der Verbindungsabbruch ist in diesem Falle korrekt, da das Zertifikat nicht in Ihrem Keystore enthalten ist und somit die Identität des Clients nicht sichergestellt werden kann.

Die automatische Importierung in den Keystore greift jedoch nur, wenn der Parameter „Client Auth. erforderlich?“ mit dem Wert *YES gesetzt ist.

*YES	Ja, nicht vertrauenswürdige Client Zertifikate werden automatisch importiert.
*NO	Nein, nicht vertrauenswürdige Client Zertifikate werden NICHT automatisch importiert.

Client Authentifizierung erforderlich?

Bei der Auswahl *YES für den Parameter „SSL“ können Sie in diesem Parameter angeben ob der Client, der eine Verbindung zu Ihnen aufbaut, sich gegenüber (Ihrem) HTTP Server mit seinem X509 Zertifikat authentifizieren muss. Wenn Sie hier die Auswahl *YES treffen und im vorhergehenden Parameter „Import nicht vertrauenswürdiger Zertifikate“ den Wert *NO angeben, muss das Zertifikat Ihres Partners schon vor dem Verbindungsaufbau in Ihrem Keystore vorhanden sein. Somit ist gewährleistet, dass das über die aufgebaute HTTPS-Verbindung automatisch gesendete Zertifikat Ihres Partners vom HTTP Server geprüft werden kann. Nur wenn diese Prüfung des vom Client gesendeten Zertifikates gegen das Zertifikat aus Ihrem Keystore erfolgreich ist, akzeptiert der HTTP Server die eingehende Verbindung. Andernfalls schließt er die vom Client aufgebaute Verbindung, da nicht sichergestellt ist, dass es wirklich Ihr Partner ist, der versucht eine Verbindung zu Ihnen aufzubauen.

Geben Sie in diesem Parameter den Wert *NO an, findet die Prüfung des Zertifikats während des Verbindungsaufbaus nicht statt.

*YES	Ja, es wird Client Authentifizierung verlangt.
*NO	Nein, es wird keine Client Authentifizierung verlangt.

Bitte beachten Sie, dass diese Form der SSL Authentifizierung nicht von sehr vielen Clients unterstützt wird und im Internet im allgemeinen nicht üblich ist.

SSL Verbindungszertifikat

Hier können Sie den Namen des Schlüsselpaars im Keystore eintragen, der Ihren öffentlichen Schlüssel (das Zertifikat) enthält. Dieses Zertifikat wird an jeden Client der eine SSL Verbindung zu Ihrem HTTP Server aufbaut übermittelt. Hiermit authentifiziert sich Ihr Server gegenüber dem Client. Diese Zertifikat sollte sich natürlich vor Verbindungsaufbau im Keystore des Clients Ihres Partners befinden.

Diese Form der HTTPS Authentifizierung ist das Standardverfahren im Internet.

Beschreibung

In diesem Parameter können Sie eine Kurzbeschreibung für den angelegten HTTP Server angeben. Diese Beschreibung hat rein informellen Charakter und kann somit von Ihnen frei gewählt werden.

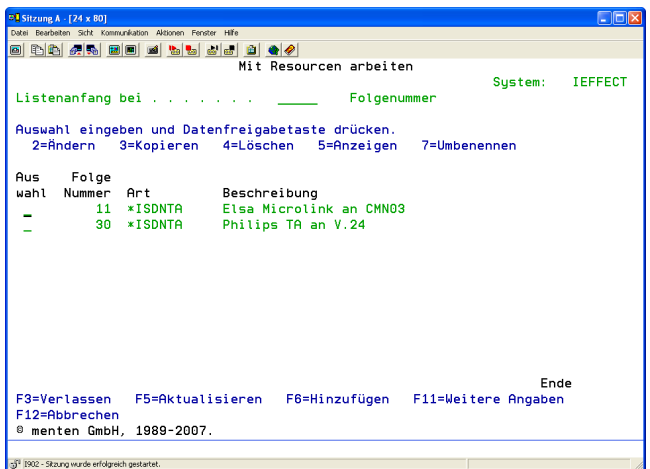
Menüpunkt 53: EDI- Kommunikationsressourcen

Der Menüpunkt 53 hat für Sie nur Relevanz, wenn Sie Kommunikation über TELEBOX betreiben möchten.

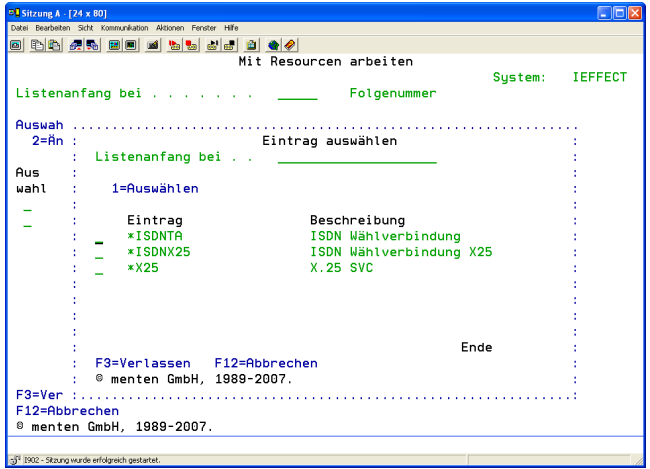
In diesem Menü können Sie alle für Kommunikationsaufgaben zur Verfügung stehenden Hardware-Ressourcen verwalten. Eine hier hinterlegte Hardware- konfiguration kann dann in Menü 52 (Auswahl 8) dem gewünschten *TELEBOX Kommunikationsprofil zugeordnet werden. Folgende Hardwaretypen stehen als Ressource zur Auswahl:

- o ISDN (*ISDN TA)
Digitaler ISDN Terminaladapter an der V.24 der AS/400
- o ISDN X25 (*ISDN X25)
Ein X.25 ISDN Terminaladapter an der V.24 oder X.21 der AS/400 auf dem PC.
- o X.25 SVC (*X25)
Ein Datex-P Hauptanschluss

Folgende Abbildung zeigt Menü 53 mit zwei angelegten Ressourcen:



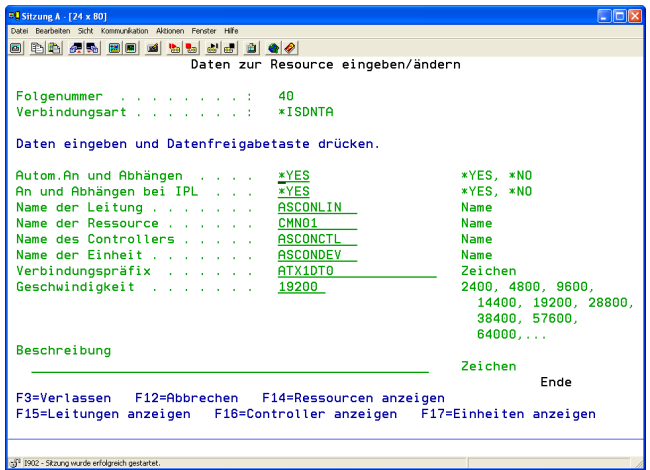
Um eine Kommunikationsressourcen anzulegen, drücken Sie bitte in die Taste F6. Es erscheint das folgende Dialogprogramm:



Gehen Sie nun mit Auswahl 1 vor den gewünschten Typ und drücken die Datenfreigabetaste.

Im Folgenden werden die Parameter der verschiedenen Ressourcen erklärt.

*ISDN TA Ressource



Autom.An und Abhängen

Hier kann angegeben werden, ob das An- und Abhängen der Leitungen automatisch erfolgen soll. In diesem Fall ist eine Aktivierung der Leitungsbeschreibungen durch das Bedienungspersonal nicht erforderlich.

- *YES Ja, die Leitungen werden automatisch an- und abgehängt.
- *NO Nein, die Leitungen müssen vom Systembediener an- und abgehängt werden.

An und Abhängen bei IPL

Nach einem Systemneustart können die hier verwalteten Leitungen automatisch angehängen werden. Die Eintragung in diesem Feld steuert den Wert IPL() in der Leitungsbeschreibung.

- *YES Ja, nach einem Systemstart wird die Leitung angehängen IPL(*YES).
- *NO Nein, die Leitungen werden nach einem Systemstart nicht angehängen IPL(*NO).

Name der Leitung

Name der Leitungsbeschreibung, die für diese Ressource verwendet werden soll.

Name der Ressource

Hier ist der AS400 Ressourcenname einzutragen (CMN01/LIN011....)

Name des Controllers

Name der Controllerbeschreibung, die für diese Ressource verwendet werden soll.

Name der Einheit

Name der Einheitenbeschreibung, die für diese Ressource verwendet werden soll.

Verbindungspräfix

Hier können für die Anwahl weitere Ziffern hinterlegt werden, die VOR die in der Profil-Ressource Zuordnung hinterlegte Verbindungsnummer eingefügt werden. Durch z.B. ATX1DT0 kann somit das Vorwählen einer „0“ zur Erreichung eines Amtsanschlusses innerhalb einer Telefonanlage erreicht werden.

Geschwindigkeit

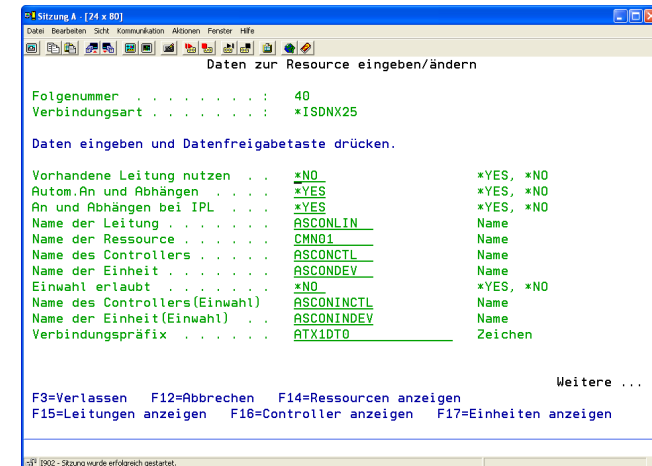
Die Leitungsgeschwindigkeit dieser Ressource.

Gültige Werte sind 2400,4800,9600,14400,19200,38400,57600,64000....

Beschreibung

Eine Kurzbeschreibung des Ressourceneintrags

*ISDNX25 Resource



Vorhandene Leitung nutzen

Legt fest, ob eine bereits auf dem System bestehende Leitungsbeschreibung genutzt werden soll oder ob eine eigene Leitungsbeschreibung erstellt werden soll. Eine vorhandene Leitung liegt sicherlich dann vor, wenn bereits ein DATEX-P Anschluß genutzt wird, an dem mehrere logische Kanäle bedient werden.

- *YES Ja, eine vorhandene Leitung soll genutzt werden.
- *NO Nein, es soll eine neue Leitung erstellt werden.

Autom.An und Abhängen

Hier kann angegeben werden, ob das An- und Abhängen der Leitungen automatisch erfolgen soll. In diesem Fall ist eine Aktivierung der Leitungsbeschreibungen durch das Bedienungspersonal nicht erforderlich.

- *YES Ja, die Leitungen werden automatisch an- und abgehängt.
 *NO Nein, die Leitungen müssen vom Systembediener an- und abgehängt werden.

An und Abhängen bei IPL

Nach einem Systemneustart können die hier verwalteten Leitungen automatisch angehängen werden. Die Eintragung in diesem Feld steuert den Wert IPL() in der Leitungsbeschreibung.

- *YES Ja, nach einem Systemstart wird die Leitung angehängen IPL(*YES).
 *NO Nein, die Leitungen werden nach einem Systemstart nicht angehängen IPL(*NO).

Name der Leitung

Name der Leitungsbeschreibung, die für diese Ressource verwendet werden soll.

Name der Resource

Hier ist der AS400 Ressourcenname einzutragen (CMN01/LIN011....)

Name des Controllers

Name der Controllerbeschreibung, die für diese Ressource verwendet werden soll.

Name der Einheit

Name der Einheitenbeschreibung, die für diese Ressource verwendet werden soll.

Einwahl erlaubt

Bei bestimmten installierten Kommunikationsmodulen (z.B. OFTP) kann die Einwahl von Partnern in dieses System AS/400 zugelassen werden. Mit diesem Parameter wird mitgeteilt, ob dies grundsätzlich bei dieser Ressource möglich sein soll.

- *YES Ja, eine Einwahl ist bei bestimmten Modulen möglich.
 *NO Nein, mit dieser Resource ist eine Einwahl nicht möglich.

Name des Controllers (Einwahl)

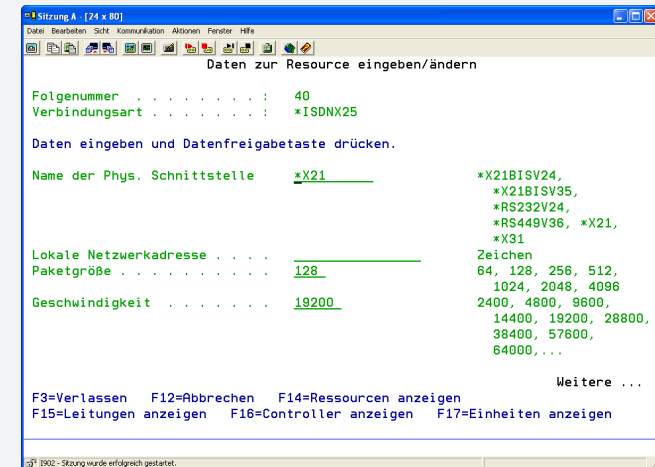
Hier wird, falls Einwahl erlaubt ist, der Name der Controllerbeschreibung festgelegt, der hierfür verwendet werden soll.

Name der Einheit (Einwahl)

Hier wird, falls Einwahl erlaubt ist, der Name der Einheitenbeschreibung festgelegt, der hierfür verwendet werden soll.

Verbindungspräfix

Hier können für die Anwahl weitere Ziffern hinterlegt werden, die VOR die in der Profil-Resource Zuordnung hinterlegte Verbindungsnummer eingefügt werden. Durch z.B. ATX1DT0 kann somit das Vorwählen einer „0“ zur Erreichung eines Amtsanschlusses innerhalb einer Telefonanlage erreicht werden.

**Name der Phys. Schnittstelle**

Der Name der Schnittstelle, an die die hier beschriebene Resource angeschlossen ist.

Mögliche Werte: *X21BISV24, *X21BISV35, *RS232V24, *RS449V36, *X21, *X31

Lokale Netzwerkadresse

Die Adresse (Anschlußnummer), die Ihrem Anschluß zugeordnet ist.

Paketgröße

Die zu verwendende Paketgröße.

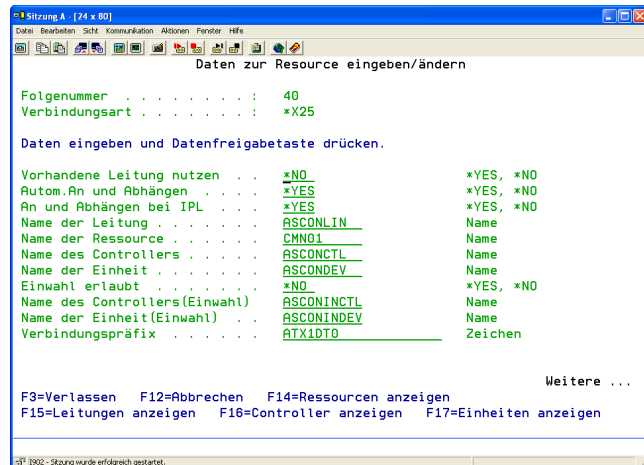
Mögliche Werte: 64, 128, 256, 512, 1024, 2048, 4096

Geschwindigkeit

Die Leitungsgeschwindigkeit dieser Resource. Gültige Werte sind 2400,4800,9600,14400,19200,38400,57600,64000....

Beschreibung

Eine Kurzbeschreibung des Ressourceneintrags

***X25 Resource****Vorhandene Leitung nutzen**

Legt fest, ob eine bereits auf dem System bestehende Leitungsbeschreibung genutzt werden soll oder ob eine eigene Leitungsbeschreibung erstellt werden soll. Eine vorhandene Leitung liegt sicherlich dann vor, wenn bereits ein DATEX-P Anschluß genutzt wird, an dem mehrere logische Kanäle bedient werden.

*YES Ja, eine vorhandene Leitung soll genutzt werden.

*NO Nein, es soll eine neue Leitung erstellt werden.

Autom.An und Abhängen

Hier kann angegeben werden, ob das An- und Abhängen der Leitungen automatisch erfolgen soll. In diesem Fall ist eine Aktivierung der Leitungsbeschreibungen durch das Bedienungspersonal nicht erforderlich.

*YES Ja, die Leitungen werden automatisch an- und abgehängt.

*NO Nein, die Leitungen müssen vom Systembediener an- und abgehängt werden.

An und Abhängen bei IPL

Nach einem Systemneustart können die hier verwalteten Leitungen automatisch angehängen werden. Die Eintragung in diesem Feld steuert den Wert IPL() in der Leitungsbeschreibung.

*YES Ja, nach einem Systemstart wird die Leitung angehängen IPL(*YES).

*NO Nein, die Leitungen werden nach einem Systemstart nicht angehängen IPL(*NO).

Name der Leitung

Name der Leitungsbeschreibung, die für diese Ressource verwendet werden soll.

Name der Resource

Hier ist der AS400 Ressourcenname einzutragen (CMN01/LIN011....)

Name des Controllers

Name der Controllerbeschreibung, die für diese Ressource verwendet werden soll.

Name der Einheit

Name der Einheitenbeschreibung, die für diese Ressource verwendet werden soll.

Einwahl erlaubt

Bei bestimmten installierten Kommunikationsmodulen (z.B. OFTP) kann die Einwahl von Partnern in dieses System AS/400 zugelassen werden. Mit diesem Parameter wird mitgeteilt, ob dies grundsätzlich bei dieser Ressource möglich sein soll.

*YES Ja, eine Einwahl ist bei bestimmten Modulen möglich.

*NO Nein, mit dieser Ressource ist eine Einwahl nicht möglich.

Name des Controllers (Einwahl)

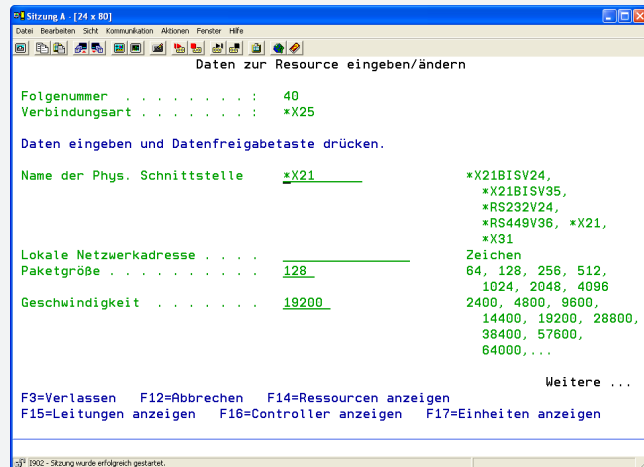
Hier wird, falls Einwahl erlaubt ist, der Name der Controllerbeschreibung festgelegt, der hierfür verwendet werden soll.

Name der Einheit (Einwahl)

Hier wird, falls Einwahl erlaubt ist, der Name der Einheitenbeschreibung festgelegt, der hierfür verwendet werden soll.

Verbindungspräfix

Hier können für die Anwahl weitere Ziffern hinterlegt werden, die VOR die in der Profil-Ressource Zuordnung hinterlegte Verbindungsnummer eingefügt werden. Durch z.B. ATX1DT0 kann somit das Vorwählen einer „0“ zur Erreichung eines Amtsanschlusses innerhalb einer Telefonanlage erreicht werden.

**Name der Phys. Schnittstelle**

Der Name der Schnittstelle, an die die hier beschriebene Resource angeschlossen ist.

Mögliche Werte: *X21BISV24, *X21BISV35, *RS232V24, *RS449V36, *X21, *X31

Lokale Netzwerkadresse

Die Adresse (Anschlußnummer), die Ihrem Anschluß zugeordnet ist.

Paketgröße

Die zu verwendende Paketgröße.

Mögliche Werte: 64, 128, 256, 512, 1024, 2048, 4096

Geschwindigkeit

Die Leitungsgeschwindigkeit dieser Ressource.

Gültige Werte sind 2400,4800,9600,14400,19200,38400,57600,64000....

Beschreibung

Eine Kurzbeschreibung des Ressourceneintrags

Benutzerauthentifizierung für Kommunikationsserver

Die Benutzerauthentifizierung ist nur für die Module *HTTP und *OFTP möglich.

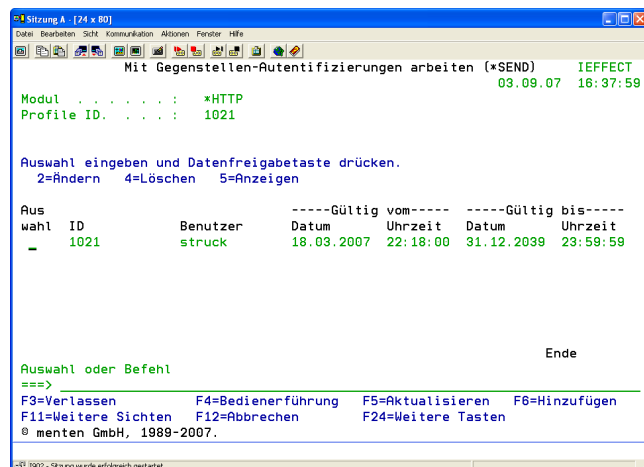
Mit der Benutzerauthentifizierung haben Sie die Möglichkeit, für jeden Partner den Zugang zu i-effect Kommunikationsservern mittels Benutzername/ID und Passwort festzulegen. Die Verknüpfung dieser Zugangsdaten mit einem Partnerprofil aus Menü 50 ermöglicht eine partnergesteuerte Verarbeitung von empfangenen Daten. Die Benutzerdaten können für das jeweilige Serverprofil (*RECEIVE) in Menü 52 eingetragen werden.

Für eine Authentifizierung mittels Benutzername und Passwort an einem entfernten Server können dies Zugangsdaten einem Sendeprofil (*SEND) in Menü 52 zugewiesen werden.

Für Flexibilität in der Verwaltung und mehr Sicherheit haben Sie die Möglichkeit, Gültigkeitszeiträume für alle Zugangsdaten festzulegen. Überschneidungen der Zeiträume sind dabei kein Problem. In solchen Fällen wird der erste gültige Eintrag für die Authentifizierung herangezogen.

In das Menü zum Anlegen der Benutzerdaten gelangen Sie, indem Sie im i-effect Hauptmenü den Menüpunkt „52“ auswählen. Im darauf folgenden Menü sehen Sie eine Liste der, falls schon Profile angelegt wurden, bereits vorhandenen *HTTP und *OFTP Kommunikationsprofile. Gehen Sie nun mit Auswahl 12 „Authentifizierungen“ vor das gewünschte *RECEIVE bzw. *SEND Kommunikationsprofil.

Sie erhalten die folgende Anzeige (hier am Beispiel eines HTTP *SEND Profils mit einem angelegten Benutzer für die Authentifizierung an der Gegenstelle):



Auswahlmöglichkeiten zum Dialogprogramm

Zur Bearbeitung der Einträge stehen Ihnen folgende Auswahlmöglichkeiten zur Verfügung. Diese können in das entsprechende Auswahlfeld vor der gewünschten Zeile eingegeben werden. Die nachfolgende Übersicht stellt die zur Verfügung stehenden Grundfunktionen dieses Dialogprogramms vor. Eine detaillierte Beschreibung der einzelnen Auswahlmöglichkeiten schließt sich an diese Übersicht an.

Hinzufügen (Auswahl F6)

Mit der Auswahl F6 legen Sie einen neuen Benutzernamen sowie das zugehörige Passwort an und verknüpfen den Benutzer mit einem existierenden Partnerprofil in Menü 50.

Ändern (Auswahl 2)

Geben Sie die Auswahl 2 in der Auswahlspalte der gewünschten Zeile ein, um diesen bestehenden Eintrag zu ändern. Bei einem bestehenden Benutzereintrag kann nur der Gültigkeitszeitraum für diesen Benutzer geändert werden. Benutzername, Passwort und zugeordneter Partner sind nach dem Anlegen nicht mehr veränderbar.

Kopieren (Auswahl 3)

Geben Sie die Auswahl 3 in der Auswahlspalte der gewünschten Zeile ein, um diesen bestehenden Benutzereintrag auf einen neuen Partneralias zu übernehmen.

Löschen (Auswahl 4)

Geben Sie die Auswahl 4 in der Auswahlspalte der gewünschten Zeile ein, um diesen bestehenden Eintrag zu löschen.

Anzeigen (Auswahl 5)

Geben Sie die Auswahl 5 in der Auswahlspalte der gewünschten Zeile ein, um diesen bestehenden Eintrag anzeigen zu lassen.

Benutzerauthentifizierung für HTTP Server

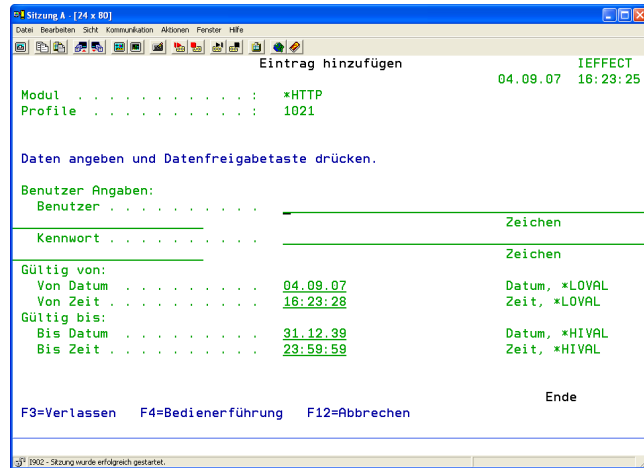
Dieser Abschnitt erklärt, wie Sie einen Benutzer für die Authentifizierung an HTTP Servern erstellen. Es wird dabei zwischen der Authentifizierung an einem lokalen i-effect HTTP Server (*RECEIVE) und der an einem entfernten HTTP Server unterschieden (*SEND).

Authentifizierung am entfernten HTTP Server

Wenn für die Verbindung zu einem HTTP Server eine Anmeldung mit Benutzername und Kennwort erforderlich ist, können Sie diese Daten für ein HTTP Sendeprofil festlegen. Sind diese Benutzerdaten für ein Sendeprofil vorhanden, werden sie automatisch beim Verbindungsaufbau an den Server gesendet. Bei mehreren hinterlegten Benutzerdaten für Sendeprofil wird jeweils das vom Gültigkeitszeitraum passende herangezogen.

Rufen Sie Menüpunkt „52“ auf und gehen mit Auswahl „12“ vor das entsprechende HTTP Sendeprofil. Im darauf folgenden Dialogprogramm drücken Sie bitte „F6“

Sie erhalten folgende Anzeige:



Benutzer Angaben

Tragen Sie hier die Authentifizierungsdaten für die Anmeldung am Server ein.

Benutzername

Der Benutzername, der zur Anmeldung am HTTP Server verwendet wird.

Kennwort

Das Kennwort zur Anmeldung für den angegebenen Benutzer.

Gültig von:

Hier können Sie den Startzeitpunkt hinterlegen, ab dem die angegebenen Benutzerdaten gültig sind.

Von Datum

Das Datum, ab dem die Benutzerdaten gültig sind.

Von Zeit

Die Uhrzeit, ab dem die Benutzerdaten an dem angegebenen Datum gültig sind.

Gültig bis:

Hier können Sie den Endzeitpunkt hinterlegen, ab dem die angegebenen Benutzerdaten ihre Gültigkeit verlieren und somit nicht mehr verwendet werden.

Bis Datum

Das Datum, ab an dem die Benutzerdaten ungültig werden.

Bis Zeit

Der Uhrzeit, ab dem die Benutzerdaten an dem angegebenen Datum ungültig werden.

Authentifizierung am i-effect HTTP Server

Für die Authentifizierung von Benutzern/Partnern an einem i-effect *HTTP Server haben Sie die Möglichkeit, Benutzerkonten für jeden definierten *HTTP Server im System zu hinterlegen. Ein Benutzer, der Daten an Ihren HTTP Server senden möchte, muss sich zuvor mit Name und Passwort anmelden. Jedem Benutzkonto muss dabei ein Partnerprofil (Menü 50) zugeordnet werden. Eine partnerngesteuerte Verarbeitung der empfangenen Daten ist somit problemlos möglich. Wenn einem Partner mehrere Benutzerkonten zugewiesen wurden, werden für die Authentifizierung immer die Daten des vom Gültigkeitszeitraum passenden Benutzkontos herangezogen.

Um Benutzkonten für einen *HTTP Server anzulegen, rufen Sie Menüpunkt „52“ auf und gehen mit Auswahl „12“ vor das entsprechende HTTP Serverprofil (*RECEIVE). Im darauf folgenden Dialogprogramm drücken Sie bitte „F6“

Sie erhalten folgende Anzeige:

Eintrag hinzufügen

Modul : *HTTP

Daten angeben und Datenfreigabetaste drücken.

Partner ID : F4

Benutzer Angaben:

Benutzer : Zeichen

Kennwort : Zeichen

Gültig von:

Von Datum : 04.09.07 Datum, *LOVAL

Von Zeit : 16:16:58 Zeit, *LOVAL

Gültig bis:

Bis Datum : 31.12.39 Datum, *HIVAL

Bis Zeit : 23:59:59 Zeit, *HIVAL

Ende

F3=Verlassen F4=Bedienführung F12=Abbrechen

1002 - Sitzung wurde erfolgreich gestartet.

Partner ID

Tragen Sie hier die ID des in den Stammdaten unter Menüpunkt 50 angelegten Partnerprofils ein. Das Benutzerkonto wird dann diesem Profil zugeordnet. Sie haben die Möglichkeit sich mit F4 die Liste der im Partnerstamm angelegten Profile anzeigen zu lassen.

Benutzer Angaben

Tragen Sie hier die Authentifizierungsdaten für die Anmeldung am Server ein.

Benutzername

Der Benutzername, der zur Anmeldung am HTTP Server verwendet werden muss.

Kennwort

Das Kennwort zur Anmeldung für den angegebenen Benutzer.

Gültig von:

Hier können Sie den Startzeitpunkt hinterlegen, ab dem die angegebenen Benutzerdaten gültig sind.

Von Datum

Das Datum, ab dem die Benutzerdaten gültig sind.

Von Zeit

Die Uhrzeit, ab dem die Benutzerdaten an dem angegebenen Datum gültig sind.

Gültig bis:

Hier können Sie den Endzeitpunkt hinterlegen, ab dem die angegebenen Benutzerdaten ihre Gültigkeit verlieren und somit nicht mehr verwendet werden.

Bis Datum

Das Datum, ab an dem die Benutzerdaten ungültig werden.

Bis Zeit

Der Uhrzeit, ab dem die Benutzerdaten an dem angegebenen Datum ungültig werden.

Benutzerauthentifizierung für OFTP Server

Für die Authentifizierung von Benutzern/Partnern an einem i-effect *OFTP Server haben Sie die Möglichkeit, Benutzerkonten für jeden definierten *OFTP Server im System zu hinterlegen. Ein Benutzer der Daten an Ihren OFTP Server senden möchte, muss sich zuvor mit Name und Passwort anmelden. Daraufhin identifiziert sich der Server gegenüber dem Client mit dem für den Client hinterlegten Benutzernamen und Kennwort. Jedem Benutzkonto muss dabei ein Partnerprofil (Menü 50) zugeordnet werden. Eine partnergesteuerte Verarbeitung der empfangenen Daten ist somit problemlos möglich. Wenn einem Partner mehrere Benutzerkonten zugewiesen wurden, werden für die Authentifizierung immer die Daten des vom Gültigkeitszeitraum passenden Benutzerkontos herangezogen.

Um Benutzkonten für einen *OFTP Server anzulegen, rufen Sie Menüpunkt „52“ auf und gehen mit Auswahl „12“ vor das entsprechende OFTP Serverprofil (*RECEIVE). Im darauf folgenden Dialogprogramm haben Sie die Möglichkeit durch drücken von „F6“ einen neuen Eintrag anzulegen.

Sie erhalten folgende Anzeige:

Eintrag hinzufügen

06.08.07 14:03:18

Modul : *OFTP

Daten angeben und Datenfreigabetaste drücken.

Partner ID : F4

Benutzer Angaben:

Benutzer : Zeichen

Kennwort : Zeichen

Benutzer Angaben Gegenstelle:

Benutzer ID : Zeichen

Kennwort : Zeichen

Weitere ...

F3=Verlassen F4=Bedienführung F12=Abbrechen

1902 - Sitzung wurde erfolgreich gestartet.

Partner ID

Tragen Sie hier die ID des in den Stammdaten unter Menüpunkt 50 angelegten Partnerprofils ein. Das Benutzerkonto wird dann diesem Profil zugeordnet. Sie haben die Möglichkeit sich mit F4 die Liste der im Partnerstamm angelegten Profile anzeigen zu lassen.

Benutzer Angaben

Tragen Sie hier die Authentifizierungsdaten für den OFTP Server ein.

Benutzername

Der Benutzername, mit dem sich der OFTP Server beim Client authentifiziert

Kennwort

Das Kennwort . mit dem sich der OFTP Server beim Client authentifiziert

Benutzer Angaben Gegenstelle

Tragen Sie hier die Authentifizierungsdaten für die Anmeldung am Server ein.

Benutzername

Der Benutzername, der zur Anmeldung am OFTP Server verwendet werden muss.

Kennwort

Das Kennwort zur Anmeldung für den angegebenen Benutzer.

Gültig von:

Hier können Sie den Startzeitpunkt hinterlegen, ab dem die angegebenen Benutzerdaten gültig sind.

Von Datum

Das Datum, ab dem die Benutzerdaten gültig sind.

Von Zeit

Die Uhrzeit, ab dem die Benutzerdaten an dem angegebenen Datum gültig sind.

Gültig bis:

Hier können Sie den Endzeitpunkt hinterlegen, ab dem die angegebenen Benutzerdaten ihre Gültigkeit verlieren und somit nicht mehr verwendet werden.

Bis Datum

Das Datum, ab an dem die Benutzerdaten ungültig werden.

Bis Zeit

Der Uhrzeit, ab dem die Benutzerdaten an dem angegebenen Datum ungültig werden.

