EDI Exchange Manual

HIPAAsuite EDI Exchange Manual

Complete EDI file pre-processor

by HIPAA Suite

EDI Processor is a module that is an option the HIPAAsuite software products for the different EDI transaction sets.

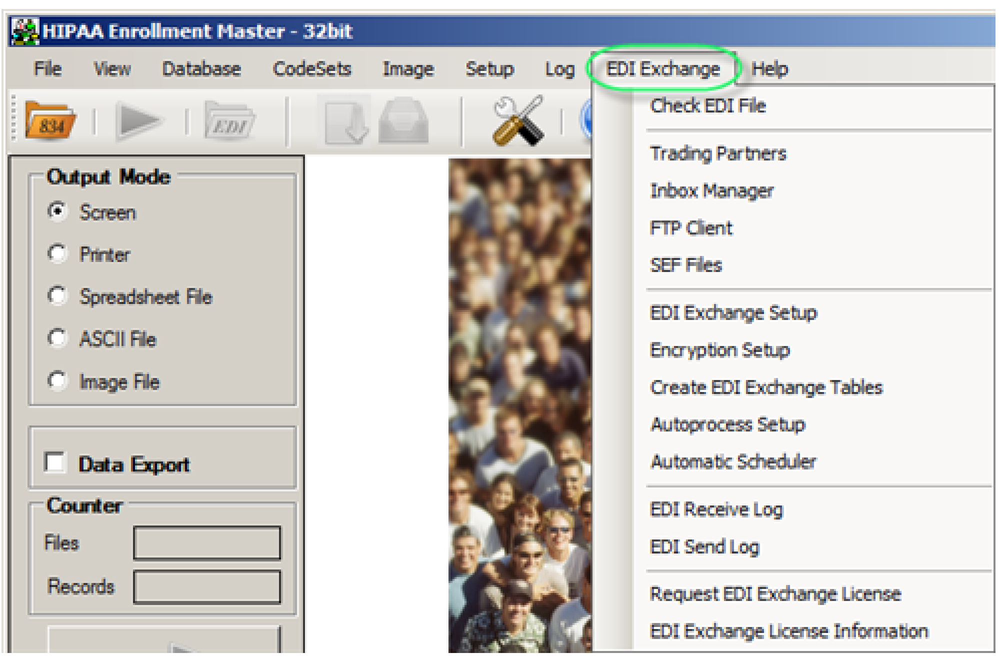
Table of Contents

1 Getting Started

1.1 About EDI Exchange

EDI Exchange is a module available in most HIPAAsuite EDI applications. It is an option that you can purchase for an additional cost. Such products as HIPAA Claim Master process EDI files but do not get or send EDI files to and from your trading partners. EDI Exchange is created to do that. EDI Exchange is designed for those organizations that have a large volume of EDI files, need more order and automation and adhere to tougher compliance rules. The EDI Exchange is an EDI pre-processor that handles FTP transport, encryption, HIPAA compliance check, trading partner management, etc. Outgoing EDI files can be checked for compliance; individual records that do not pass the check can be withheld.

HIPAAsuite products with EDI Exchange module have a main menu item called "EDI Exchange" with sub-menus to call module's functions.



The "EDI Exchange" menu in HIPAA Enrollment Master

EDI Exchange performs the following functions.

- **Trading Partners Management** — The following Trading Partner's parameters can be stored and transparently managed with the help of EDI Exchange: name, address, EDI identifiers, delivery methods, encryption parameters, FTP servers, communication numbers and folders to keep files separated, special requirements specific to this trading partner. Read more in Setting up Trading Partners.

- **File Transport** — EDI Exchange has a built-in FTP client that can securely connect to your trading partner's FTP servers. If you employ your own FTP server, you can utilize the folder structure that EDI Exchange uses to manage incoming files, users, home directories and permissions so that your Trading Partners can drop off and pick up EDI files. Supported are:
  - **Simple FTP**
  - **FTP Secure**
    - **Implicit FTPS**
    - **Explicit FTPS**
  - **Secure Shell FTP or sFTP**

  Read more in Using FTP Client.

- **Encryption** — Many healthcare-related companies use encryption to cloak the content of their EDI files. The prevalent method of encryption is **PKI** (Private Key Infrastructure) that uses the product of two incredibly large prime numbers as cipher. EDI Exchange supports **PGP** (Pretty Good Privacy), the leader in PKI products as well as the open source **GPG** project with its Windows sub project PGP4Win. Both are implementations of the same encryption mechanism. Read more in Using Encryption.

- **File Management** — EDI Exchange uses a clear directory structure to store EDI files. The structure is based on root directories for incoming files, outgoing files, processed files and suspended files. Below these root directories, there are subdirectories for each trading partner and then each transaction set. Read more in Defining Root Directory and Initializing EDI Exchange.

- **EDI Compliance Check** — EDI standards are strict and precise; adherence to the standards is very important so that any organization can work with them regardless of their backend system software. EDI Exchange has a built-in compliance engine that checks incoming files for compliance. The engine also generates a report listing each problem with the exact location. Outgoing EDI files can also be checked and you have an option to withhold individual records that violate the rules. Read more in Checking EDI Files.

- **EDI Control for Transactions** — The EDI protocols have a few supporting transaction sets that are useful to the smooth functioning of EDI exchanges. They provide the sender with an instant feedback on receipt. The following transaction sets are available:

- **TA1 Acknowledgment**
- **997/999 Functional Acknowledgment**
- **277U/277CA Unsolicited Claim Status Response** (in case of Claims)

- **Logging** — EDI Exchange has several logs that are instrumental to keep processing in order and allows to forensically investigate mishaps. There are three logs in EDI Exchange:
  - **Incoming file log** — See Accessing EDI Receive Log.
  - **Outgoing file log** — See Accessing EDI Send Log.
  - **Daily transaction log**

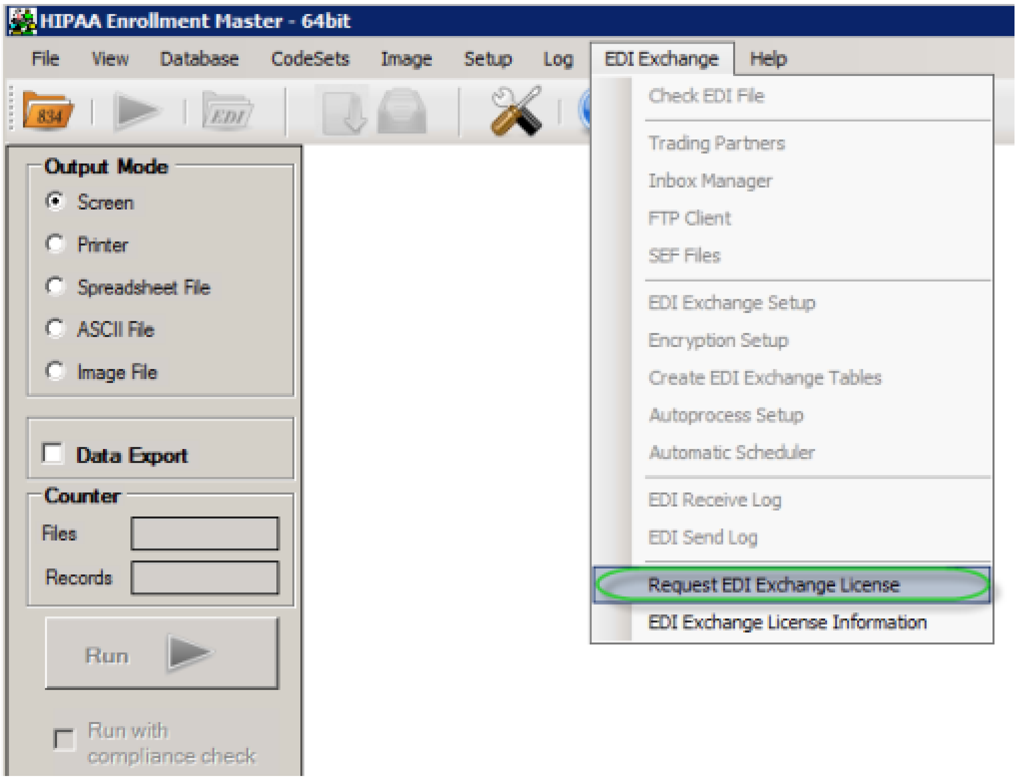
1.2 Requesting EDI Exchange License

If your trial has expired, you can request an extension to the trial.

If you purchased the product and need a final license key, you should request an EDI Exchange license.

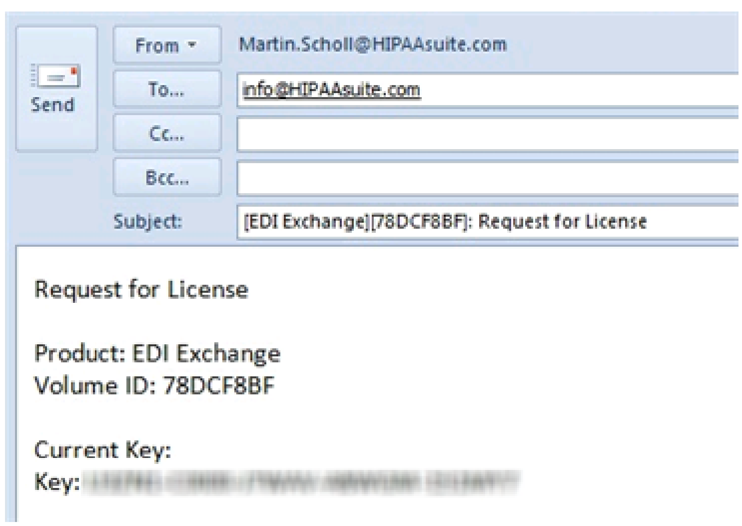
Follow the instructions below to request a trial or final license key.

1. Select "Request EDI Exchange license" under the "EDI Exchange" menu item.



A menu item to request a license key

2. Once you have clicked this menu item, your default email application appears. In our case, it is Microsoft Outlook. All information necessary to produce the key is automatically filled out.



Email message created by EDI Exchange

3. You can add a trial extension or a final key after purchasing or relocating the software.

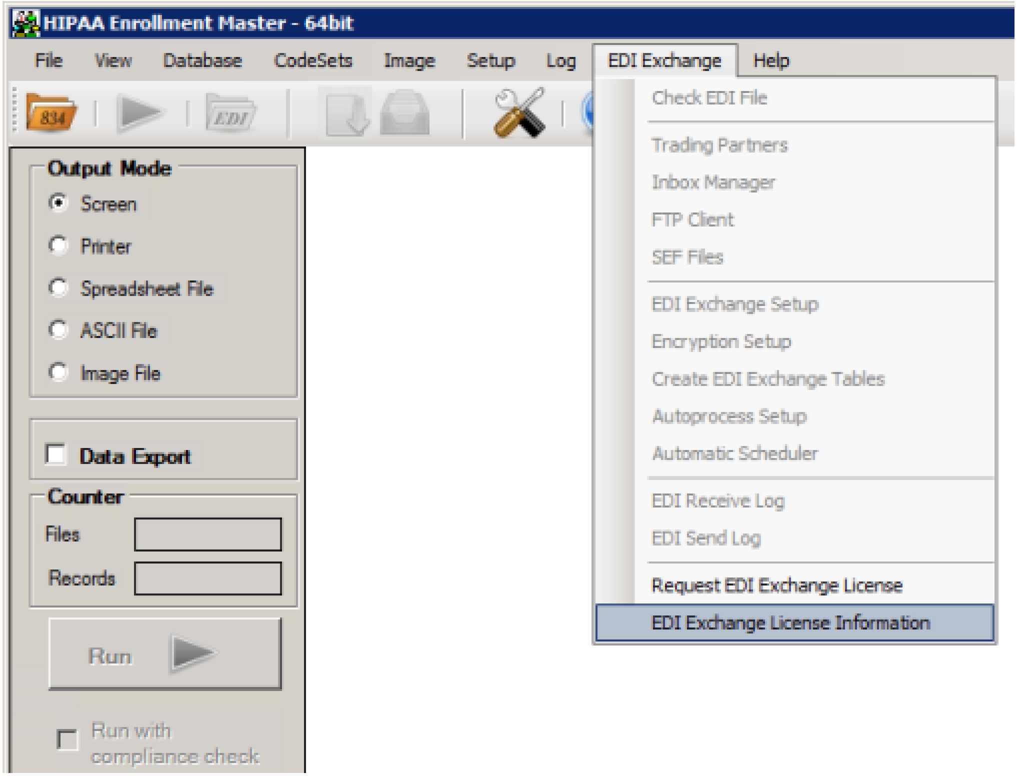
Once you receive the response with the key for EDI Exchange, you can bring the "Registration Form" screen up again and click on "Register". Enter the key to unlock EDI Exchange. In the Result area, you will see that EDI Exchange has been registered.

Entering the license key

1.3 Registering EDI Exchange

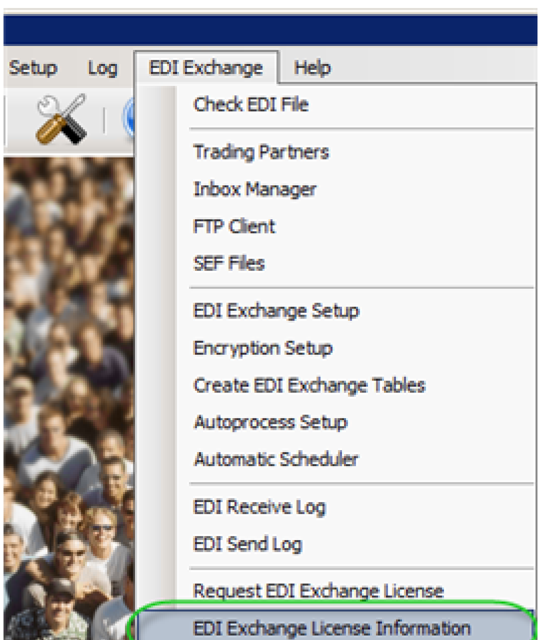
EDI Exchange is licensed separately from the host application, HIPAA Claim Master, for example. The reason is that EDI Exchange will work on all HIPAAsuite Products that are installed on your particular computer. For example, if you have HIPAA Claim Master and HIPAA Enrollment Master licensed, only one license of EDI Exchange is needed and the module will work across two products.

When you first install a HIPAAsuite product of your choice, EDI Exchange comes also with a 15-day trial period. Once the trial expires, EDI Exchange loses its functionality. The menu items under "EDI Exchange" become disabled except the last ones that allow you to license and enable the product.



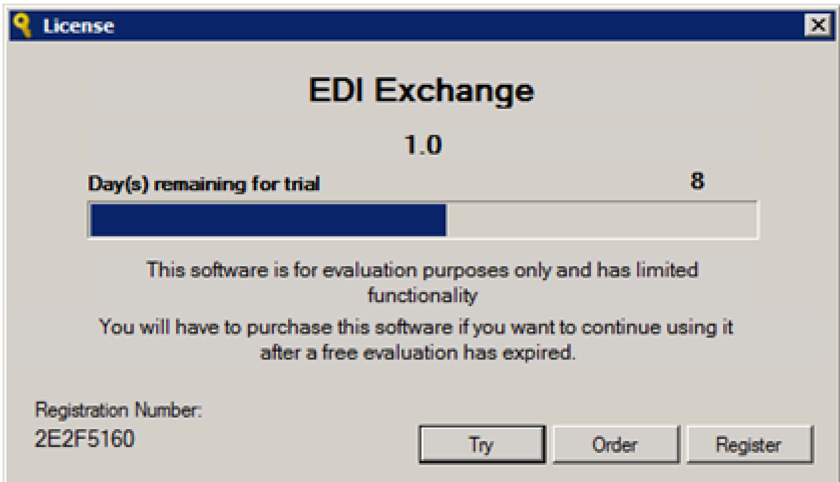
The "EDI Exchange" menu with menu items disabled

You can register the product by clicking on the "EDI Exchange License Information" option under the "EDI Exchange" menu.



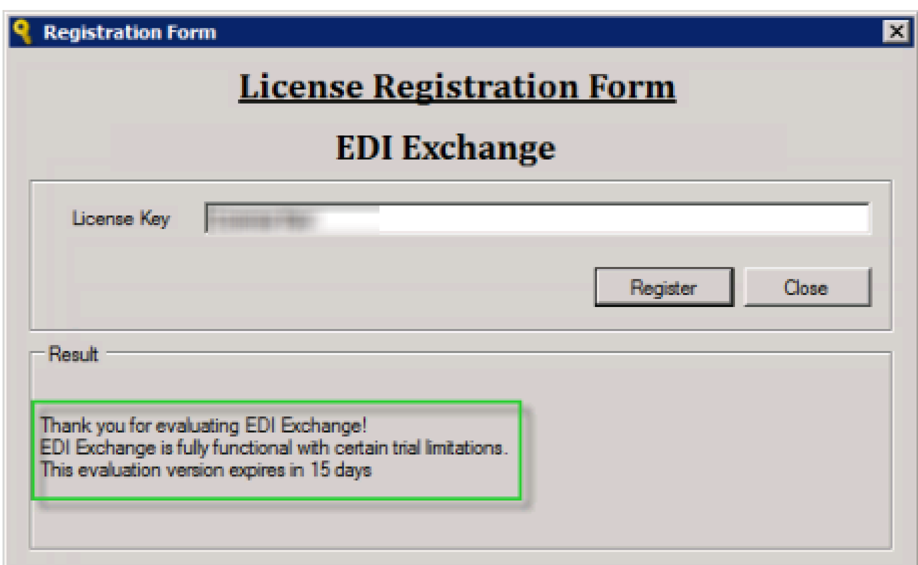
The "EDI Exchange" menu with all menu items enabled

Then the license screen appears. In the lower left corner you can find the unique registration number needed to create either trial extensions or final licensing.



The license information screen

Once you click on "Register," you can enter the license key that you have previously received via email from us (see Requesting EDI Exchange License.) Click on "Register" and you will see the registration message in the "Result" area.



Extending the trial by entering a license key

Close the "Registration Form" and continue using the EDI Exchange.

2 Configuring EDI Exchange (Obligatory Settings)

2.1 1 Setting up Database Connection

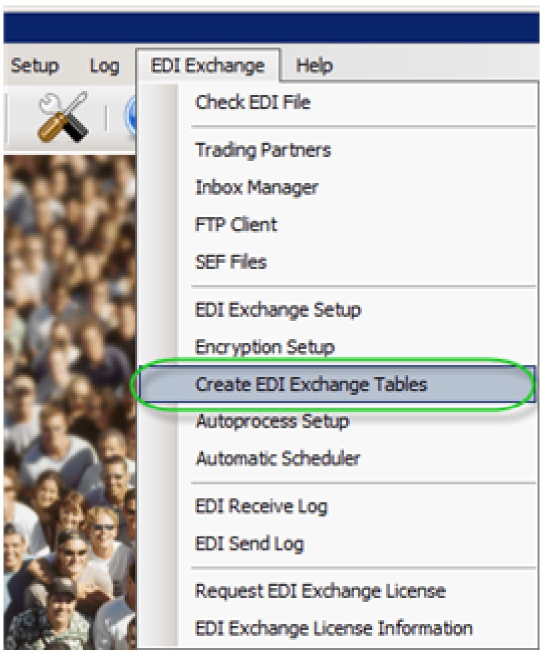
EDI Exchange work is based on the database connection that you can define under *Database* ▸ *Connection and Data Fields* in the main menu of the HIPAA host application. Make sure the connection has already been set up before proceeding with EDI Exchange.

Then proceed to the next step: Creating Database Tables.

2.2 2 Creating Database Tables

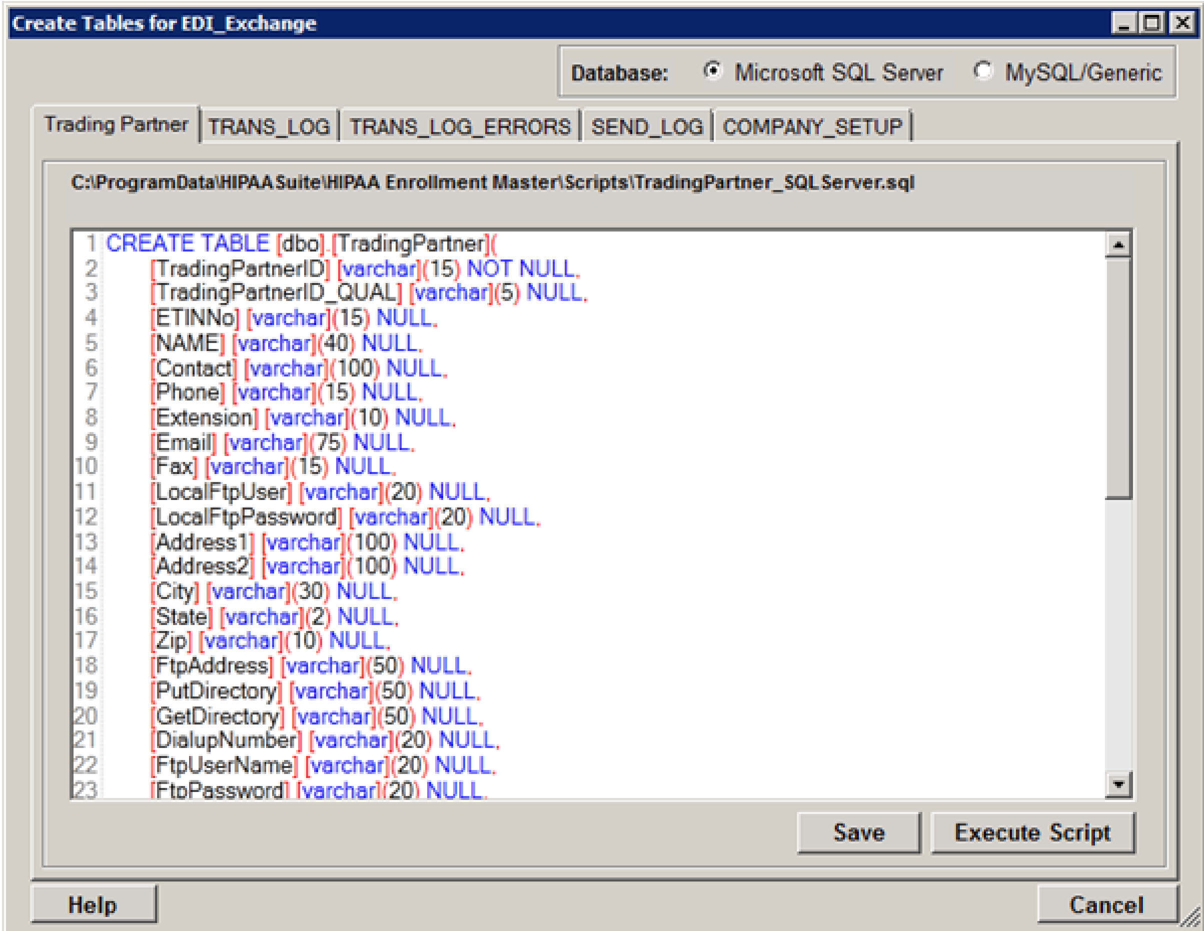
Once you have configured the database connection (Setting up Database Connection), follow the instructions below.

1. Select *EDI Exchange* ▸ *Create EDI Exchange Tables* in the main menu.



The menu item to create the necessary tables

2. The following screen will appear.



The screen to create the tables

3. Select the database type you use for your host HIPAA application.

- **Database**
    - **Microsoft SQL Server**
    - **MySQL**

> Note: In case your database is not listed, modify the scripts or ask your database administrator to make the necessary modifications.

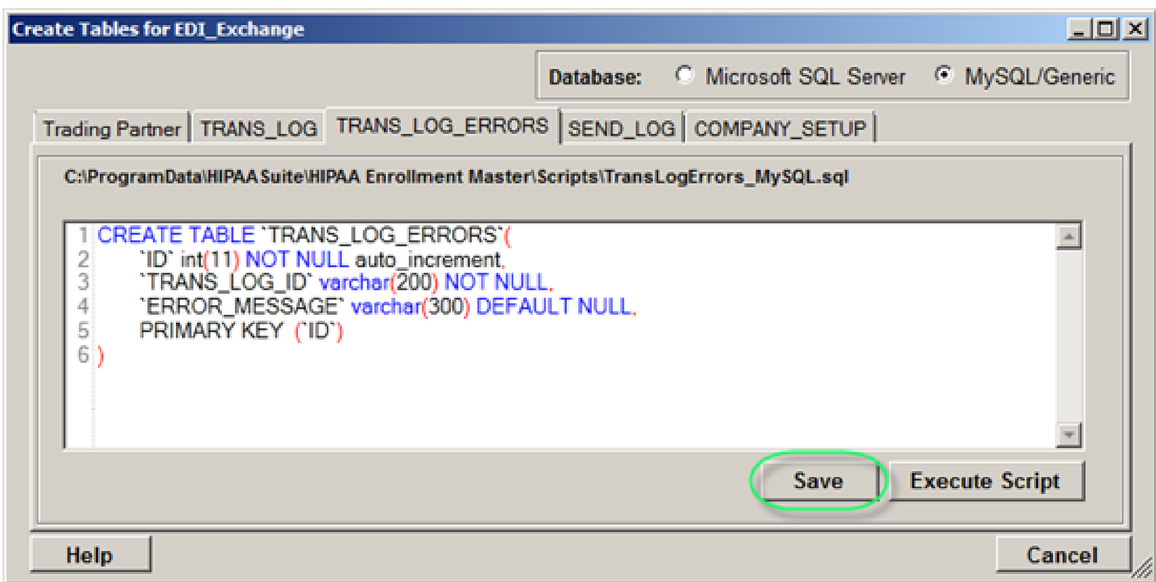
4. The following tables are part of EDI Exchange:

- **TradingPartner** — SQL statements to create the "TradingPartner" table in your database. This table contains information about trading partners.
- **Trans_Log** — SQL statements to create the "TRANS_LOG" table in your database. This table contains incoming file information, keeps track of all EDI files that you receive and the compliance check report.

- **Trans_Log_Errors** — SQL statements to create the "TRANS_LOG_ERRORS" table in your database. This table collects the results of the compliance check and keeps track of all sent files.
- **Send_Log** — SQL statements to create the "SEND_LOG" table in your database. The table contains information about EDI files created and sent to trading partners.
- **Company_Setup** — SQL statements to create the "COMPANY_SETUP" table in your database. This table collects information about you, the sender of EDI information.

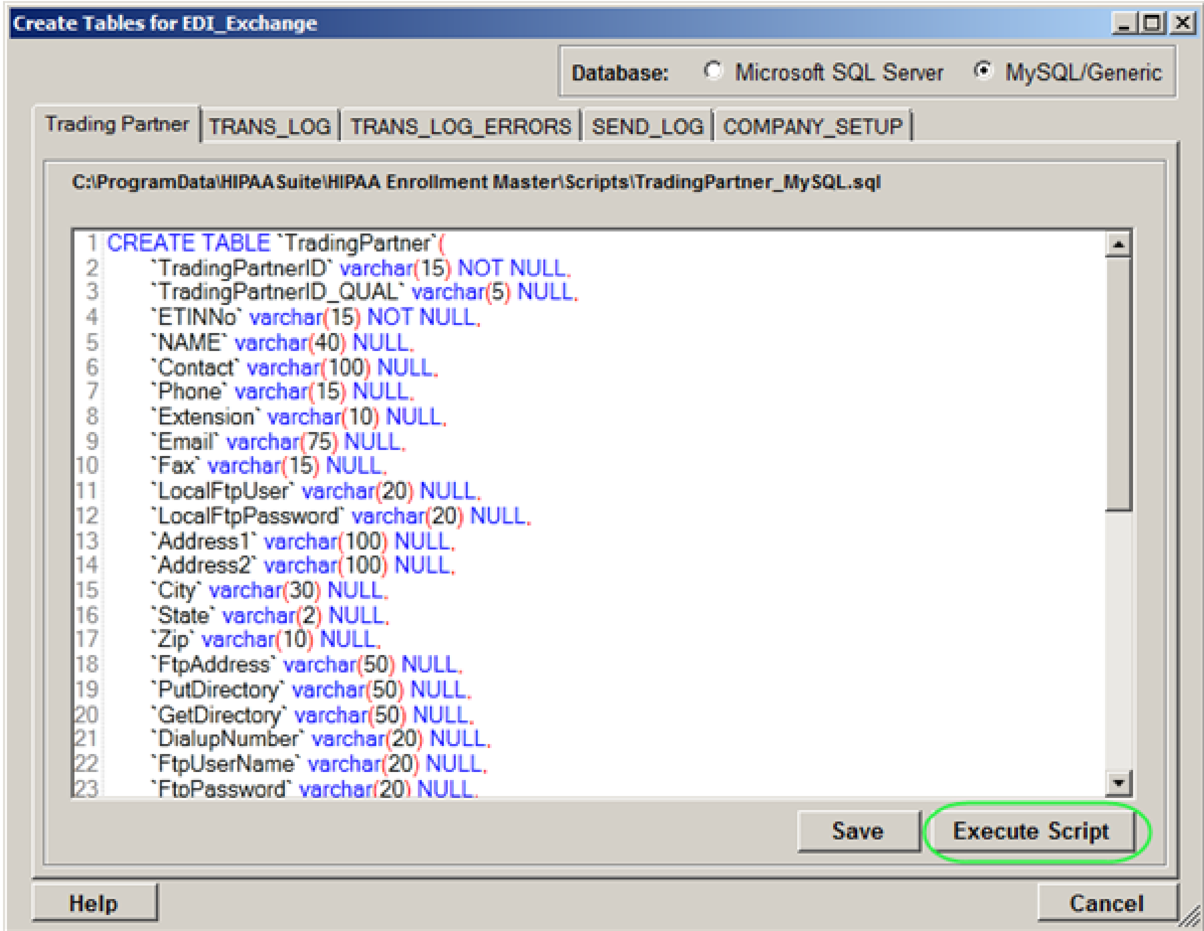
5. You can modify the scripts so that they run on your specific database. Once you have you modified the script, click "Save."

> Tip: Every database system has their own little syntax idiosyncrasies and the scripts might require tweaking. You can edit the table scripts in this screen and save your modified scripts.



The "Save" button

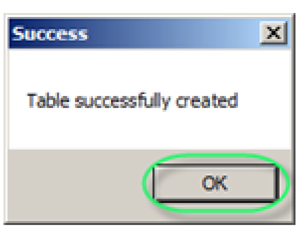
6. For **each** script on every tab, click "Execute Script" to create the corresponding table in the database.



The "Execute Script" button

> Notice: Creating tables means clicking the "Execute Script" button in all five tabs of the "Create Tables for EDI_Exchange" window. Then close this window.

7. Once the table has been created successfully, you will see the following notification:



The success message

> **Warning: Double-execution of a script wipes out the previous table you have created. Remove the script files once you have created the table so nobody can destroy the tables by accident.**

Make sure there are no any error messages and the table creation has been completed successfully.

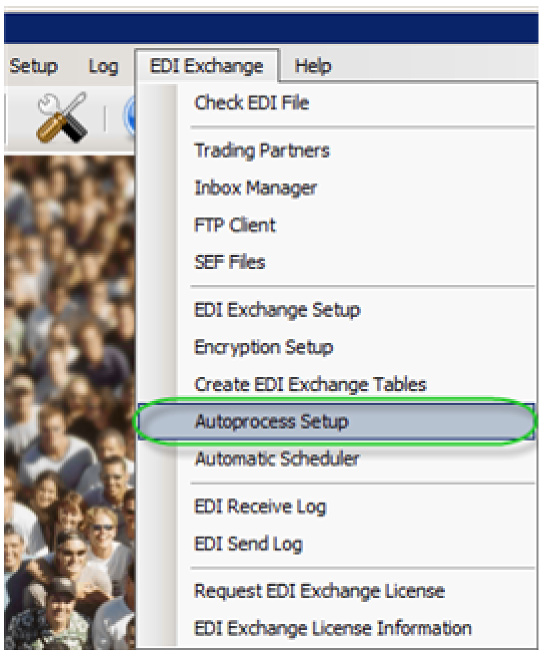
Once you have created the tables, you can start setting up the other application options. See the next step: Defining Auto-Processing Options.

2.3 3 Defining Auto-Processing Options

In the "Auto-Process Setup" you can instruct the program on what to do after analyzing and decrypting the received files in the Inbox Manager. The auto processing enables you to combine and run multiple fulfillment steps together (for example, export, saving, printing.) These options are important for the hand-over from EDI Exchange to the other HIPAAsuite program that hosts EDI Exchange.

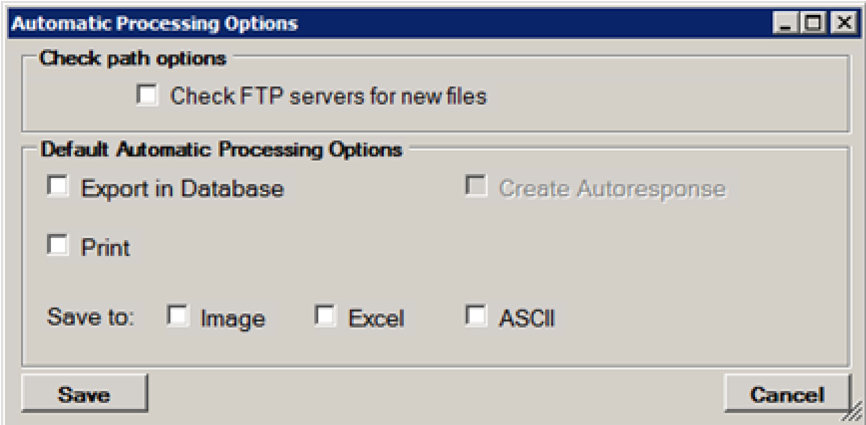
Follow the instructions below to specify the Auto Process Options.

1. Select *EDI Exchange* ▸ *Autoprocess Setup* in the main menu.



The "Autoprocess Setup" menu item

2. The following screen will appear if the host HIPAA application is Enrollment Master.



Defining the Auto Processing Options

3. The following options can be specified:

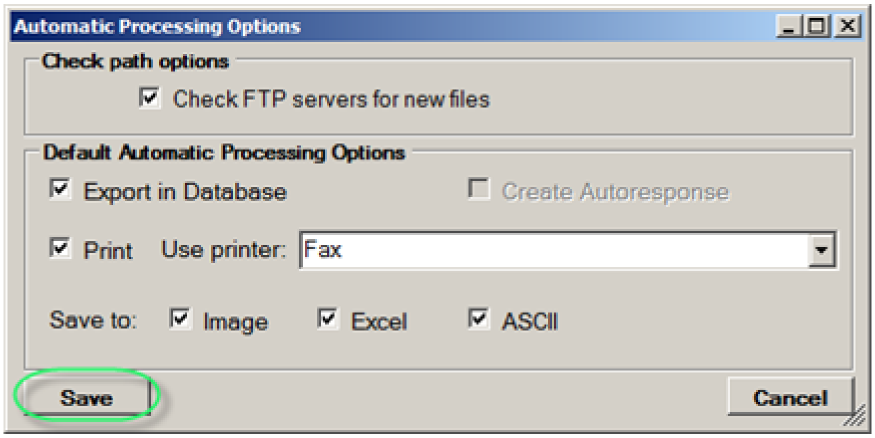
Check Path Options

- **Check FTP servers for new files** — If checked, EDI Exchange automatically looks for new files for all trading partners that have FTP connection set up. Then the program gets all the waiting files and puts them into the Inbox. In the second step, it goes through every file.

Default Automatic Processing Options

- **Export in Database** — If selected, the module exports new files to the database.
- **Print** — If selected, the module prints files using the selected printer.
- **Create Auto-Response** — If selected, the module creates an auto-response to the received files.
- **Save to** — If selected, the system automatically saves files as:
    - **Image**
    - **Excel**
    - **ASCII**

4. Click "Save."



The "Save" button

Once you have saved the auto-processing options, the files will not only be analyzed but also processed according to the defined settings. Proceed to the next step: Defining Communications Directory.

2.4 4 Defining Communications Directory

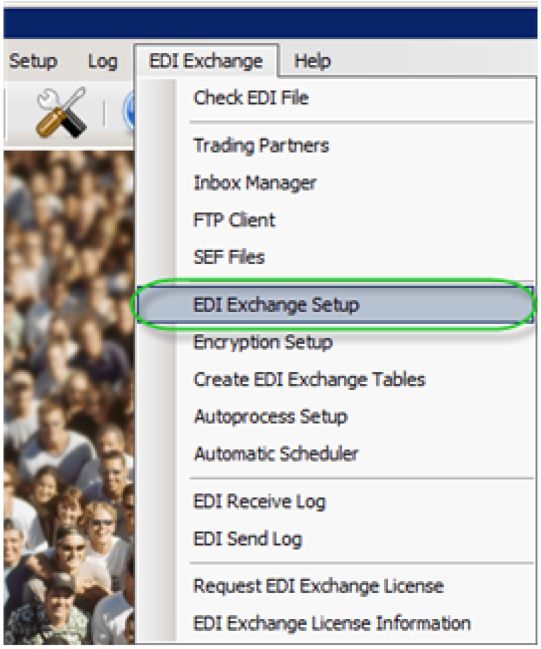
EDI file directory is an obligatory setting you need to set up before starting using the EDI Exchange. In order to keep track of the thousands of EDI files that accumulate over time, EDI Exchange uses a folder structure which we call the "HIPAAsuite Communications Directory" or "HIPAAsuiteCommDir" in short. In it, you will find all your EDI files sorted into several categories:

- **Inbox**
- **Outbox**
- **ProcessedFiles**
- **EncryptedFiles**
- **SuspendedFiles**

Within these directories, there will be folders for each Trading Partner and type of transactions. The location and names of the sub-folders are handled in the "Trading Partner Setup." See Setting up Trading Partners.

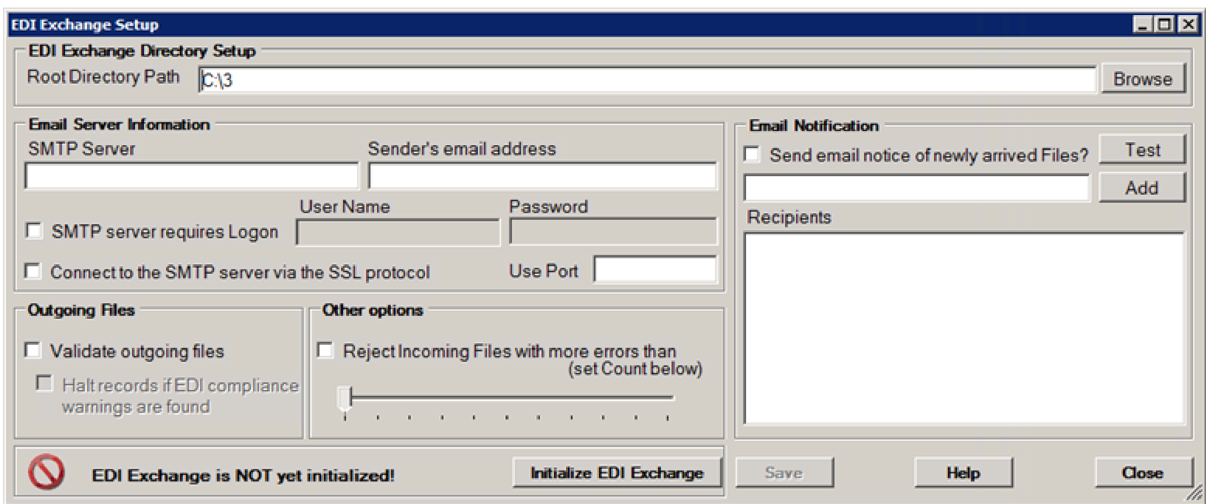
Follow the instructions below to specify EDI communications root directory.

1. Select "EDI Exchange Setup" under the "EDI Exchange" menu item.



The "EDI Exchange Setup" menu item

2. The following window will appear.

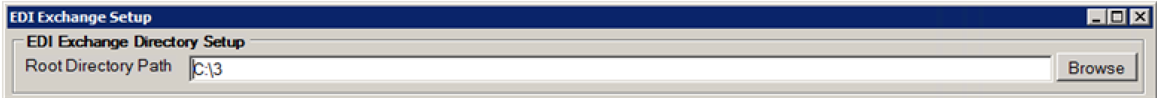


The "EDI Exchange Setup" window

> Note: The icon in the lower left corner indicates that EDI Exchange has not been initialized yet.

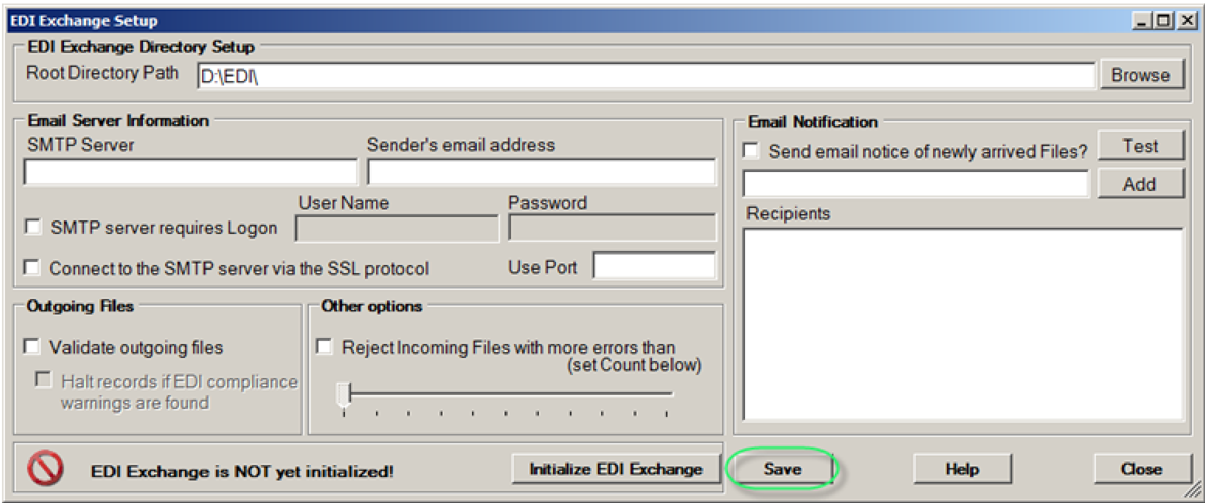
3. Under "EDI Exchange Directory Setup" specify the following setting:

   - **Root Directory Path** — Define the root path in the "Root Directory Path" text field. The root path is the folder where all your EDI files reside. EDI Exchange will later create sub-directories required to operate.



The root communications directory setup

4. Click "Save."



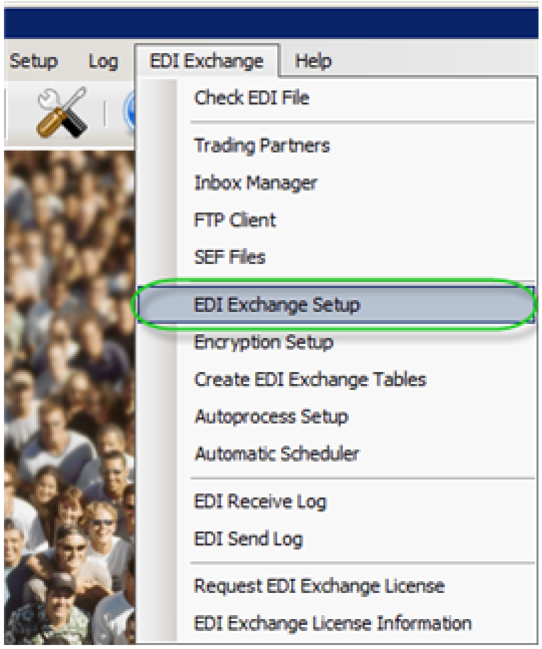
The "Save" button

After setting the root directory, you can click the "Initialize EDI Exchange" button. Read more in Initializing EDI Exchange.

2.5 5 Initializing EDI Exchange

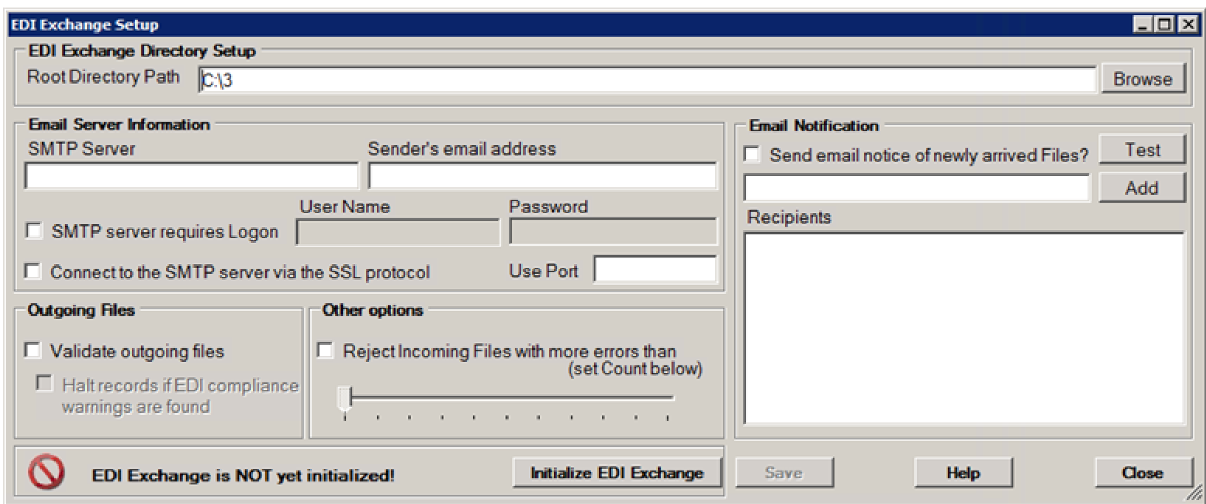
Before you can use EDI Exchange, and after you have configured the obligatory settings, you have to perform the initialization. Follow the instructions below.

1. Select "EDI Exchange Setup" under the "EDI Exchange" menu item.



The "EDI Exchange Setup" menu item

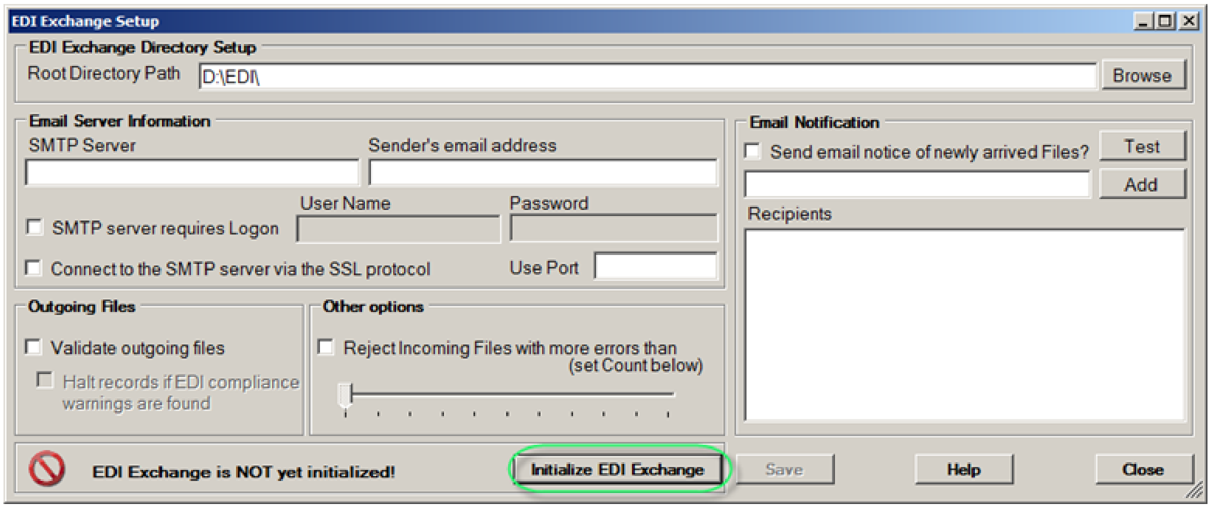
2. The following window will appear.



The "EDI Exchange Setup" window

> Note: The icon in the lower left corner, indicating that EDI Exchange has not been initialized yet.

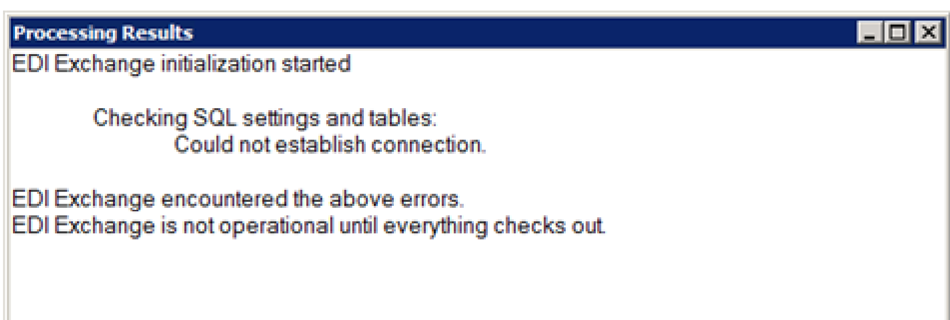
3. After setting the root directory (see the previous step Defining Communications Directory), you can initialize EDI Exchange module. Click the "Initialize EDI Exchange" button to accomplish the process.



The "Initialize EDI Exchange" button

Once the "Initialize EDI Exchange" button is clicked, the system checks if all settings have been configured correctly.

1. The first thing the initialization process checks is the connection to the database and the presence of the necessary tables. EDI Exchange relies on the database connection that is part of the HIPAAsuite application that you are using. EDI Exchange needs Database Connectivity licensed and enabled. If this part is not yet set up, then you will get an error like this:



Initialization failed because of SQL connection problems

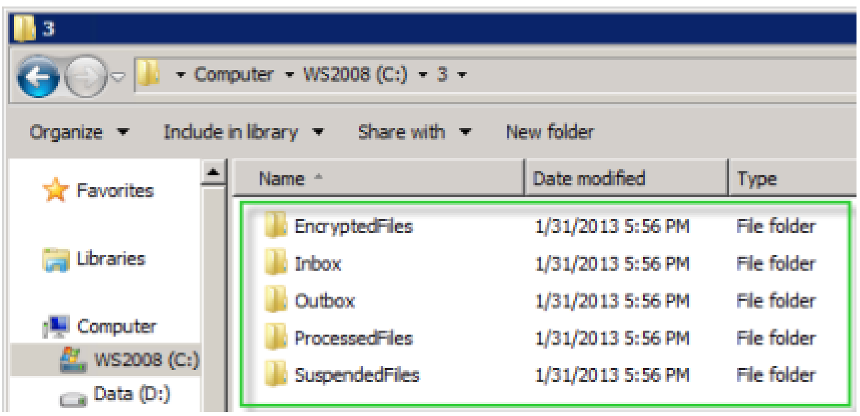
Read more in Setting up Database Connection.

2. Once the connection is established, the program checks if the correct tables exist in the database. See Creating Database Tables. Once the SQL part checks out, you will see the following message.

```
Checking SQL settings and tables:
          Connection settings are checked. Trading Partners table is checked.
          TRANS_LOG table is checked.
          TRANS_LOG_ERRORS table is checked.
          SEND_LOG table is checked.
```

3. The next step of the initialization processes — the program checks and, if necessary, creates the root directory and five sub-directories. Within these root directories, there will be folders for each Trading Partner and type of transactions. The location and names of the sub-folders are handled in the "Trading Partner" setup. The root folder is specified via the "EDI Exchange Setup" screen. Read more in Defining Root Directory.

   The sub-directories that EDI Exchange creates are as follows:

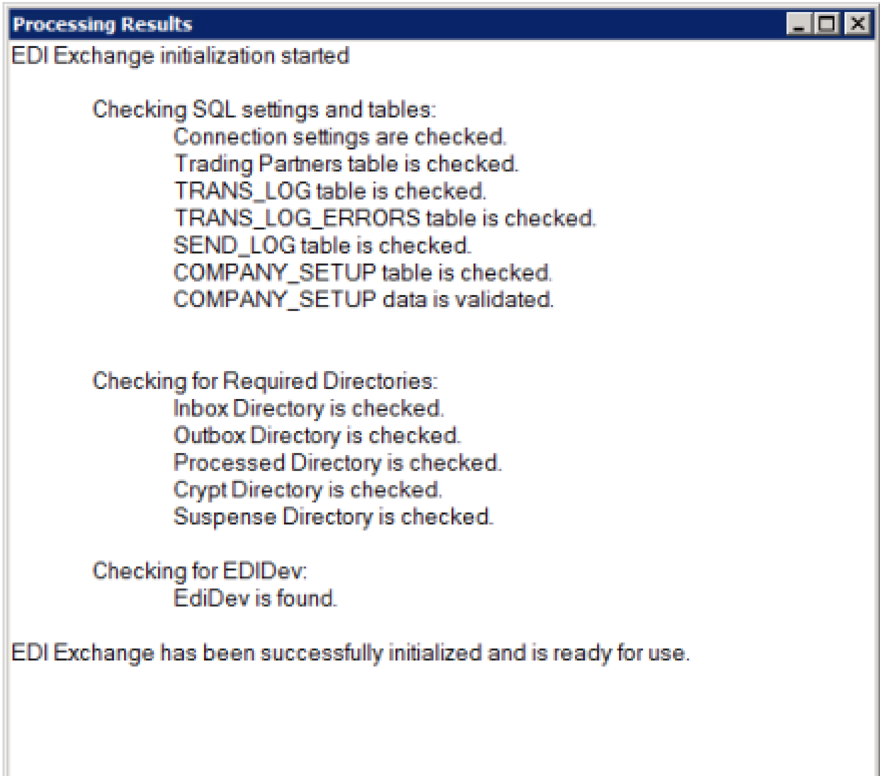


The directory structure of EDI Exchange

4. The next step of the initialization — the program checks if the HIPAA EDI compliance engine is properly installed.

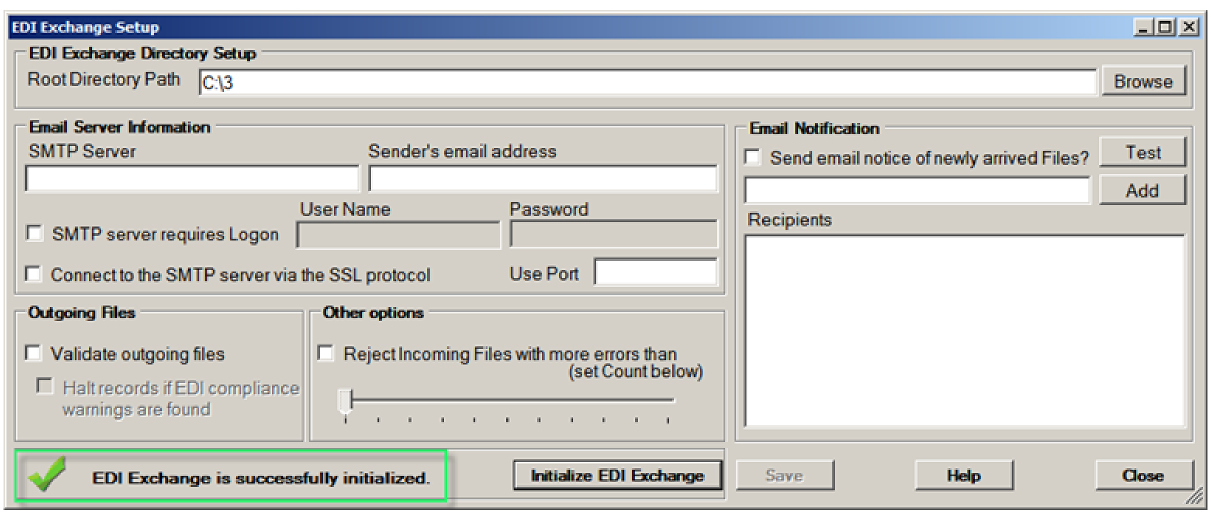
5. The last thing checked by the system is if the Automatic File Processing options have been set up. Read more in Defining Auto-Processing Options. The options are important for the hand over from EDI Exchange to the other HIPAAsuite program that hosts EDI Exchange.

Once all verifications have been completed successfully, you will see the following message:



Successful initialization of EDI Exchange

After that your EDI Exchange is initialized.



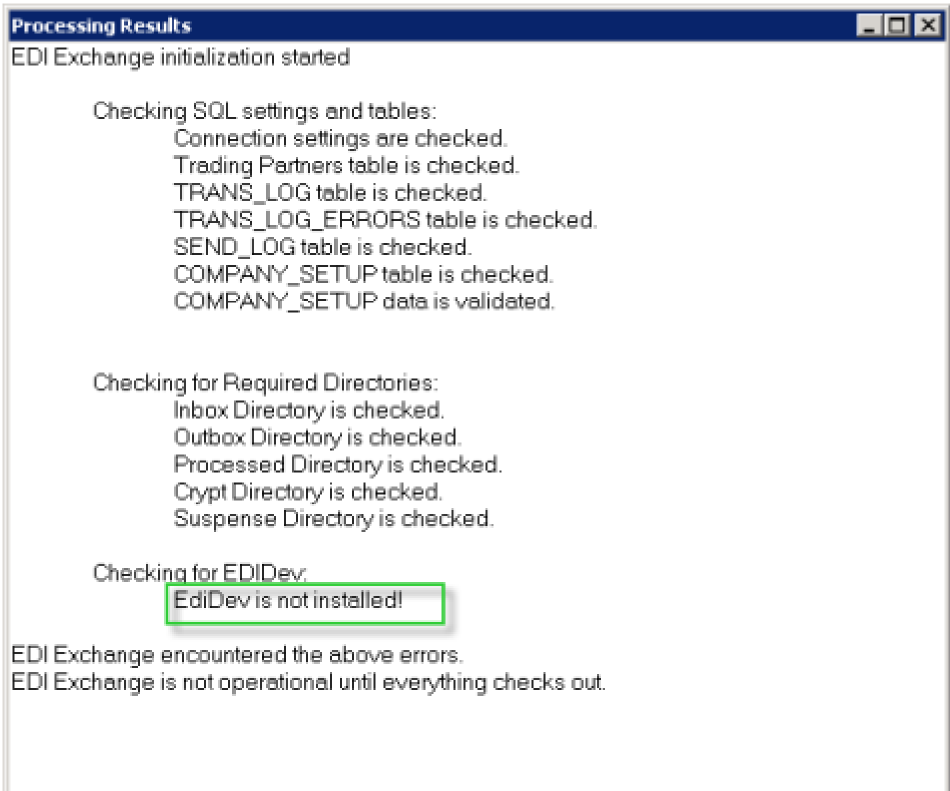
The "EDI Exchange is successfully initialized" message on the bottom of the "EDI Exchange Setup" window

Troubleshooting Initialization

When you are going through the Initialization process of the EDI Exchange, you can encounter the following message in the "Processing Results" window:

```
Checking for EDIDev:

EDIDev is not installed!
```

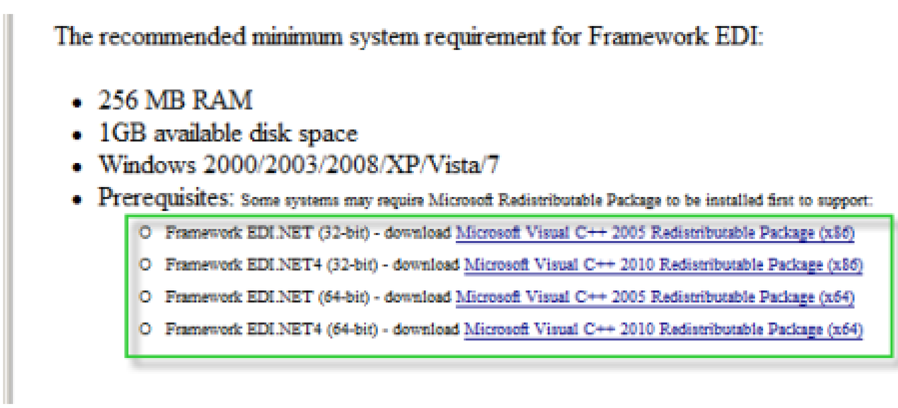


The EdiDev component is not installed

To resolve this issue, do the following.

1. Go to the http://www.edidev.com/ediregis.htm site.

2. Some systems may require Microsoft Redistributable Package to be installed first. In this case, download one of the following components according to your OS' bit depth.



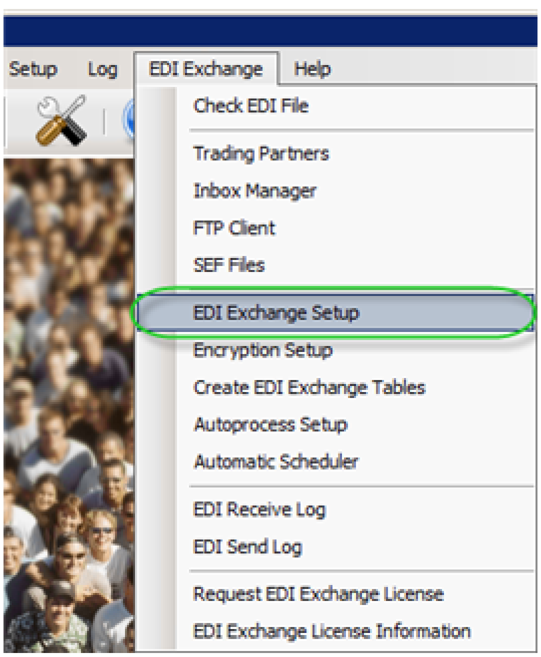
3. Download one of the following components you need according to your OS' bit depth:
   - Framework EDI Enterprise evaluation 32-bit
   - Framework EDI Professional evaluation 64-bit
4. Install downloaded components and start again the EDI Exchange initialization procedure.

3 Configuring EDI Exchange (Optional Settings)

3.1 Setting up Email Notifications

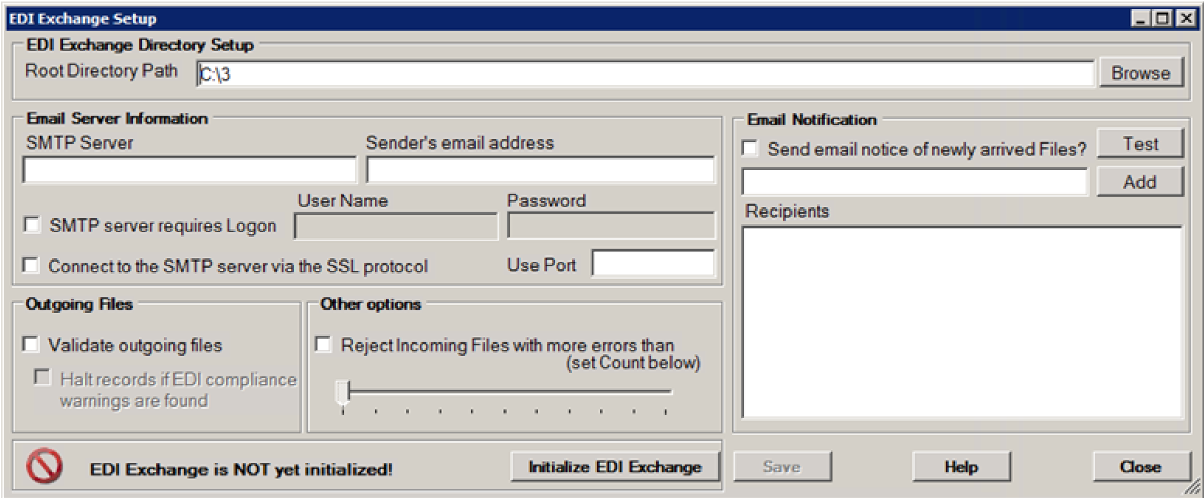
EDI Exchange can send emails to operators and trading partners to notify them about files and processing results. This functionality of EDI Exchange lies beyond the most basic setup that the initialization checks for. For this feature to work properly, you need to set up an email server which EDI Exchange communicates with. You can do this in the "Email Server Information" frame of the setup screen. Follow the instructions below.

1. Select "EDI Exchange Setup" under the "EDI Exchange" menu item.



The "EDI Exchange Setup" menu item

2. The following window will appear.

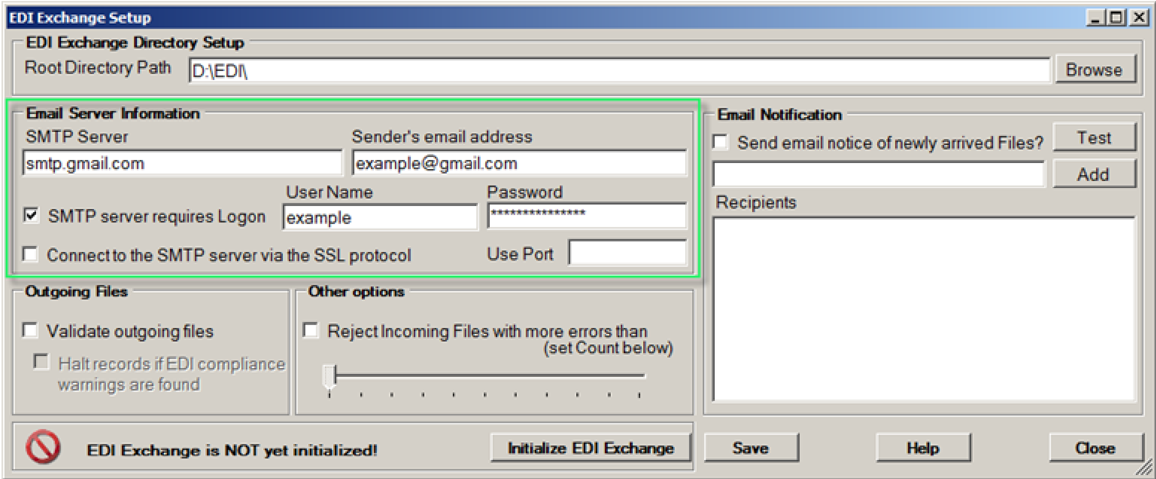


The "EDI Exchange Setup" window

3. Specify the following email options:

Email Server Information

- SMTP server
- Sender's email address
- SMTP server requires logon
- Username
- Password
- Connect to the SMTP server via the SSL protocol
- Use port



Setting up the email server

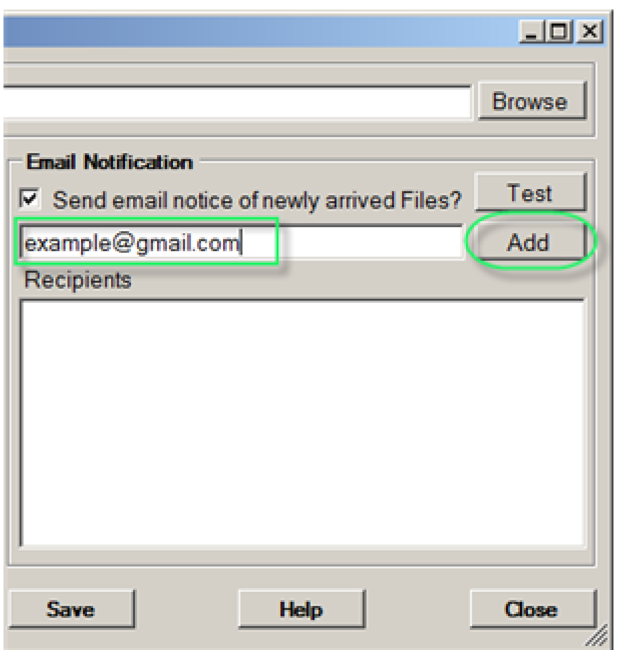
> Note: If you do not have this information, please ask your administrator to set this portion up for you.

4. To configure email notifications, specify the following options:

Email Notification

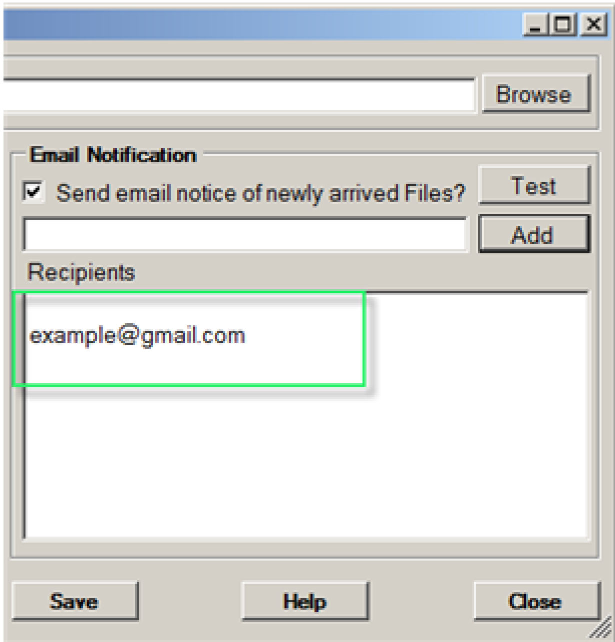
- **Send email notice of newly arrived files?** — Use this checkbox to define if you want to send email notice once new files have arrived.
- **Recipients** — You can add your staff's email(s) and the processing messages will be sent to these emails.

Enter an email address and click "Add."



Setting up the email recipients

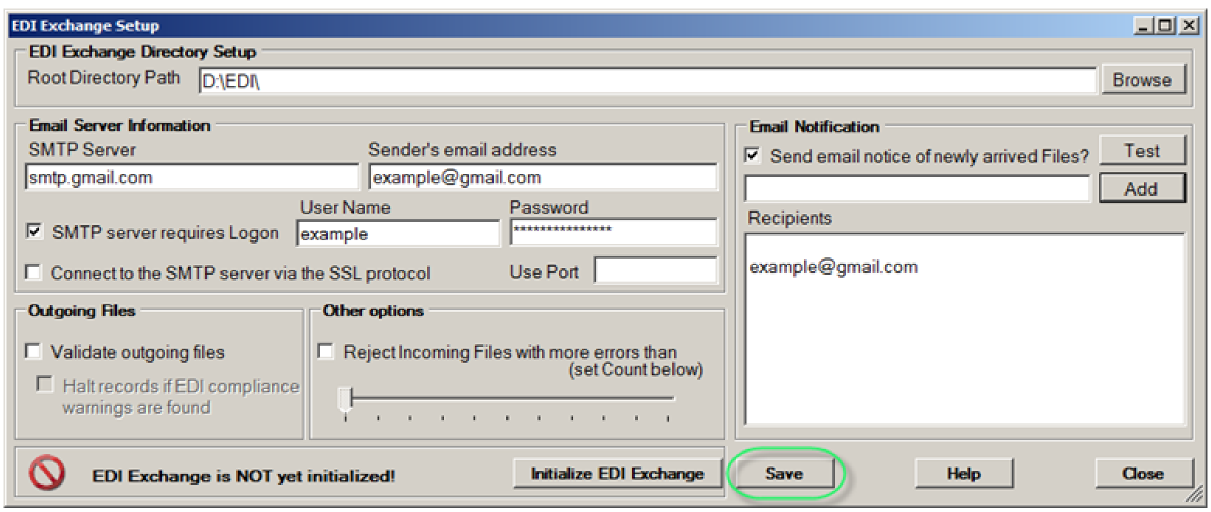
The email address will appear in the list.



Added email recipient

5. Click on the "Test" button to verify your settings.

6. Click on the "Save" button.



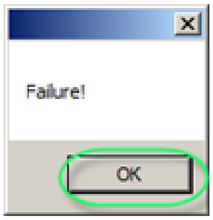
The "Save" button

Troubleshooting Email Settings

If you have problems with setting up the email server, please contact your administrator. He/

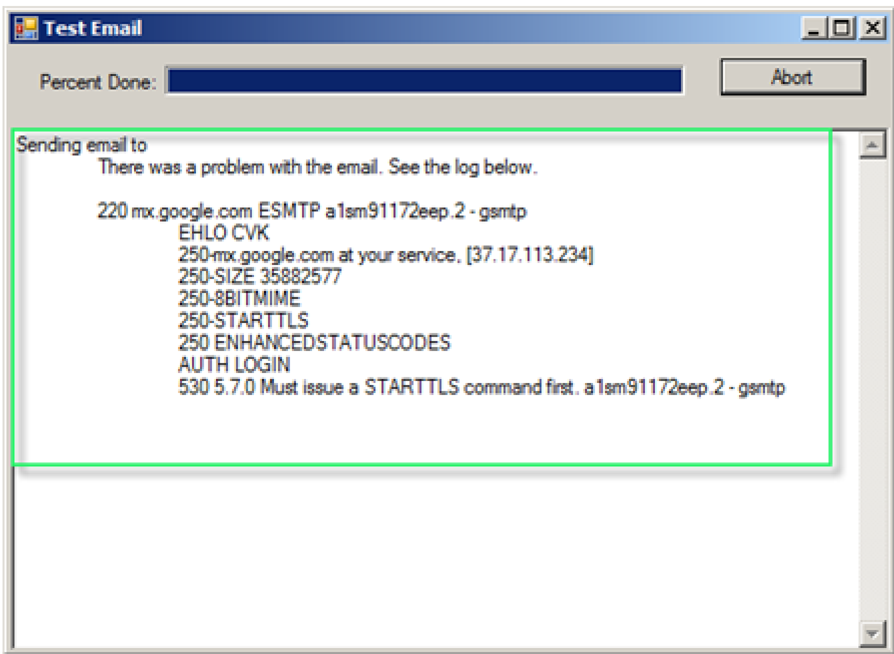
She should know values to specify and how to test the settings.

Below is an example of what happens when the email server does not respond.



After a time out, you get a failure notice

After acknowledging the failure, you get a more detailed error message in the process result screen.



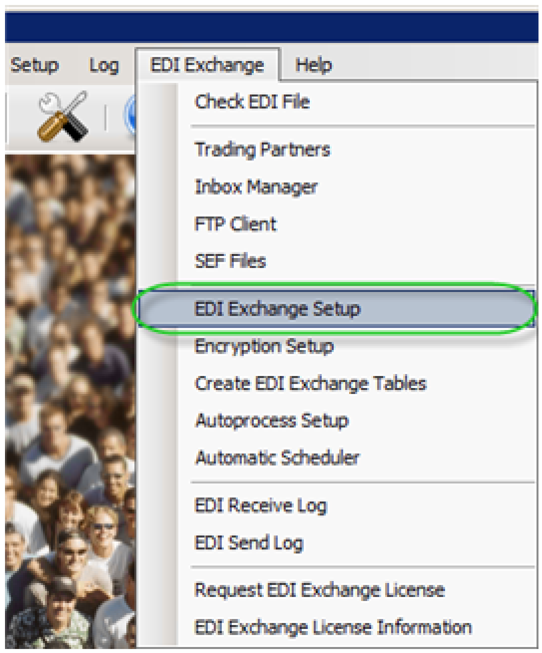
The process result screen with a detailed error message

3.2 Setting up Incoming and Outgoing Files Options

To check if your files are HIPAA-compliant, EDI Exchange can run a compliance check on outgoing EDI files. For incoming files, you can specify an acceptable error level. These settings are especially important with new trading partner relationships or with new processes since it always takes a while until an EDI process runs without issues and problems.

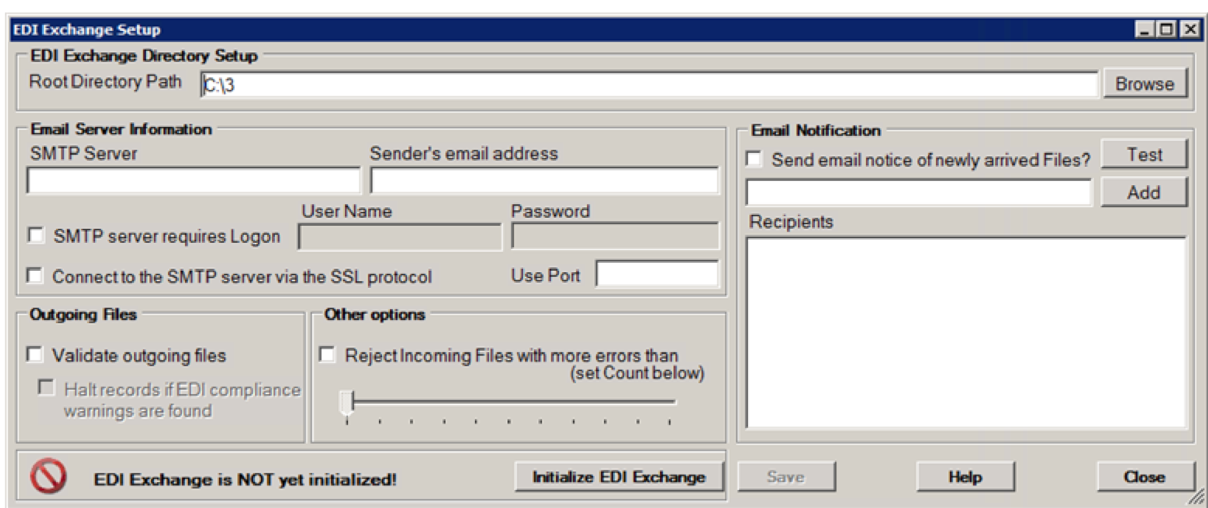
Follow the instructions below.

1. Select "EDI Exchange Setup" under the "EDI Exchange" menu item.



The "EDI Exchange Setup" menu item

2. The following window will appear.



The "EDI Exchange Setup" window

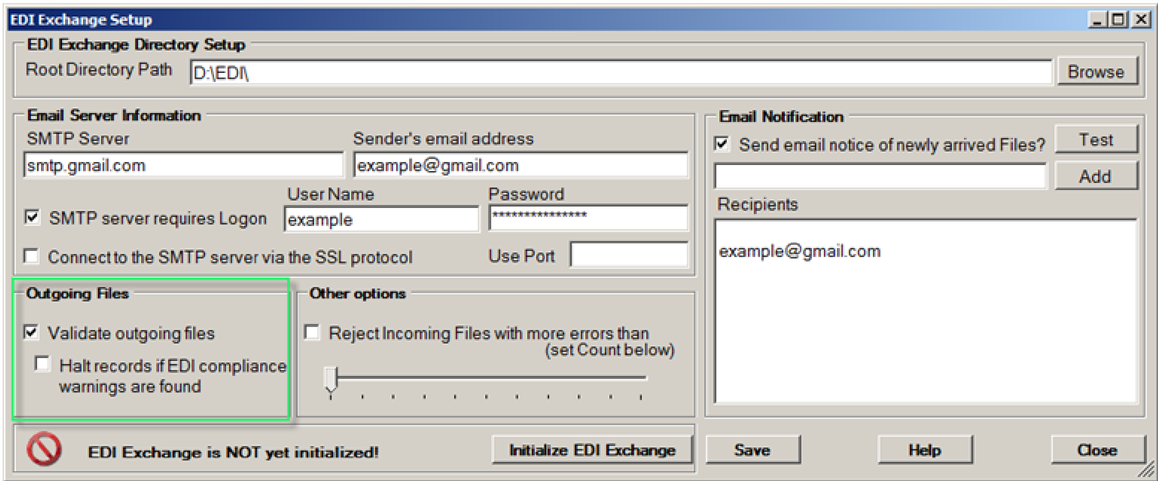
3. Specify the following outgoing files options:

Outgoing Files

- **Validate outgoing files** — Select this checkbox to validate if the outgoing files are

HIPAA-compliant.

- **Halt records if EDI compliance warnings are found** — Select this checkbox to suppress the sending of files with warnings or errors.

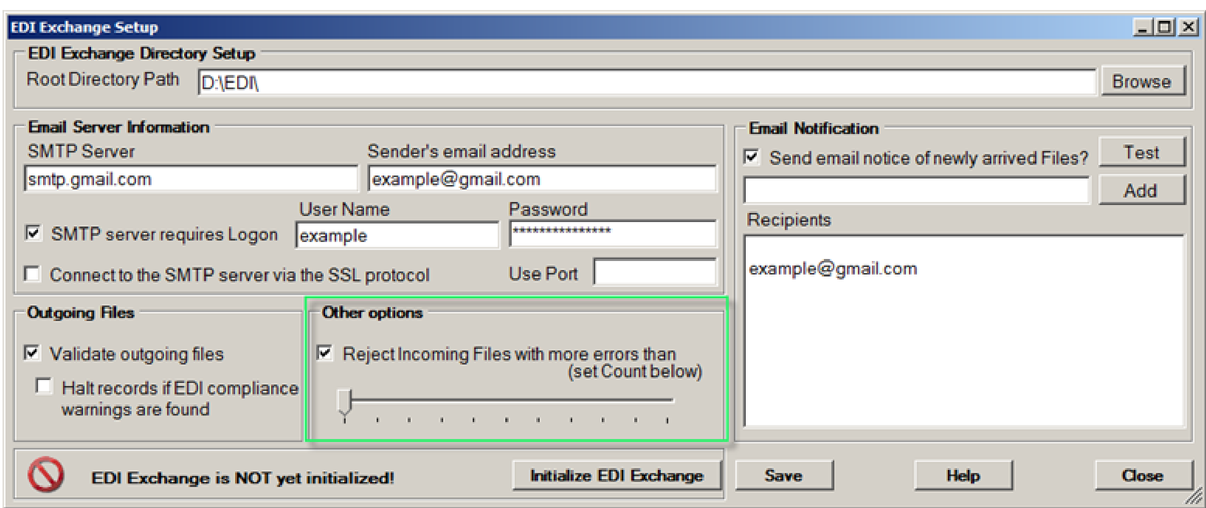


Validating outgoing files

4. Specify the following incoming files options:

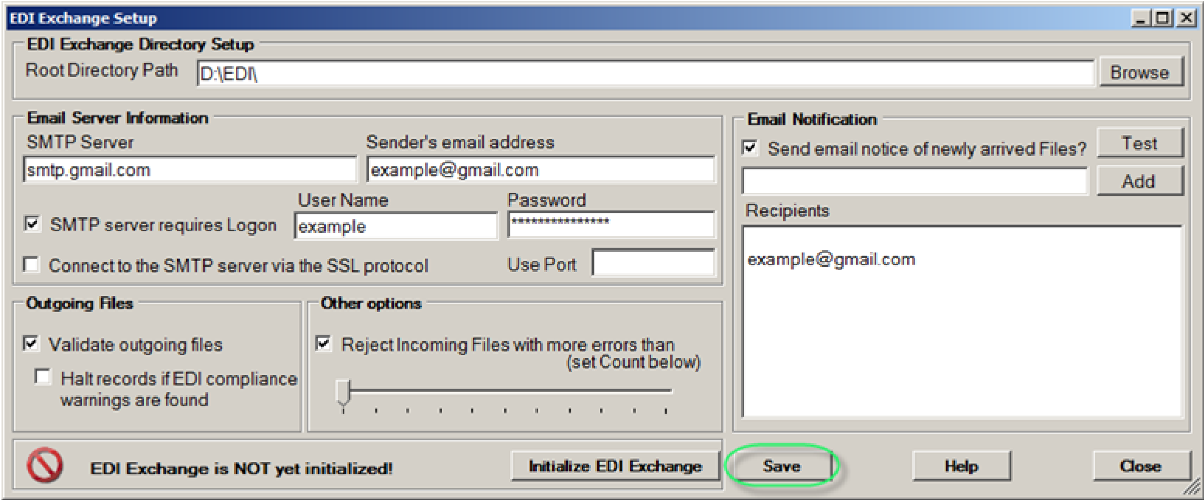
Other Options

- **Reject incoming files with more errors than (set count below)** — If checked, the incoming files with more errors than defined will not be placed into the "Inbox" folder.



The "Reject incoming files with more errors than" option

5. Click on "Save."

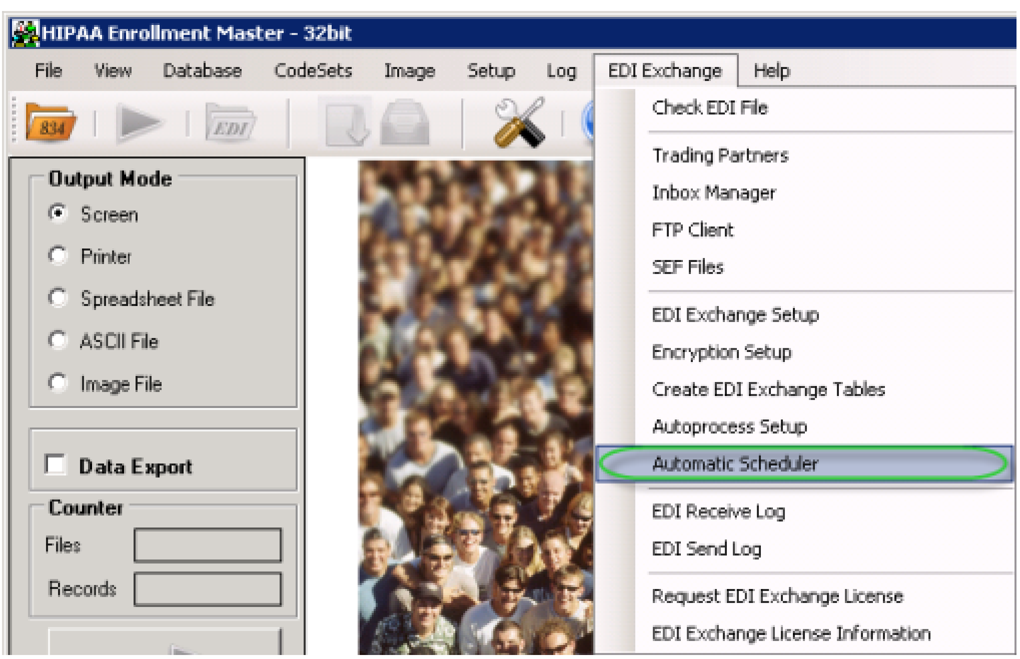


3.3 Running the Application via Scheduler

EDI Exchange integrates with the Windows Scheduler to allow the automation of the EDI file exchange process. You can set up EDI Exchange to go out to the trading partner's FTP server, download files, decrypt and compliance check them and further process them with the appropriate HIPAAsuite application, for example load claims into a SQL database.

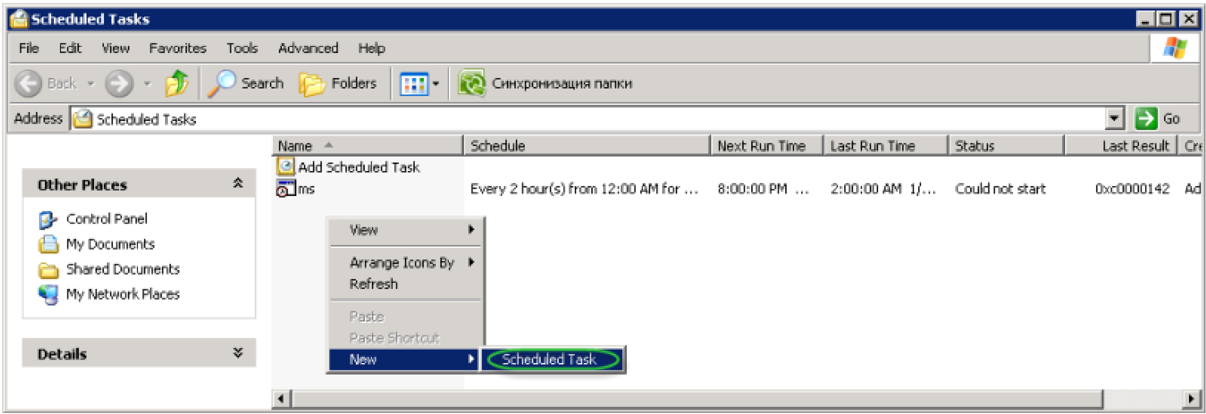
Follow the instructions below to schedule the EDI files exchange process.

1. Select "Automatic Scheduler" under the "EDI Exchange" menu.



The "Automatic Scheduler" menu item

2. In the opened window, right click and choose the "Scheduled Task" menu item.



The "Scheduled Task" menu item

See "Running the Application via Scheduler" in the help of the host HIPAA application for detailed instructions on how to schedule a task.

3.4 Using the Command Line Arguments (CLI)

Under construction.

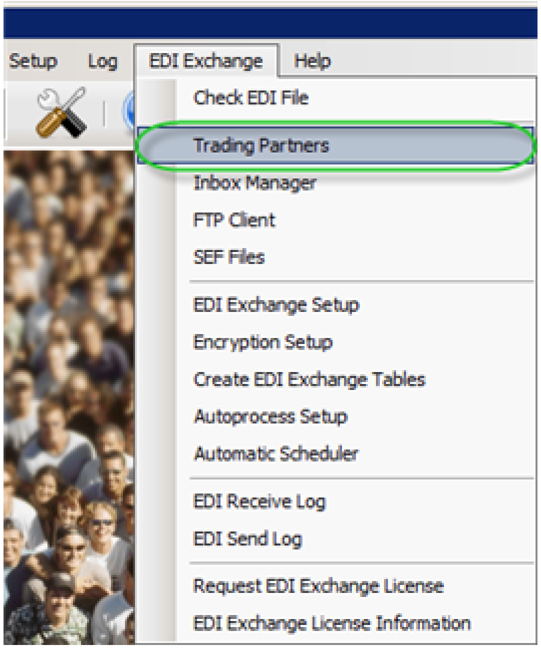
4 Working with Trading Partners

4.1 Setting up Trading Partners

With EDI Exchange you can keep track of your trading partners. You can set up their identifiers to send them EDI files or 999 acknowledgment, send email notifications and compliance check results, encryption keys and file transport mechanisms.

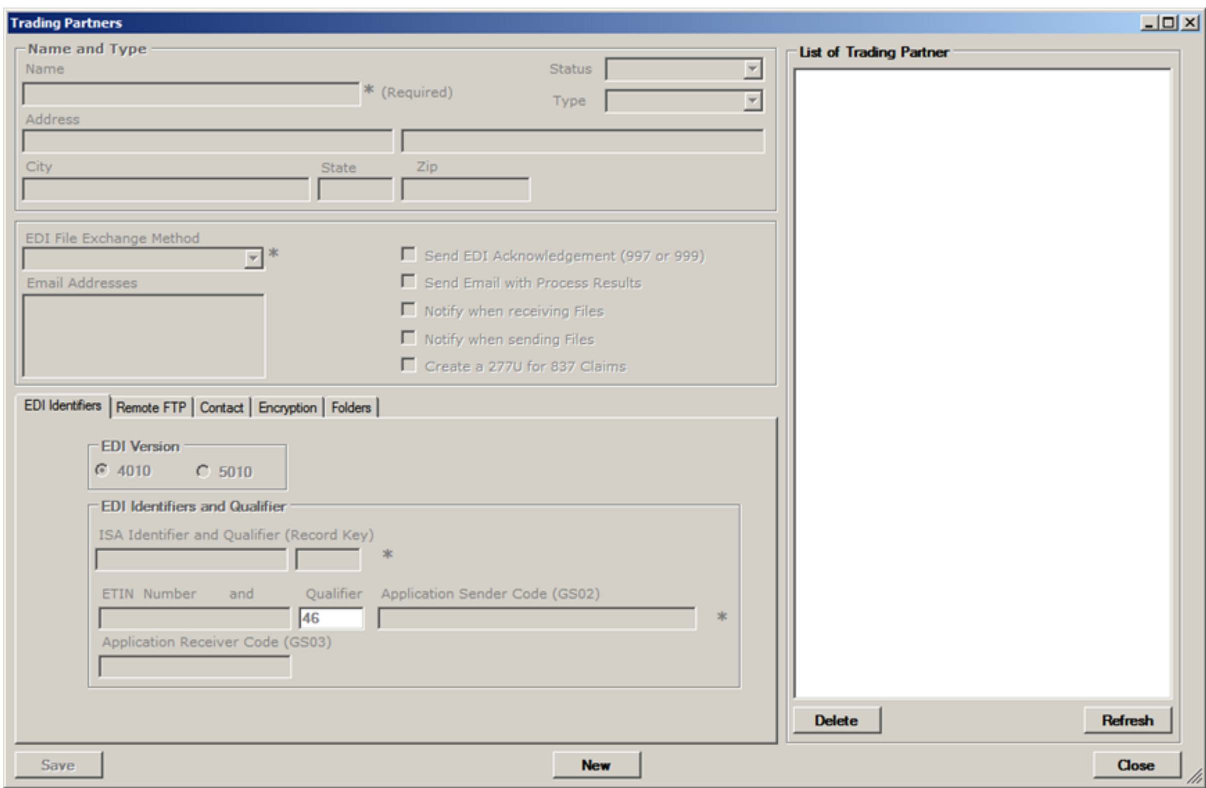
Once you have created the trading partner table (see Creating Database Tables) and initialized EDI Exchange (see Initializing EDI Exchange), you can set up the relationships with your trading partner. Follow the instructions below.

1. Select "Trading Partners" under the "EDI Exchange" menu.



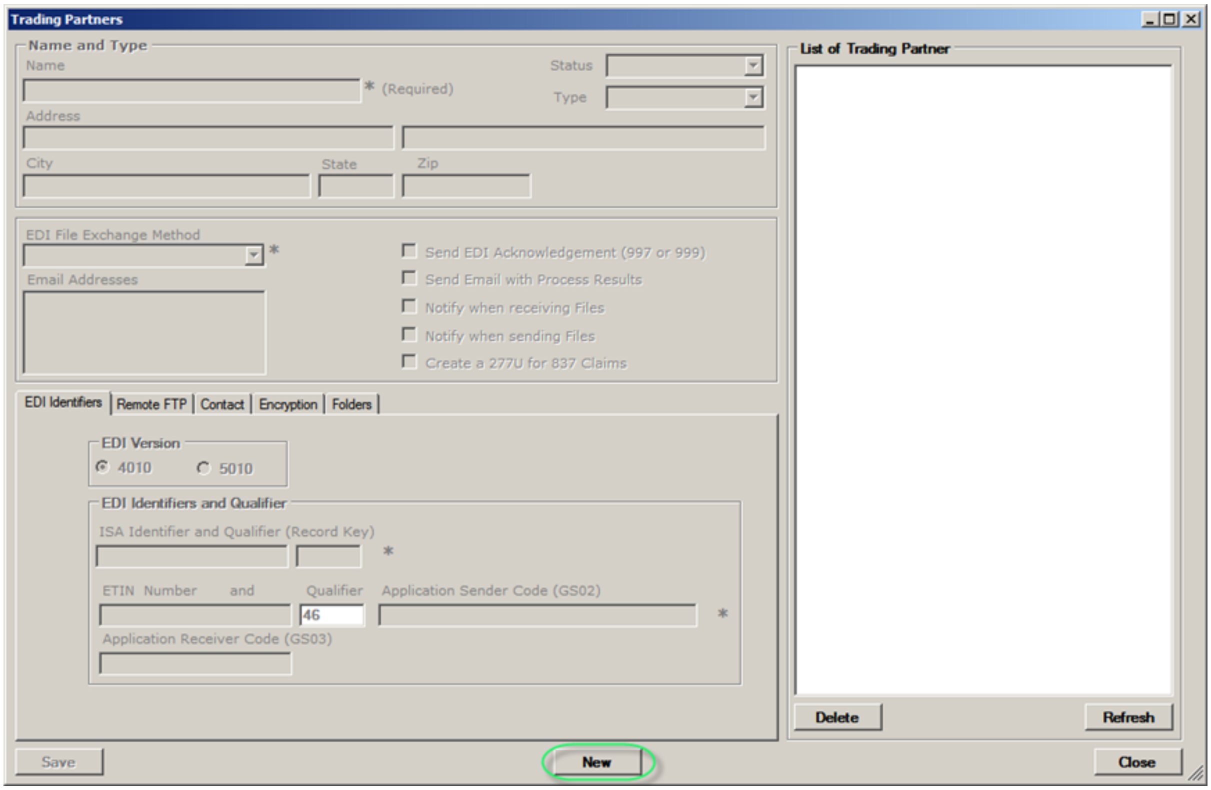
The "Trading Partners" menu item

2. The following screen will appear.

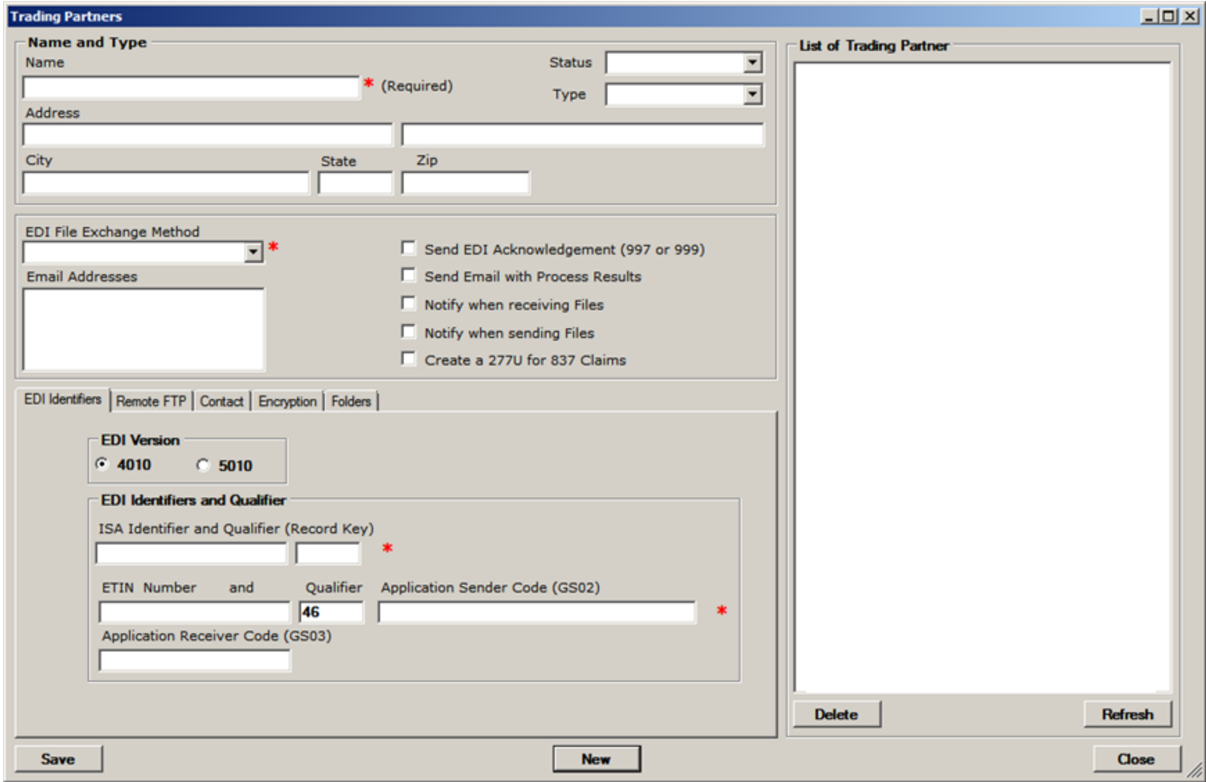


The "Trading Partners" window

3. Click the "New" button to start entering the trading partner information.



4. Define the necessary options. They are described further.



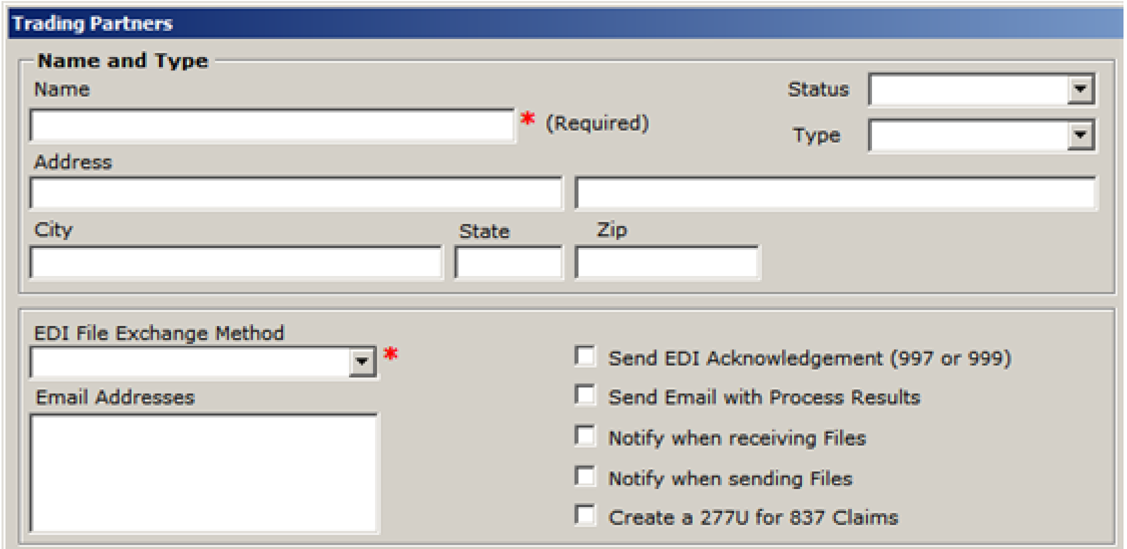
5. Click on "Save."

The "Save" button

6. The newly added Trading Partner's name will appear in the right pane.

Trading Partner Options

The company information of a trading partner can be specified on the top of the form.



Top area of the "Trading Partners" window

Name and Type

- **Name** — Trading partner's company name. Required field.
- **Address** — Trading partner's company address.
- **City**
- **State**
- **Zip**
- **Status** — Trading partner's status. Choose one of the available options:
  - **Inactive** — No upload into a database system through ODBC will be done.
  - **Test Only** — All outgoing EDI messages will be stamped with "Test" (ISA_15). Records will only be exported to the test environment.
  - **Approved** — All outgoing EDI messages will be stamped with "Production" (ISA_15). Records will be exported to the Life system with ODBC.
- **Type** — There are five types of trading partners, select the necessary one:
  - **Providers** — Hospitals, doctors or other health care providers.
  - **VANs** — Value Added Networks like clearing houses or EDI Networks.
  - **Service bureaus** — Third party entities such as repricing organizations.
  - **Sponsors** — Entities that sponsor the benefits of subscribers such as MedicAid, government agencies or large employers.

  - **Payers** — Entities that pay for health care benefits such as health insurers.

The next block on the form lists the communication methods and preferences.

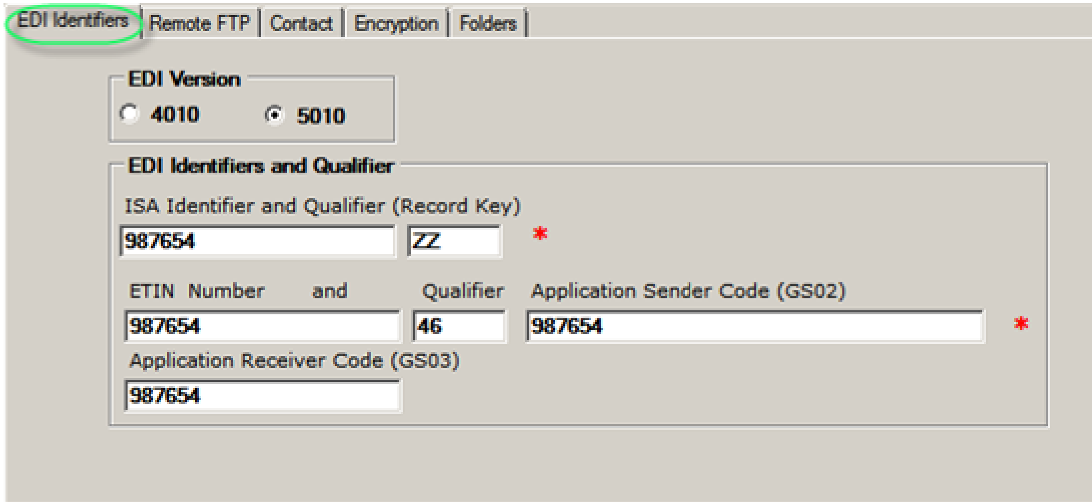
- **EDI File Exchange Method** — Obligatory setting. HIPAAsuite supports three communication methods. Choose a preferred mode of sending EDI communications to the trading partner:
  - **FTP** — Allows you to transmit files actively to the Trading Partner or his Clearinghouse.
  - **Outbox** — All files for Trading Partner are stored locally. The Trading Partner is responsible for picking up files in his special directory of the local FTP or HTTP server.
- **Email Addresses —** Enter the email address(es) into the text field.

You can also choose one of the following options:

- **Send Acknowledgment (997 or 999)** — This check-box allows sending Functional Acknowledgment transactions to the Trading Partner.
- **Send email with process results** — This option allows sending the compliance check results back to your contact at the Trading Partner via email. No PMI will be transmitted. Adding an email address is important, even when the Communication method is not "Email."
- **Notify when receiving files** — This option allows sending an acknowledgment email of EDI files. This option is not necessary when you choose 997 or 999 acknowledgments.
- **Notify when sending files** — This option allows sending a file to the Trading Partner notifying them that a file has been created for them.
- **Create a 277U for 837 claims** — This option does not apply to the Eligibility Responder.

EDI Identifiers Tab

This tab relates to the EDI identifiers and EDI Version.



The "EDI Identifiers" tab

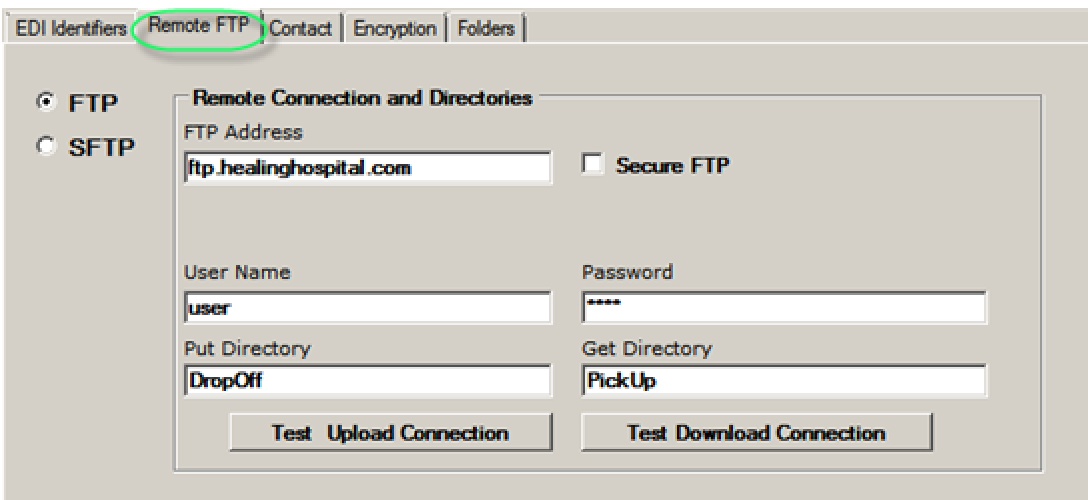
- **EDI Version —** There are two standards for HIPAA:
  - 4010 — This standard was introduced in the original transaction from 2003 to 2011.
  - 5010 — From 2012 on all HIPAA transactions must be conducted in the 5010 version.
- **EDI Identifiers and Qualifier**
  - **ISA Identifier and Qualifier (Record Key)** — The ISA Identifier and Qualifier are the unique key to the trading partner database file. The ISA identifier can be up to 15 bytes long, the qualifier has to be 2 bytes. Approved qualifiers are:
    - **01** — Duns (Dun and Bradstreet)
    - **14** — Duns Plus Suffix
    - **20** — Health Industry Number (HIN)
    - **27** — Carrier Identification Number as assigned by HCFA
    - **28** — Fiscal Intermediary Identification Number as assigned by HCFA
    - **29** — Medicare Provider and Supplier Identification Number as assigned by HCFA
    - **30** — U.S. Federal Tax Identification Number
    - **33** — National Association of Insurance Commissioners Company Code (NAIC)
    - **ZZ** — Mutually Defined. Many organizations use the ZZ qualifier with their name as the ID, for example ZZ and HIPAASUITE.

- **ETIN number** – The Electronic Transmitter Identification Number established by a Trading Partner Agreement. This number occurs only in the 837 transactions. Often, the ETIN is same as the ISA ID.

- **Application Receiver Code (GS_02)** – A code identifying a part that sends a transmission or the specific application within the sender's organization. Codes are agreed by Trading Partners. Again, usually this code is same as the ISA ID. This code is placed in the GS_02 element in the Functional Group Header (GS). Some Trading Partners want to send a specific code in GS_03, the application receiver code. You can enter it into the corresponding field. Most of the time it is not necessary.

Remote FTP Tab

If your trading partner has an FTP Server, then you can set up here the connection information. Read more in Using Built-in FTP Client.



The "Remote FTP" tab

- **FTP**

- **SFTP –** For security reasons, EDI Exchange supports secure FTP or FTPs.

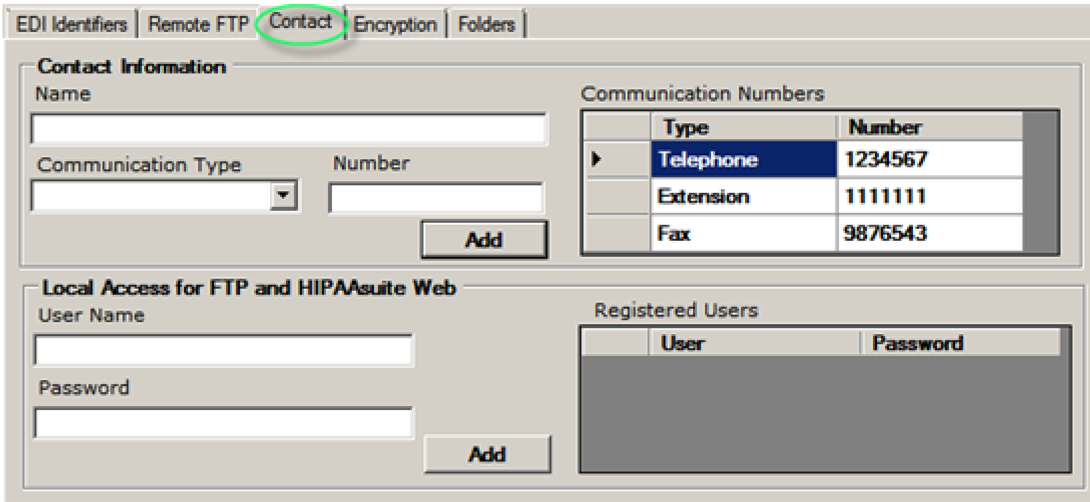
Remote Connection and Directories

You need the FTP address, the user name and password to establish the connection and the directory information where files are picked up and where dropped off. Fill in the following fields:

- **FTP Address**

- **Secure FTP —** Secure FTP comes in two modes:
  - **Explicit FTPS Connection** — The explicit method is a legacy compatible implementation where FTPS aware clients can invoke security with an FTPS aware server without breaking overall FTP functionality with non-FTPS aware clients. In explicit mode (also known as FTPS), an FTPS client must "explicitly request" security from an FTPS server and then step-up to a mutually agreed encryption method. If a client does not request security, the FTPS server can either allow the client to continue insecure or refuse/limit the connection.
  - **Implicit FTPS Connection** — The implicit method requires that all clients of the FTPS server be aware that SSL is to be used on the session, and thus is incompatible with non-FTPS-aware clients. Negotiation is not allowed with implicit FTPS configurations. A client is immediately expected to challenge the FTPS server with a TLS/SSL ClientHello message. If such a message is not received by the FTPS server, the server should drop the connection. In order to maintain compatibility with existing non-TLS/SSL aware FTP clients, implicit FTPS was expected to listen on the IANA Well Known Port 990/TCP for the FTPS control channel and 989/TCP for the FTPS data channel. This allowed administrators to retain legacy compatible services on the original 21/TCP FTP control channel.
- **User Name**
- **Password**
- **Put Directory**
- **Get Directory**

Contact Tab



The "Contact" tab

Contact Information

Enter the name and the number into the corresponding fields and select the communication type from the drop-down list.

- **Name**
- **Communication Type**
- **Number**
- **Communication Numbers** — Valid Communication number qualifiers are:
  - **TE** — Stands for Telephone.
  - **FX** — Stands for Fax.
  - **EX** — Stands for Extension.
  - **EM** — Stands for email.

Click the "Add" button and the contact will appear in the "Communication Numbers" table.

> Note: The information that you fill in goes also into EDI files in the "PER" segment.

Local Access for FTP and HIPAAsuite Web

To register a user, enter the user name and the password into the corresponding fields and click the "Add" button. The user will appear in the "Registered Users" table.

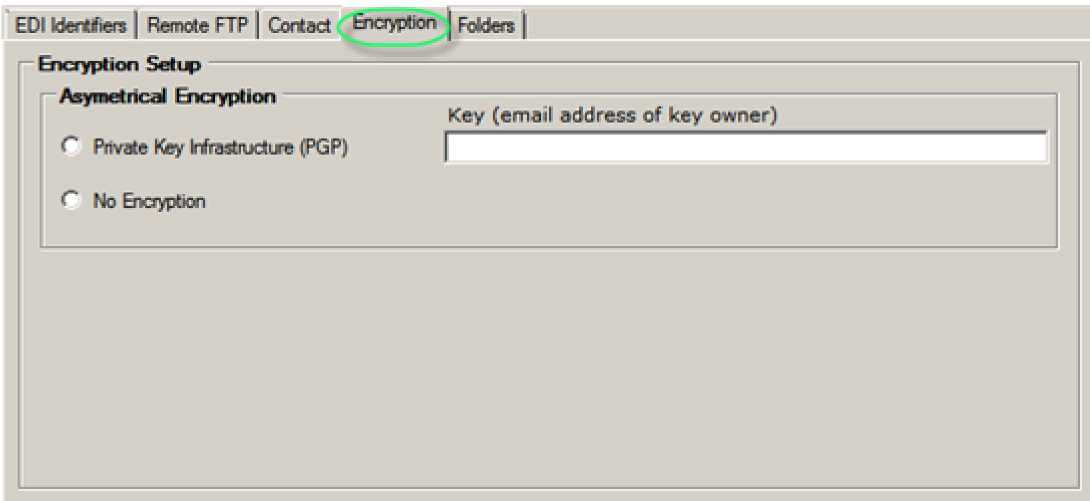
- **User Name**
- **Password**

- **Registered Users**

Encryption Tab

EDI Exchange supports PKI encryption. Encryption keys are defined by the email address of the owner. Both supported products, PGP and GnuGP use this logic. Read more in Using Encryption.

You can set up the encryption parameters for a Trading Partner on the "Encryption" tab.



The "Encryption" tab

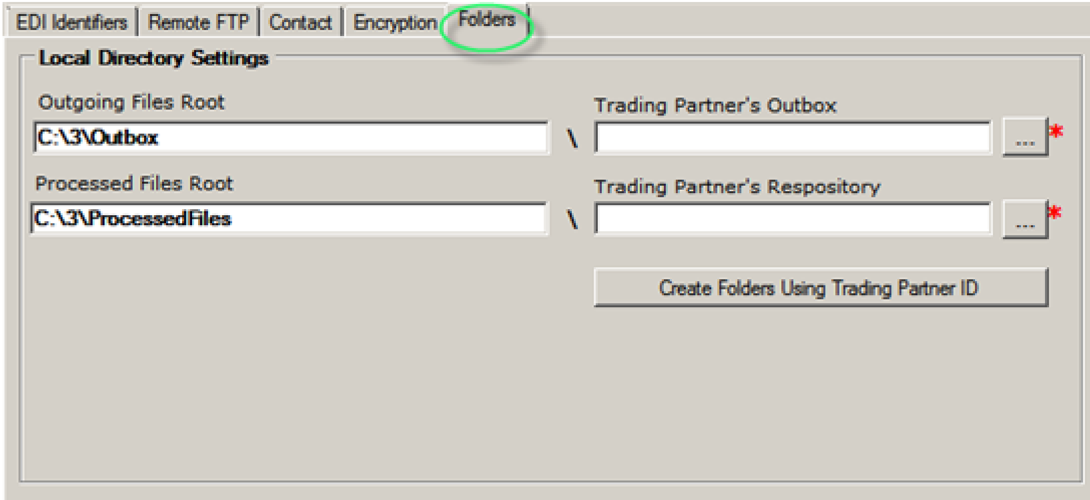
Encryption Setup

- **Asymmetrical Encryption**
  - **Private Key Infrastructure (PGP)**

    Key (email address of key owner)
  - **No Encryption**

Folders Tab

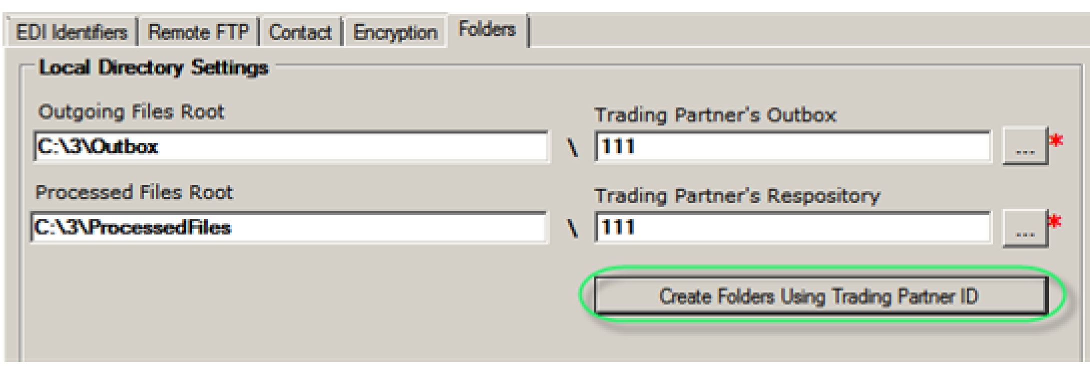
Within the HIPAAsuite Communications Directory, each Trading Partner has his own folder. This keeps files finely separated and in order. Here is where you can set this up. Read more in Defining Communications Directory.



The "Folder" tab

- **Outgoing Files Root** — This field has a pre-generated path. You can change this path.
- **Trading Partner's Outbox** — Mandatory setting. Click on the three-dots button to access the "Select Folder" window. There you choose an existing folder or create a new one.
- **Processed Files Root —** This field has a pre-generated path. You can change this path.
- **Trading Partner's Repository —** Mandatory setting. Click on the three-dots button to access the "Select Folder" window. There you choose an existing folder or create a new one.

Once you have specified the directory settings, click on the "Create Folders Using Trading Partner ID."



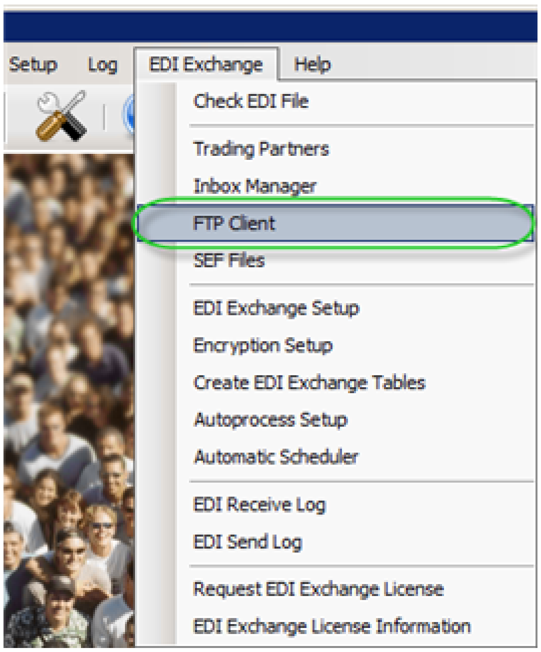
The "Create Folders Using Trading Partner ID" button

4.2 Using Built-in FTP Client

EDI Exchange has a built-in FTP client. This utility allows you to drop-off and pick-up files from a trading partner that you have defined in the "Trading Partners" menu (see Setting up Trading Partners.)

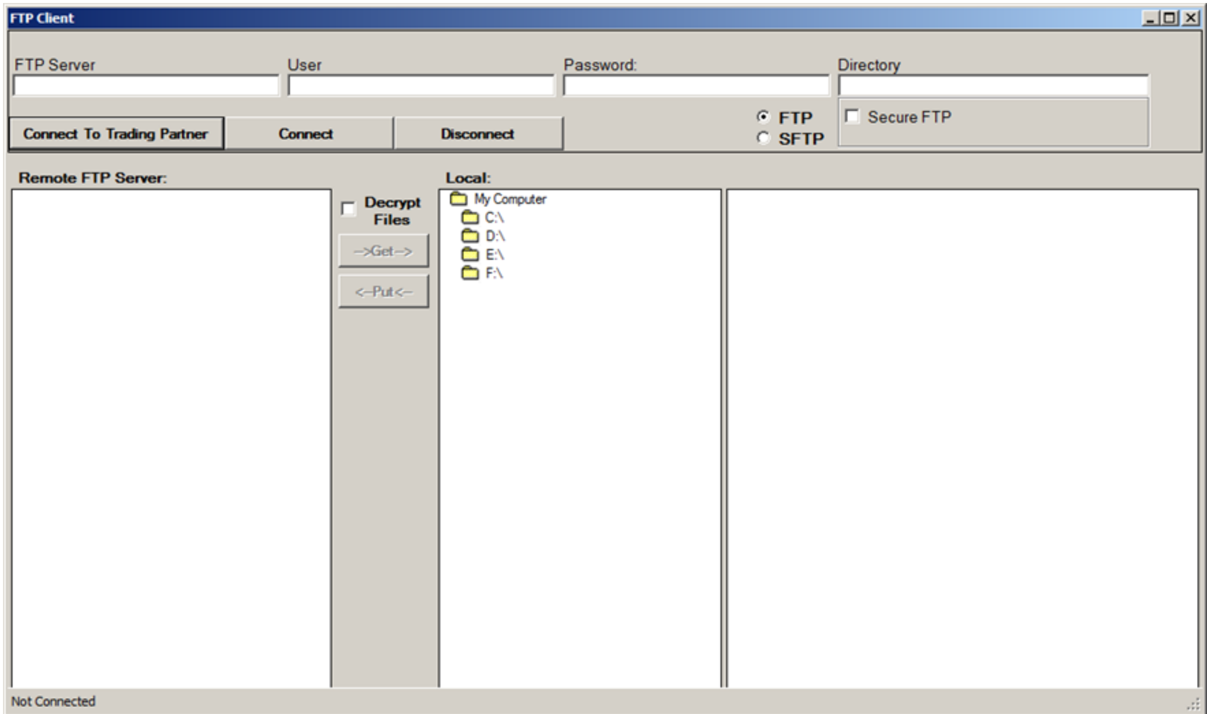
Follow the instructions below to exchange EDI files with your Trading Partner.

1. To access the FTP client, select "FTP Client" under the "EDI Exchange" menu item.



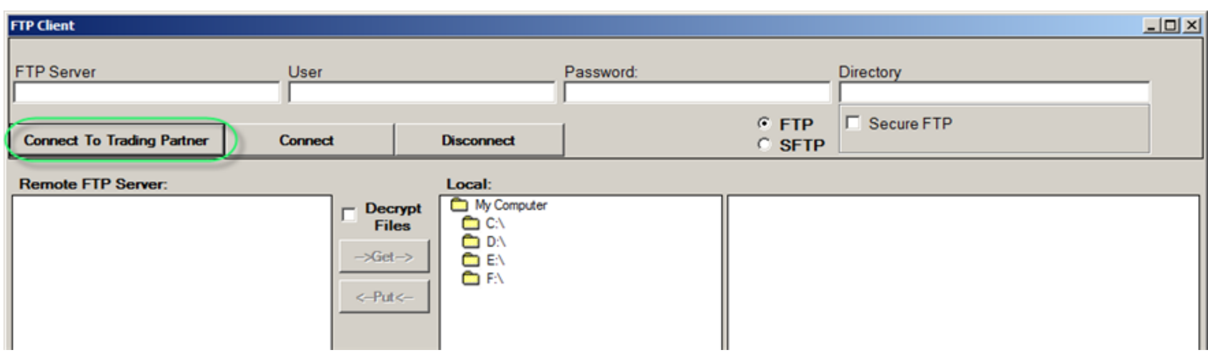
The "FTP Client" menu item

2. The following window will appear.



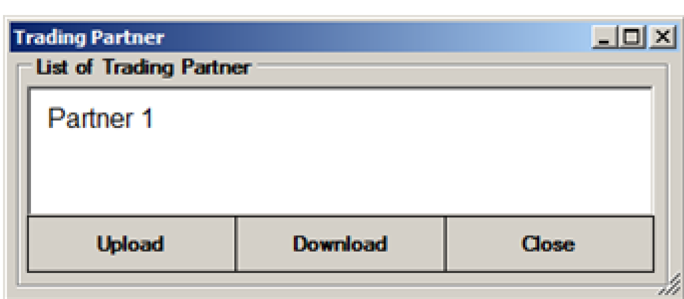
The built-in FTP client

3. Click the "Connect to Trading Partner" button on the FTP client window.



The "Connect to Trading Partner" button

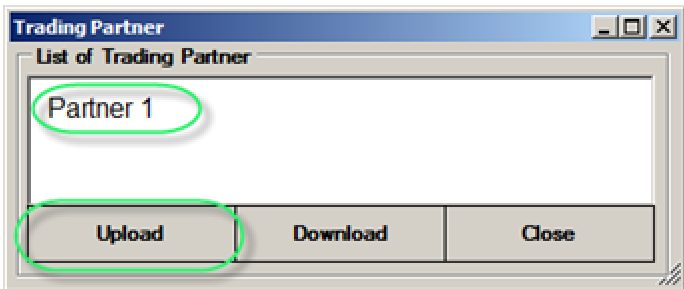
4. The following screen opens.



Selecting a Trading Partner for FTP transfer

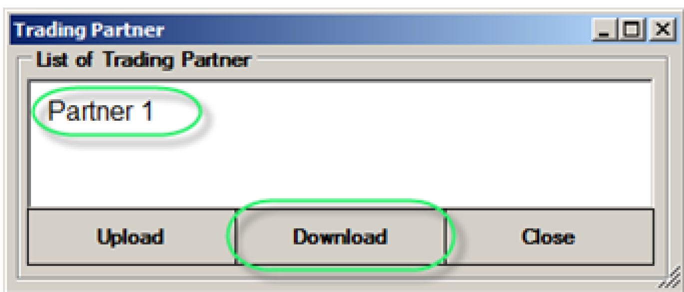
5. Highlight the trading partner that you want to connect to.

6. Click on the "Upload" button to connect to the "Put" directory that you set up in the trading partner screen.



The "Upload" button

Or click on the "Download" button to connect to the "Get" directory that you set up in the trading partner screen.

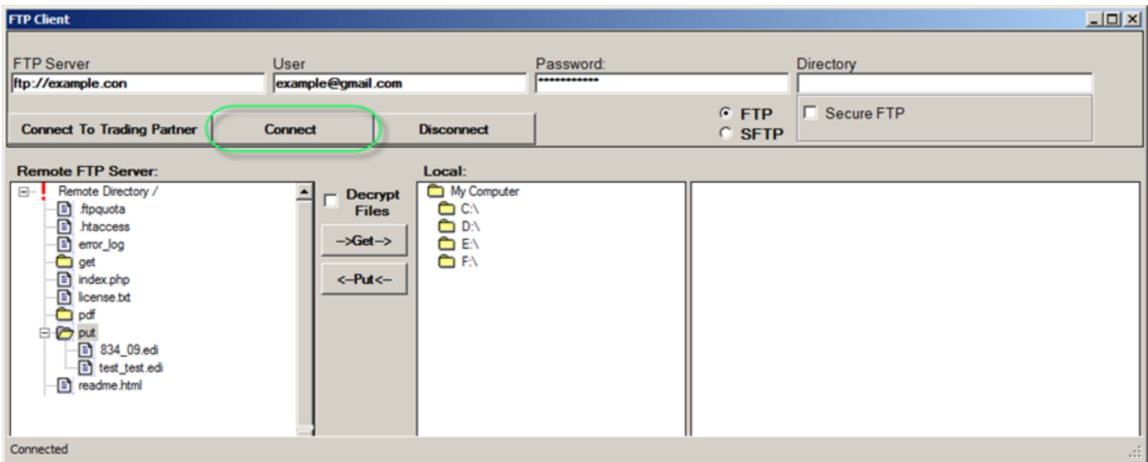


The "Download" button

5. Once you have chosen a trading partner, the following fields will contain values derived from the trading partner's properties. You can change them manually if you need.

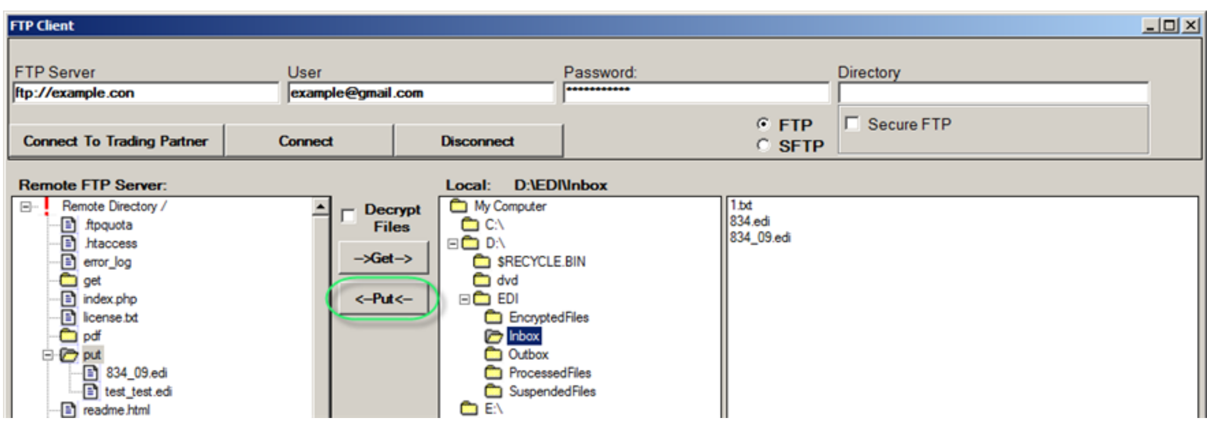
- **FTP server** — IP Address or URL of the FTP server.
- **Username**
- **Password**
- **Directory —** If you leave this value blank, the FTP root directory will be opened.
- **Secure FTP** — If you enable this option, then you can select between implicit and explicit FTPs. See Setting up Trading Partners for an explanation of the two secure methods:
  - **Explicit FTPS Connection**
  - **Implicit FTPS Connection**

Note: You can also fill in the connection information manually. In this case, the entered credentials will not be saved once you close the FTP client window. Click on the "Connect" button to establish connection to the FTP server.

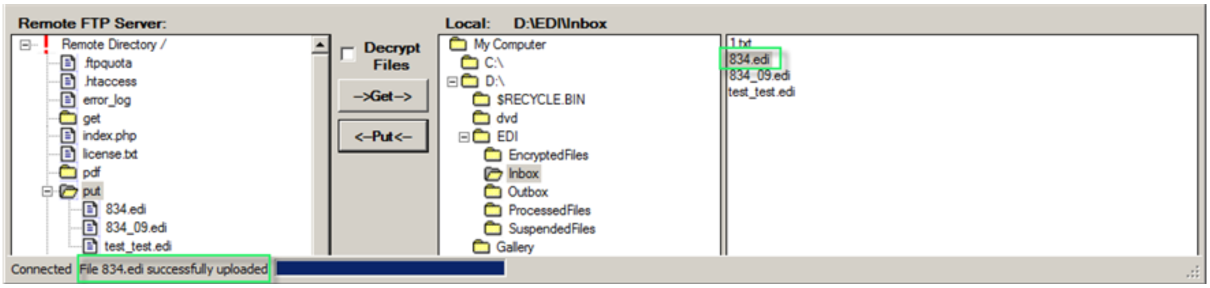


4. Once connected, the content of the folder on the server is displayed. On the right side, you can browse your local PC.

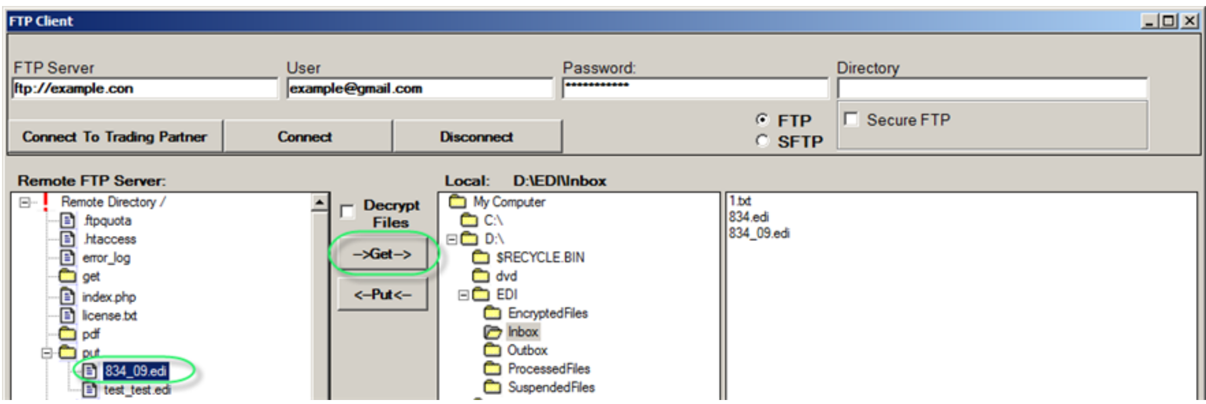
5. To upload a file to the server, select the file on your local PC and click on the "Put" button.



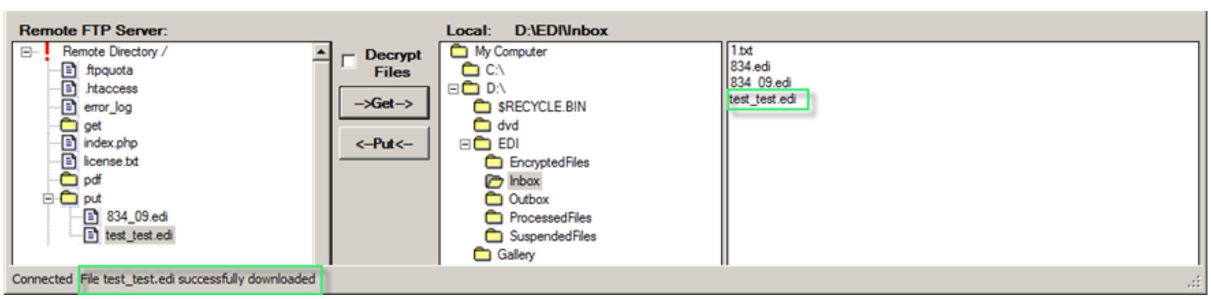
The file will appear in the remote folder. You will receive the "File <filename> successfully uploaded" message on the bottom status bar of the FTP client.



6. To download a file from the server, select a file in the left side, and then click on the "Get" button.

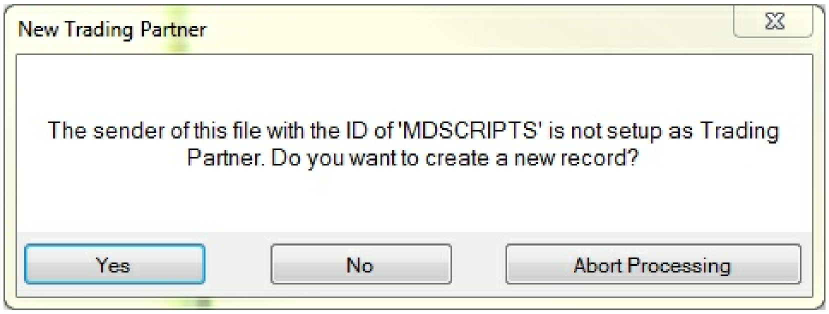


The file will appear in the local folder. You will receive the "File <filename> successfully downloaded" message on the bottom status bar of the FTP client.



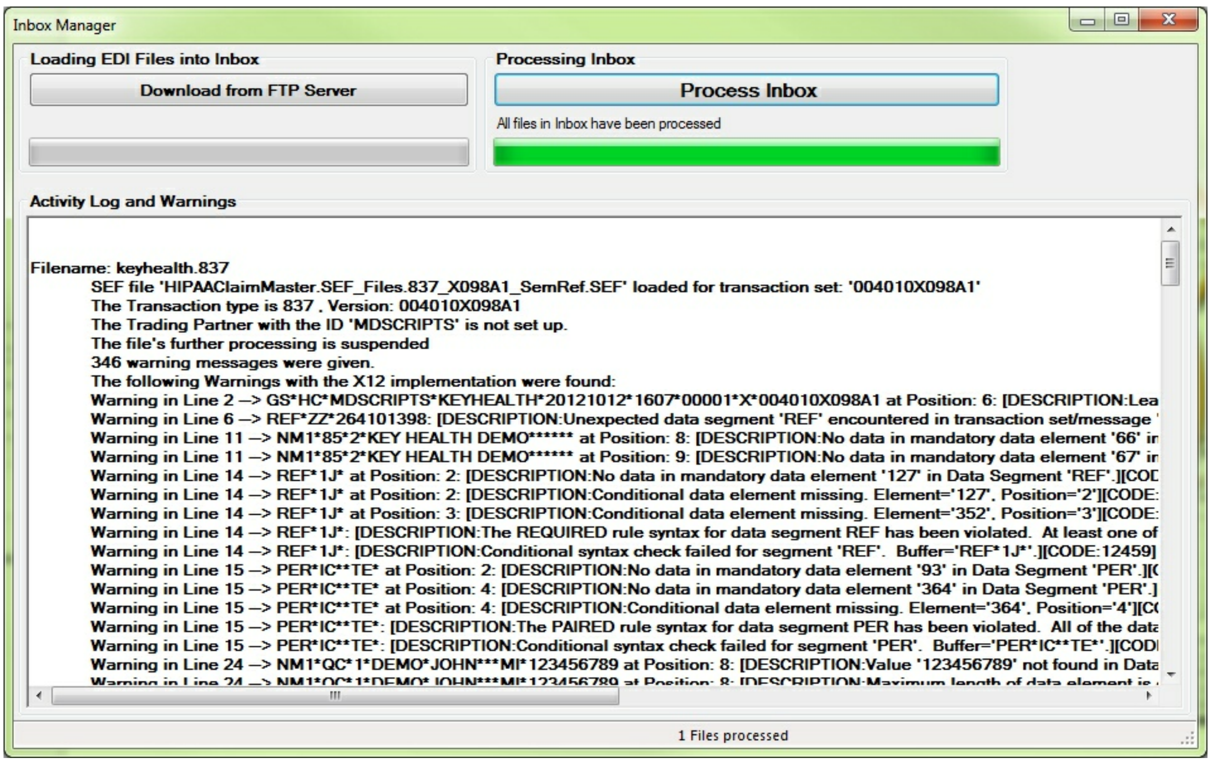
4.3 Creating a Trading Partner Automatically

When you process a file with EDI Exchange the sender's ID is compared to the trading partners on file. If the trading partner does not exist you have the opportunity to create a rudimentary new trading partner record. Now you have the choice to either create this new record, process the file without the trading partner record or to abort the operation.



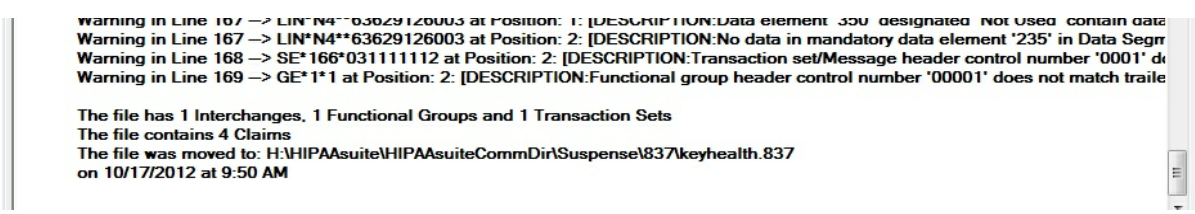
The "New Trading Partner" dialog box

If you abort the process, you still will get the EDI file analysis.



EDI compliance check results after further processing was aborted.

Files without a valid trading partner will be placed into suspension. The final action taken after the analysis is recorded at the end of the results.



This file's processing was aborted. The file was moved to the suspense folder

5 Using Encryption

5.1 About Encrytion

EDI Exchange supports the **Private Key Infrastructure** (PKI) encryption method. This type of encryption is the most generally accepted method of protecting EDI Files from being pried upon by unauthorized persons. Without going further into the details of PKI, Public-key encryption is a cryptographic technique which enables users to securely communicate on an insecure public network, and reliably verify the identity of a user via digital signatures. Read more in Private Key Infrastructure.

A public-key infrastructure (PKI) is a system for the creation, storage, and distribution of digital certificates which are used to verify that a particular public key belongs to a certain entity. The PKI creates digital certificates which map public keys to entities, securely stores these certificates in a central repository, and revokes them if needed.

A PKI consists of:

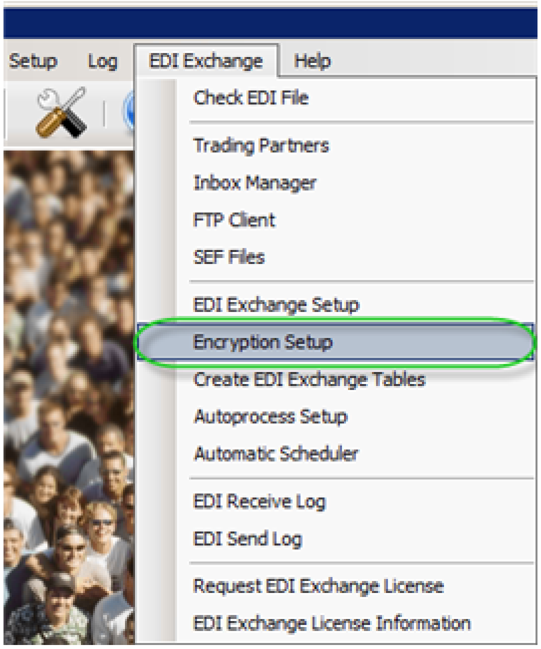
- A certificate authority (CA) that both issues and verifies the digital certificates.
- A registration authority which verifies the identity of users requesting information from the CA.
- A central directory is a secure location to store and index keys.
- A certificate management system.

EDI Exchange relies on other software to establish the PKI. It only uses the capabilities of these programs through their Application Programming Interface (API). You need to install separately either PGP Desktop or the open source GPG4Win programs and set them up with the public keys of your trading partners and your own private key.

5.2 Setting up Encryption

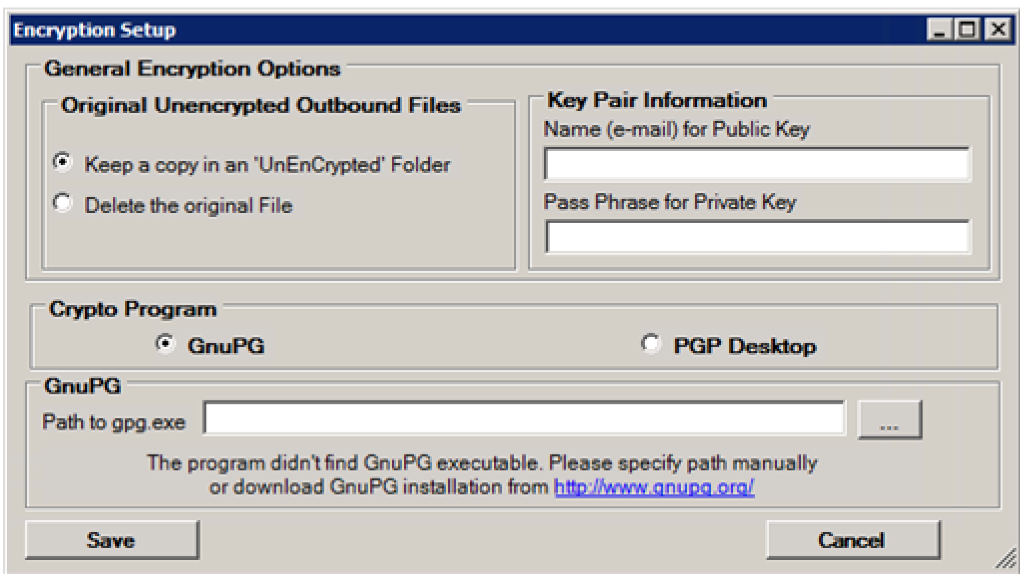
EDI Exchange allows you to set up the encryption for your EDI files. Follow the steps below.

1. Access the "Encryption Setup" window by selecting "Encryption Setup" under the "EDI Exchange" menu.



The encryption setup menu

2. The following window will appear.



The encryption setup screen

3. In this window define the following options:

General Encryption Options

- **Original Unencrypted Outbound Files**
  - **Keep a Copy in an 'Unencrypted' Folder** — When the HIPAAsuite program

creates an EDI file for a trading partner that has selected encryption, you can keep an unencrypted copy in the "Outbox/*[trading partner]*/Unencrypted" folder. This is useful when you need to go back to the file and check on problems.

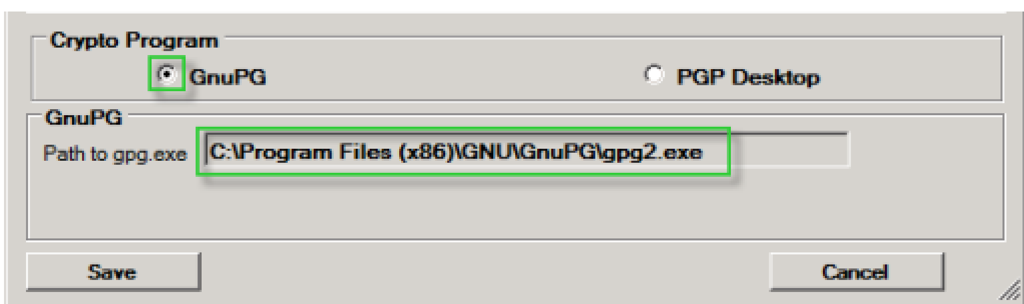
> Note: Once you encrypt a file with the public key of your trading partner, you will not be able to open it again. Only the owner of the private key can decrypt it and read it.

- **Delete the Original File** — If you do not want to keep the unencrypted copy, select this option.

- **Key Pair Information**
  - **Name (e-mail) for Public Key** — Enter name or e-mail that will be used to encrypt files for you by your trading partners.
  - **Pass Phrase for Private Key** — Enter passphrase here to decrypt files encrypted previously with the pass phrase.

> Note: The keys are identified by the email address of their owner.

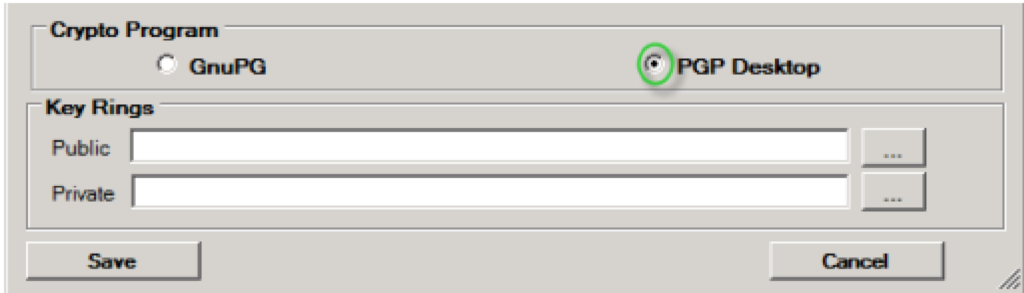
- **Crypto Program**
  - **GnuPG** — Select this option if you have already installed the GnuPG software and want to use it.



The configuration using GnuPG

> Note: When you select GnuPG, the program checks if the executable `gpg.exe/gpg2.exe` is present on your computer. If it is not found, you will have to specify the path manually or install the program first.

  - **PGP Desktop** — Select this option if you have already installed the PGP Desktop program and want to use it. You will see a different lower half of the screen, where you can indicate the location of the keys. PGP Desktop uses "key rings" — encrypted folders that contain all your keys. The location of these two files is very important for PGP Desktop.

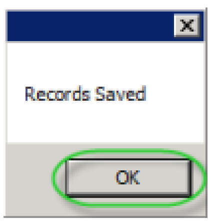


The configuration using PGP Desktop

4. Once the settings are done, click the "Save" button.

The "Save" button

5. The following notification will appear. Click the "OK" button.



Notification window

5.3 Using PGP Desktop

Pretty Good Privacy (PGP) is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication. PGP is often used for signing, encrypting and decrypting texts, e-mails, files, directories and whole disk partitions to increase the security of e-mail communications. PGP and similar products follow the OpenPGP standard (RFC 4880) for encrypting and decrypting data. For more information, see How PGP works.

EDI Exchange supports PGP encryption and works seamlessly with PGP Desktop and open source Gpg4Win applications.

PGP Desktop (Symantec's encryption solutions) is a comprehensive suite of encryption applications which provides flexible, multi-layered encryption by bundling Drive Encryption to secure the files stored on local hard drives, and Desktop Email Encryption to secure confidential data in email. For more information, see PGP Desktop documentation.

PGP Desktop key features:

1. Hard drive encryption software locks down the entire contents of a laptop, desktop, external drive, or USB flash drive, including boot sectors, system, and swap files.

2. Enables encrypted email and secure AIM® Instant Messages.

3. Creates storage-independent encrypted containers for transport and sharing of specific files using included utilities; PGP Self-Decrypting Archive, PGP Virtual Disk, and PGP Zip.

4. Includes PGP Shredder which can completely destroy unwanted disk-based files and folders.

5. Drive Encryption can be centrally deployed and managed by Symantec Encryption Management Server.

PGP Desktop key benefits:

1. Secures email without burdening users, to improve compliance with policies and regulations without hindering productivity.

2. Allows users to easily and transparently share encrypted files and folders, improving data security without impacting user productivity.

3. Management by Encryption Management Server centralizes creation, deployment and management of data security policies and reporting.

PGP Desktop bundles the following products:

1. Drive Encryption. See System Requirements.

2. Desktop Email Encryption. See System Requirements.

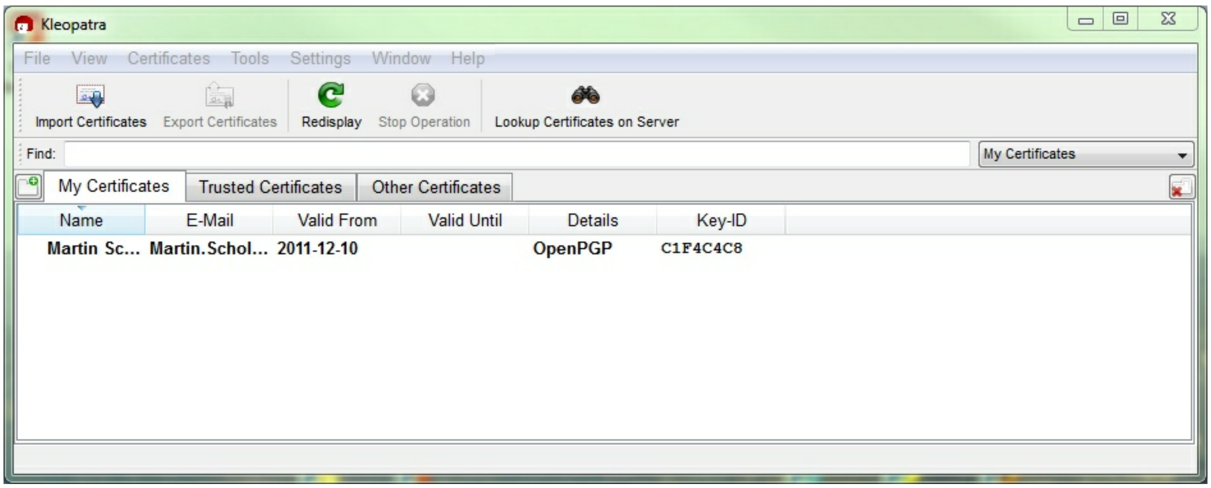
3. Encryption Management Server. See System Requirements.

5.4 Using GnuPG

GnuPG is an Open Source project for the implementation of the OpenPGP (pretty good privacy) protocols of encryption. GnuPG allows to encrypt and sign your data and communication, features a versatile key management system as well as access modules for all kinds of public key directories. GnuPG, also known as GPG, is a command line tool with features for easy integration with other applications. Front-end applications and libraries are also available. Version 2 of GnuPG also provides support for S/MIME.

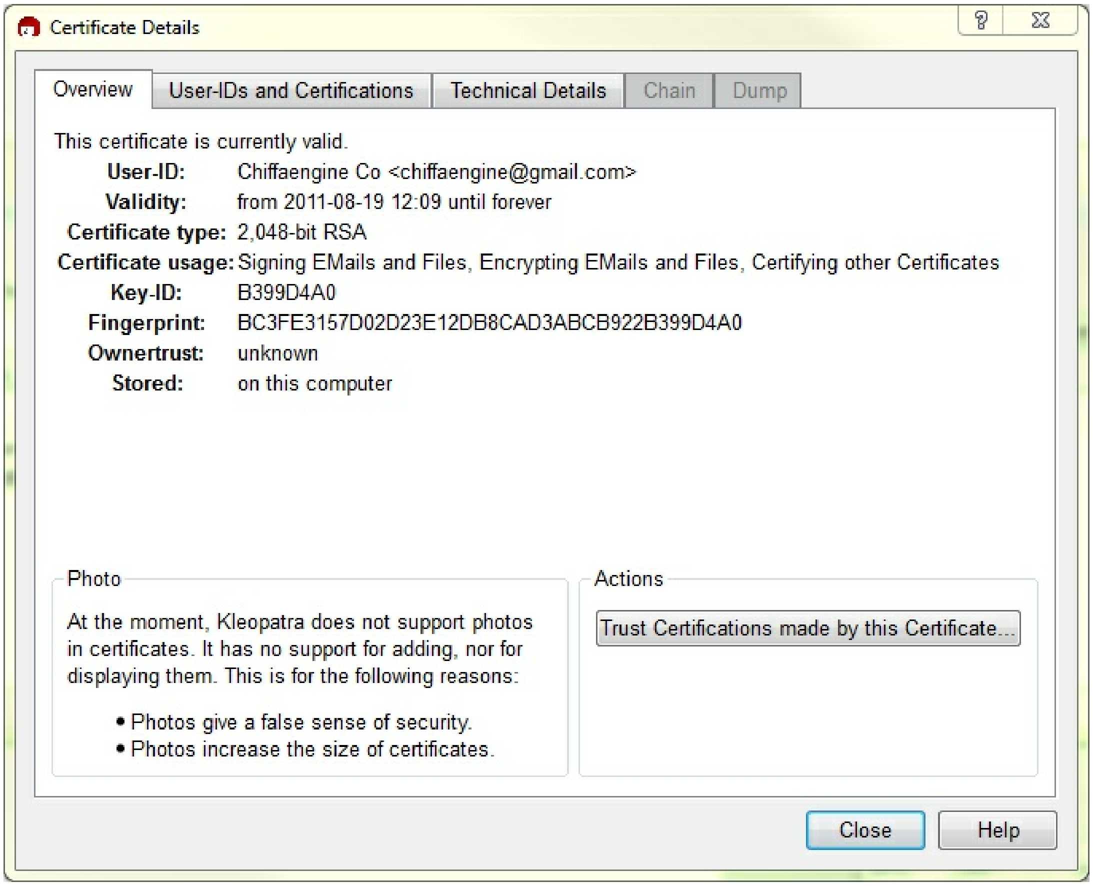
GnuPG is a free software, so it can be freely used, modified and distributed under the terms of the GNU General Public License.

We recommend Gpg4Win for encrypting of your files and emails. Gpg4Win supports both relevant cryptography standards, OpenPGP and S/MIME (X.509), and is the official GnuPG distribution for Windows. Gpg4Win contains Kleopatra as one of its Free Software components. For more information, see Gpg4Win documentation available both in PDF and HTML versions.



Kleopatra, a certificate manager for OpenPGP and X.509 (S/MIME) and common crypto dialogs

With Kleopatra, it is easy to manage your certificates and create your own ones. It seamlessly integrates with GnuPG. You can manage the key that you receive from your trading partners, because there is a screen to view the details of a key.



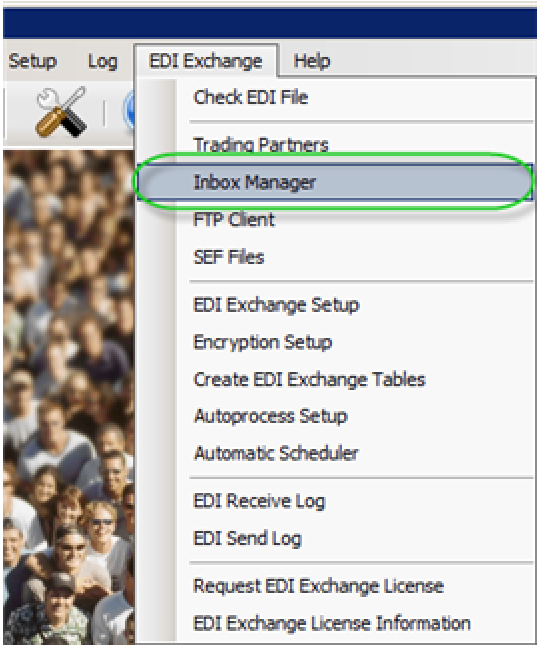
Certificate details with Kleopatra

6 Using EDI Exchange Features

6.1 Accessing Inbox Manager

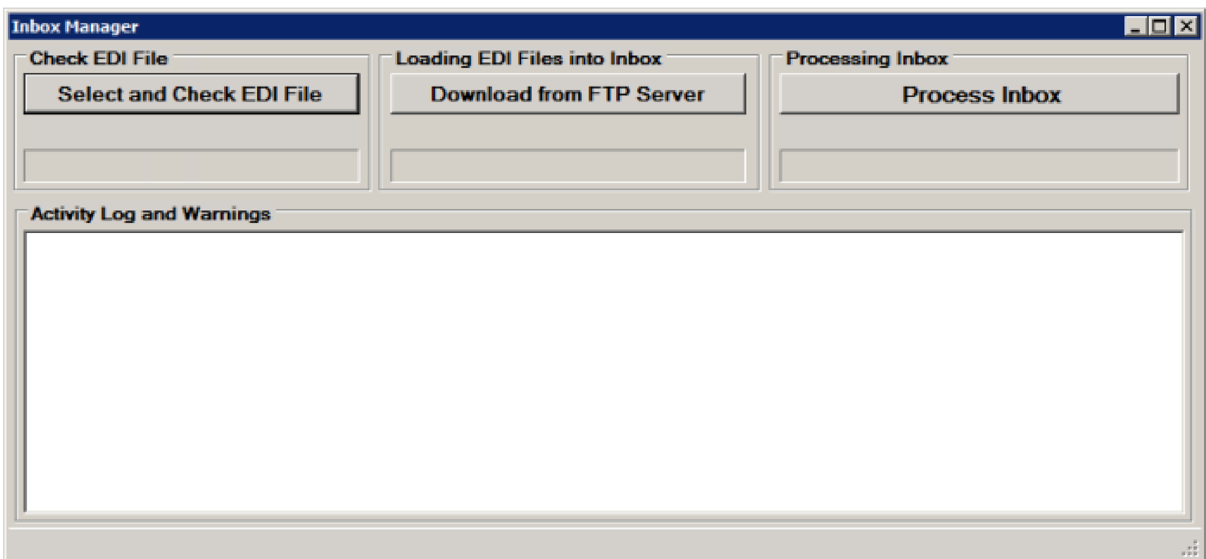
Using the Inbox Manager you can access the most important functions of EDI Exchange. Inbox Manager allows you to download EDI files into the "Inbox" folder and process these files. This screen handles the post-processing of the EDI files, their compliance check and auto-processing options.

1. To access the Inbox Manager, click the "Inbox Manager" under the "EDI Exchange" menu.



The "Inbox Manager" menu item

2. The following screen will come up.



The "Inbox Manager" window

Read more in:

- Downloading EDI Files From FTP Server
- Processing EDI Files
- Selecting and Checking EDI Files

6.2 Checking EDI Files

EDI file analysis based on the HIPAA standards. Compliance with HIPAA EDI rules is an essential part of the exchange of EDI documents. The standards are the only agreed upon rules that sender and receiver use to exchange data from completely different backend systems. Strict adherence is therefore necessary to guarantee frictionless operation.

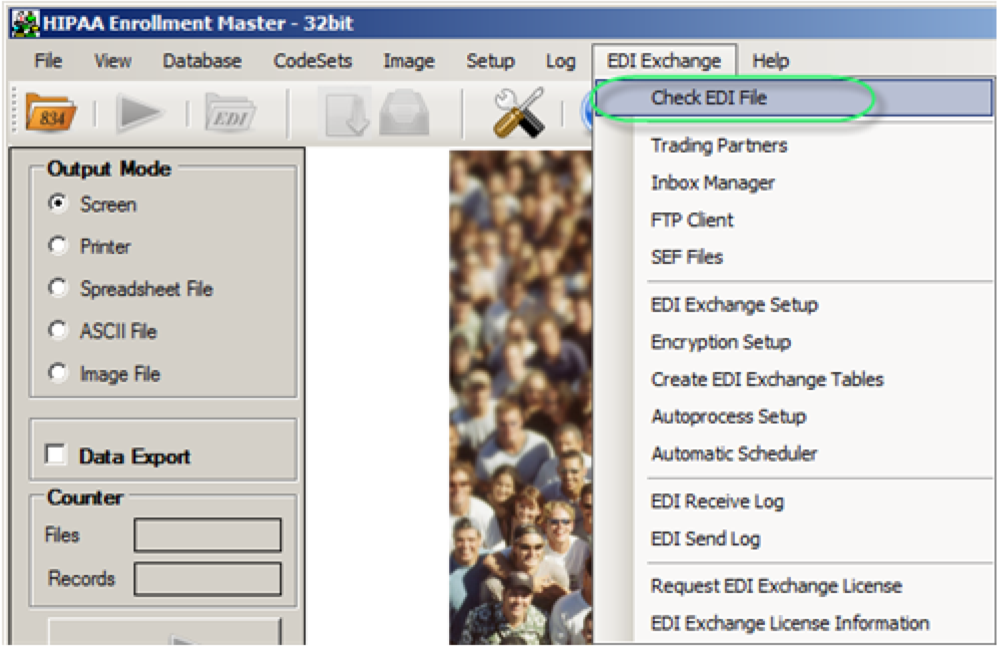
Unfortunately, HIPAA compliance is difficult and the truth is that many HIPAA EDI files are truly bad. Syntax errors, omitted loops, missing elements, wrongly formatted elements — these are the most common EDI errors. Without a true analysis, it is difficult to say what data ends up in your system.

EDI Exchange has a built-in compliance engine that analyzes each incoming and outgoing EDI transaction. Line by line, element by element, error reporting provides a powerful tool to determine the quality of the incoming and outgoing EDI files. All HIPAA file versions are supported. The compliance check creates a detailed report that lists every compliance issue. Outgoing files can also be checked and individual transaction in violation of HIPAA rules can be held back.

> Note: You can enable automatic compliance check on outgoing and incoming EDI files. See Setting up Incoming and Outgoing Files Options.

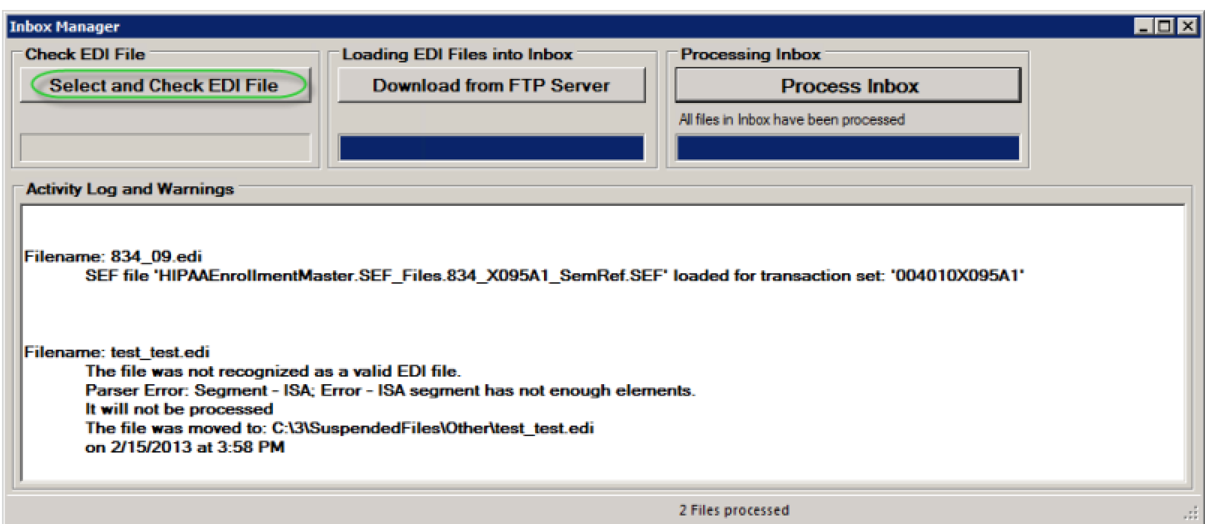
Follow the instructions below to check EDI files for compliance.

1. Select "Check EDI File" under the "EDI Exchange" menu item.



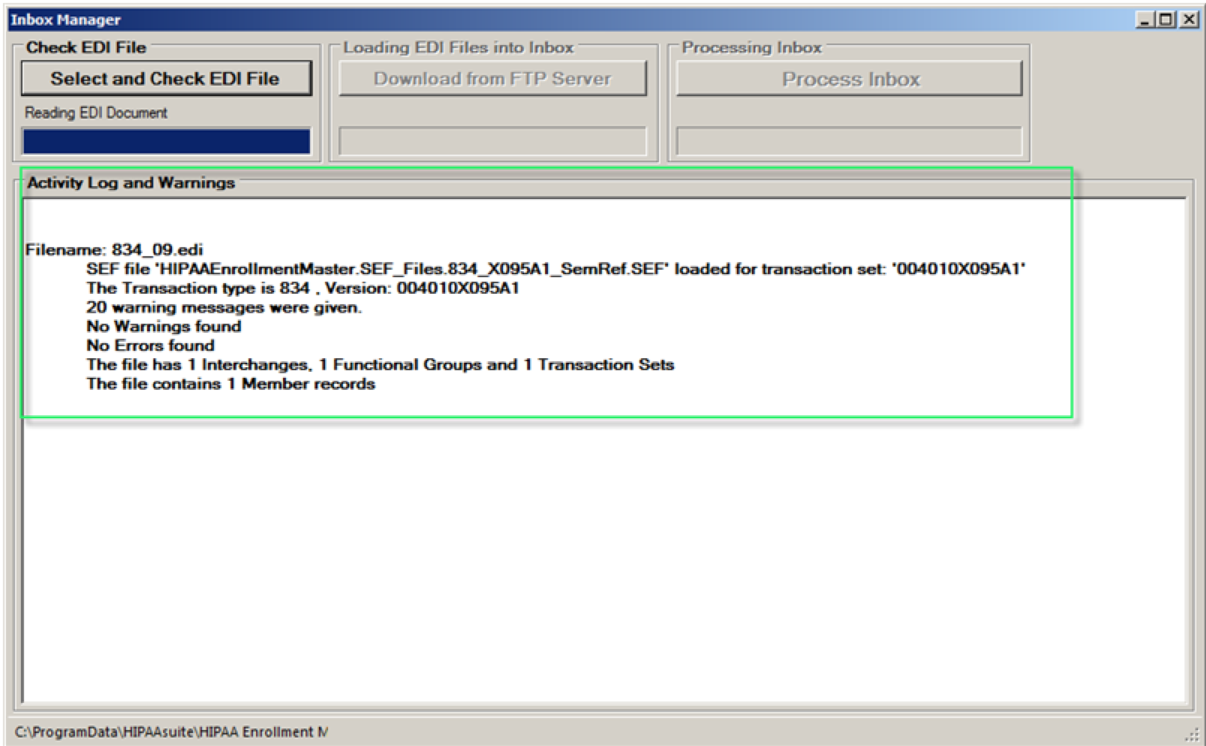
The "Check EDI File" menu item

Alternatively, you can click on the "Select and Check EDI File" button in the Inbox Manager window. Read more in Accessing Inbox Manager.



The "Select and Check EDI File" button

2. In the opened file selection dialog, select an EDI file and click "Open."
3. In the Inbox Manager, you can see the result messages for the operation. The details are displayed in the "Activity Log and Warnings" area.



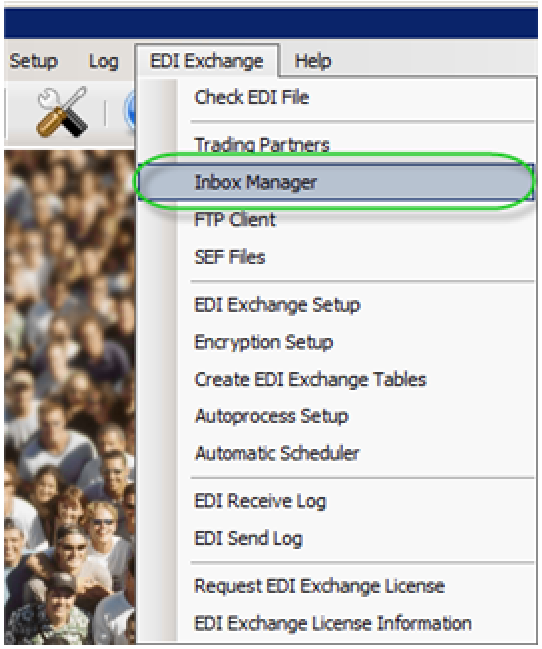
The "Activity Log and Warnings" area displaying log messages

6.3 Downloading EDI Files From FTP Server

EDI Exchange Inbox Manager allows you to load EDI files into the "Inbox" folder and process these files. Be sure you have setup FTP settings in the "Remote FTP" tab of the Trading Partner window (see Setting up Trading Partners).

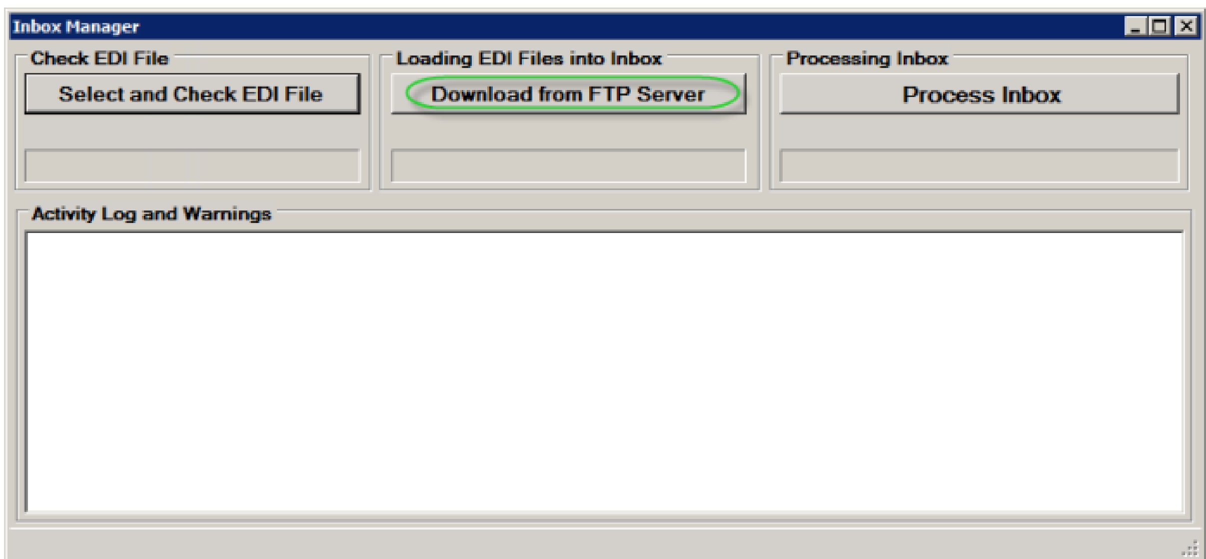
Follow the instructions below to upload EDI files into the "Inbox" folder.

1. Access the Inbox Manager by clicking the "Inbox Manager" under the "EDI Exchange" menu.



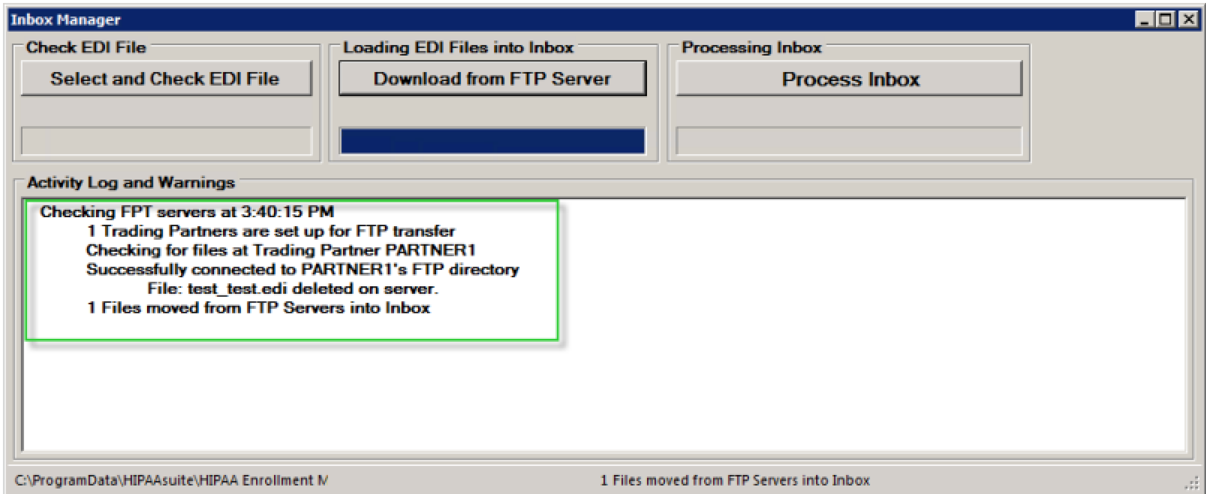
The "Inbox Manager" menu item

2. Click the "Download from FTP Server" button.



The "Download from FTP Server" button

3. When the process has been finished, the "Activity Log and Warnings" area displays the report.



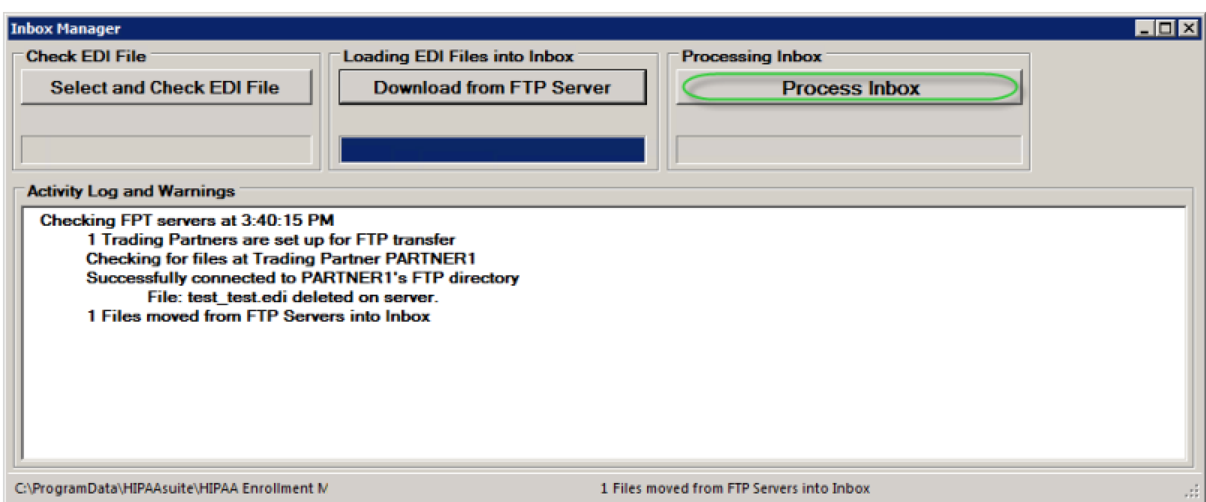
Activity Log and Warnings information

6.4 Processing EDI Files

EDI Exchange Inbox Manager allows you to process EDI files downloaded to the "Inbox" folder beforehand.

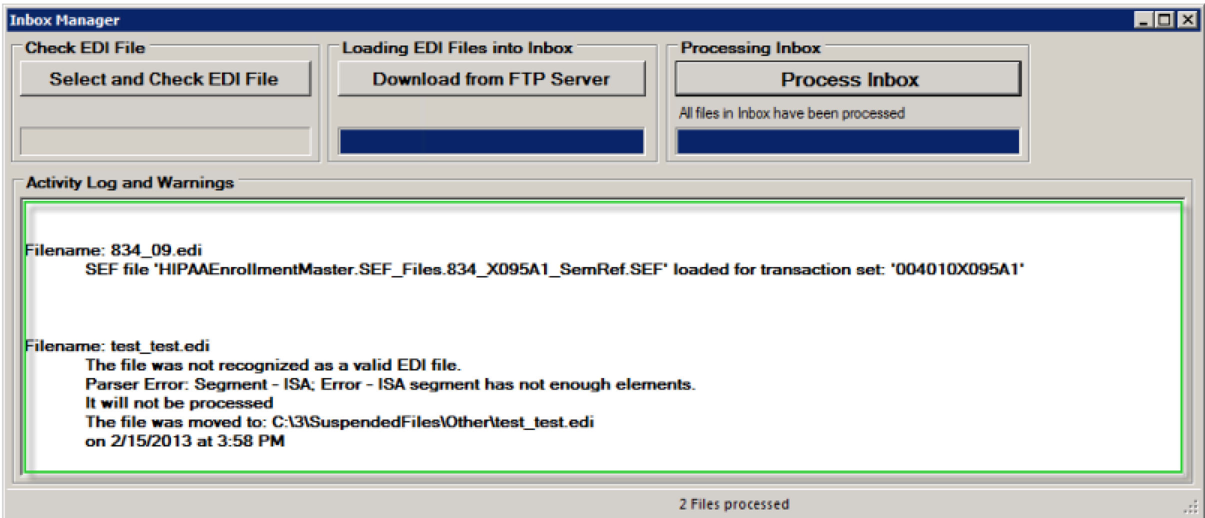
> Note: Once you have saved the auto-processing options (see Defining Auto-Processing Options), the files will not only be analyzed but also processed according to the defined settings. The auto processing enables you to combine and run multiple fulfillment steps together (for example, export, saving, printing.)

1. Once Downloading EDI Files From FTP Server is completed, and no errors are displayed, click on the "Process Inbox" button.



The "Process Inbox" button

2. Once the processing is completed, review the Activity Log and Warnings information.

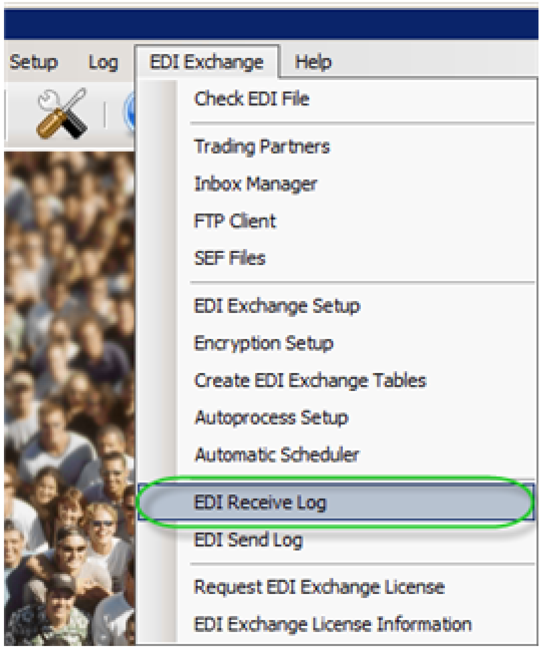


Activity Log and Warnings information

6.5 Accessing EDI Receive Log

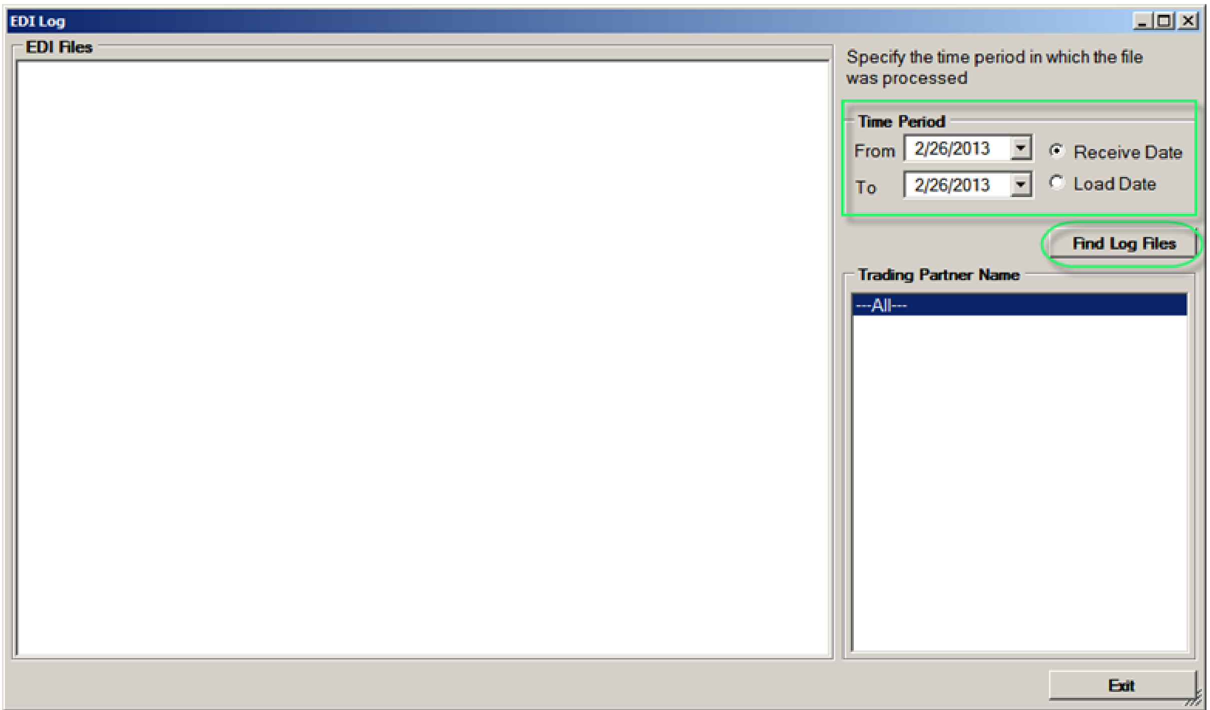
EDI Exchange has a file log. Each processed file creates an entry in the `Trans_Log` table. You can access the "EDI Log" window to query this table and see what files came in and how they were processed. You can access the EDI Receive Log once the application has been initialized. Follow the instructions below.

1. To open the "EDI Log" window, select "EDI Receive Log" under the "EDI Exchange" menu item.



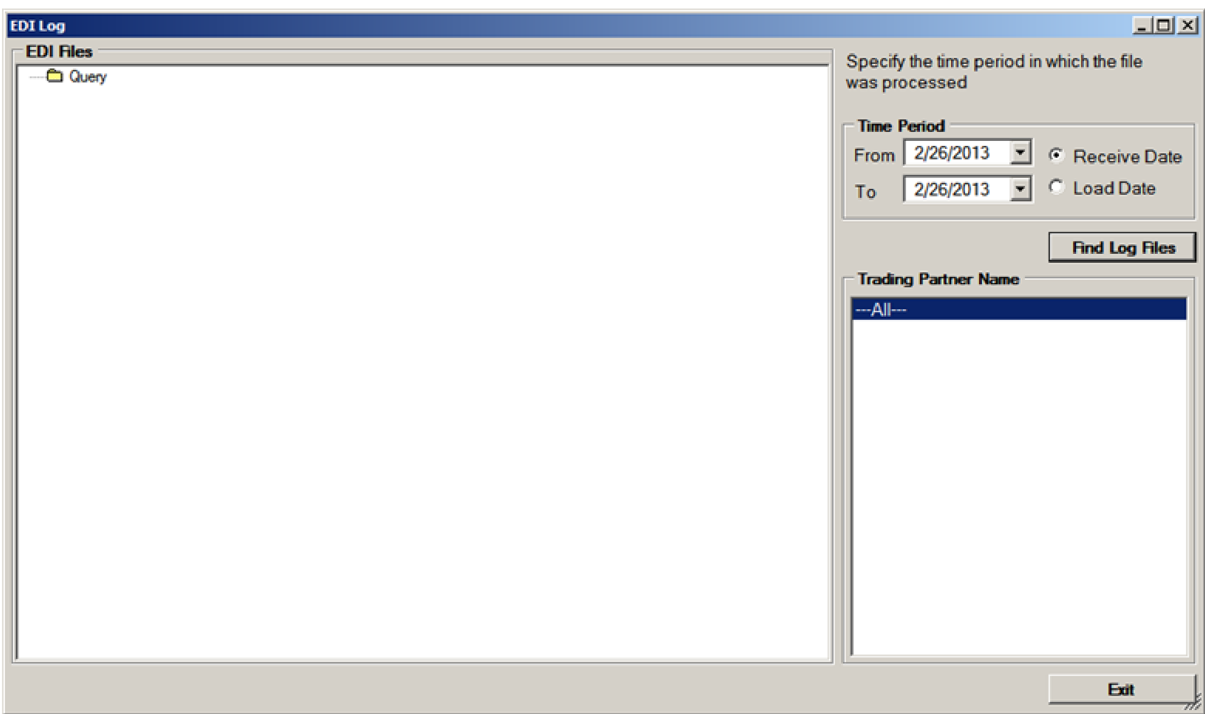
The menu for the EDI Receive Log

2. To display data, specify the time period and select trading partner.
    - **Time Period** — Period of time when the file was processed. Choose one of the available options:
        - **Receive Date**
        - **Load Date**
    - **Trading Partner Name** — You can select your trading partner from the list. If you select "---All---", all your trading partners will be included.
3. Click on the "Find Log Files" button to see the list of log files corresponding to your query.



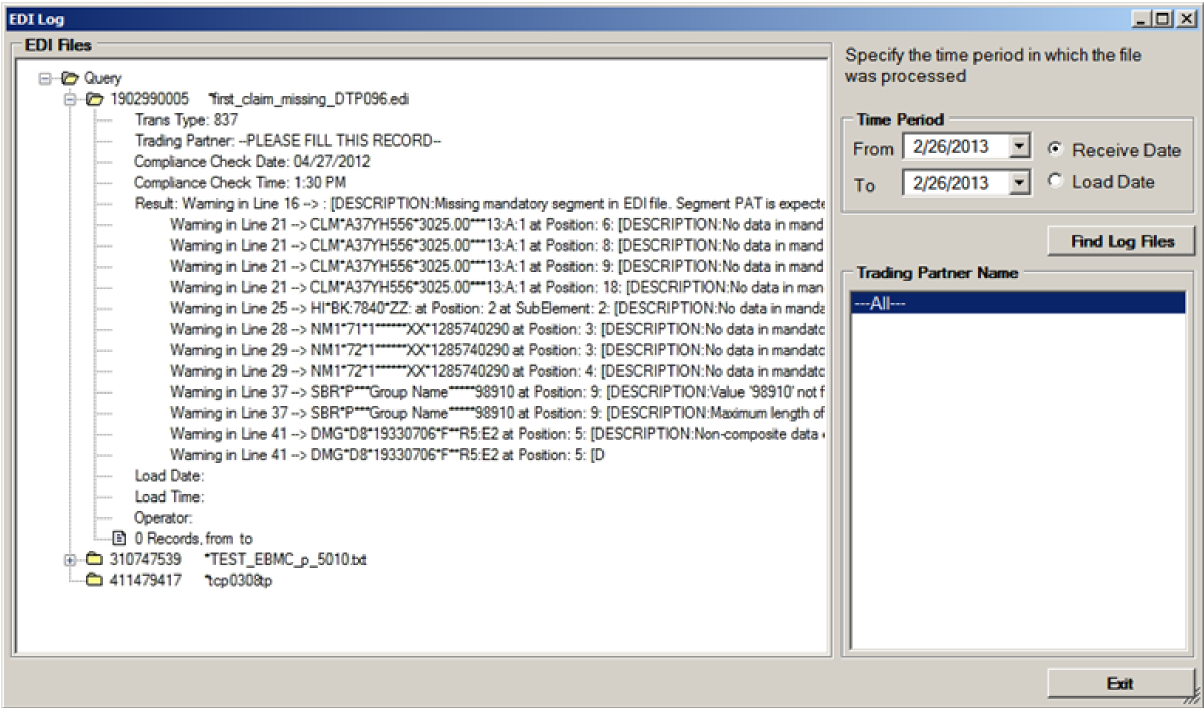
Specifying the time period

4. The log will be displayed in form of a tree.



Displayed log

5. You can open the folder icons and see details related to each file.



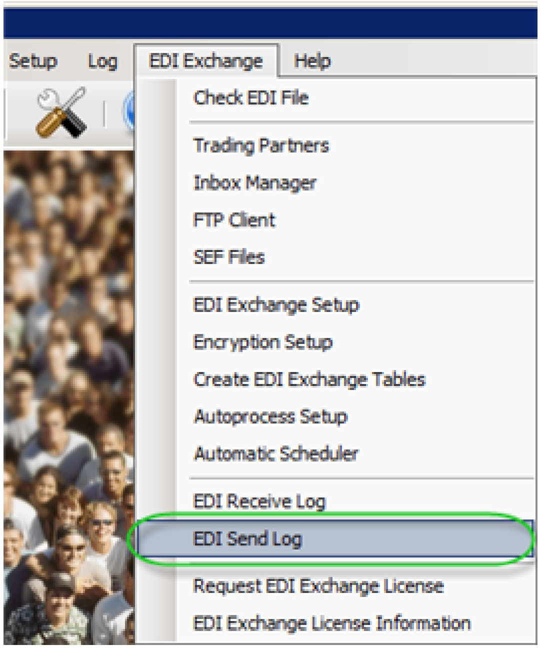
Details of the EDI Receive Log

If the records have been exported to the database, you can see the time, date and record count.

6.6 Accessing EDI Send Log

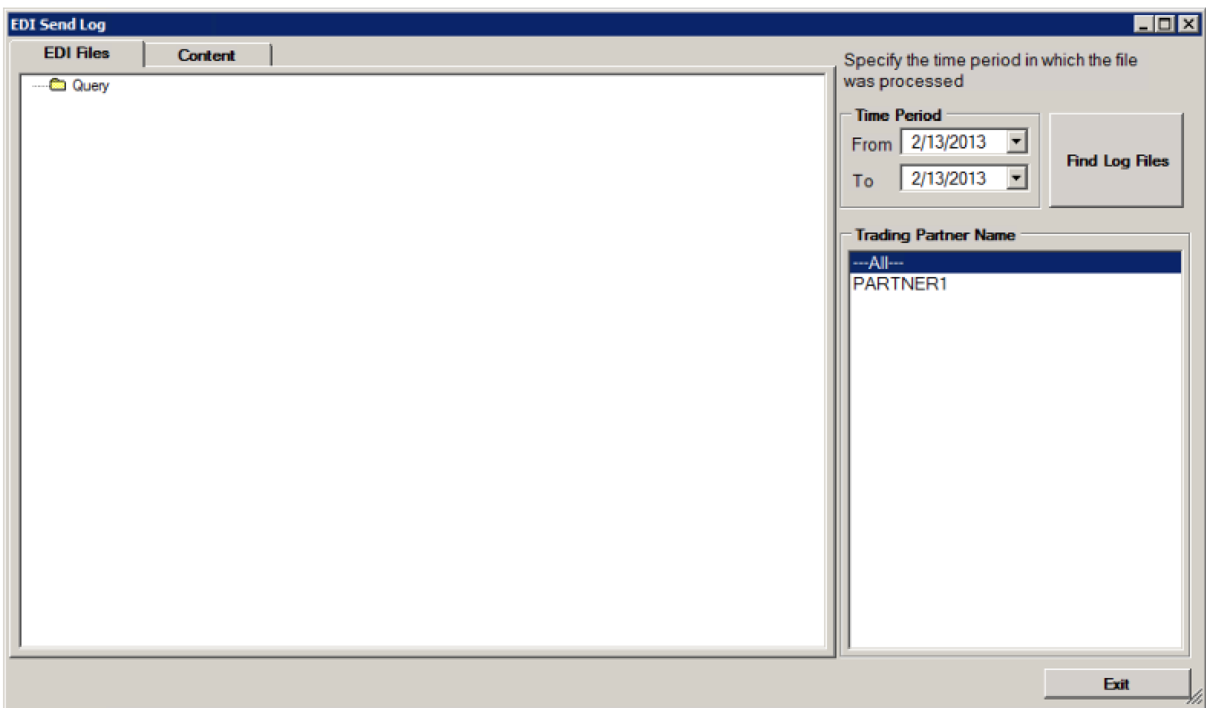
This page contains instructions on how to access the "EDI Send Log" window. It becomes available once EDI Exchange has been initialized.

1. Select "EDI Send Log" under the "EDI Exchange" menu.



The "EDI Send Log" menu

2. The following window will appear:



The "EDI Send Log" screen

3. To display the log data, select the time period and a trading partner.

   - **Time Period** — Period of time when the file was processed. Choose one of the available options:

- **Receive Date**
- **Load Date**

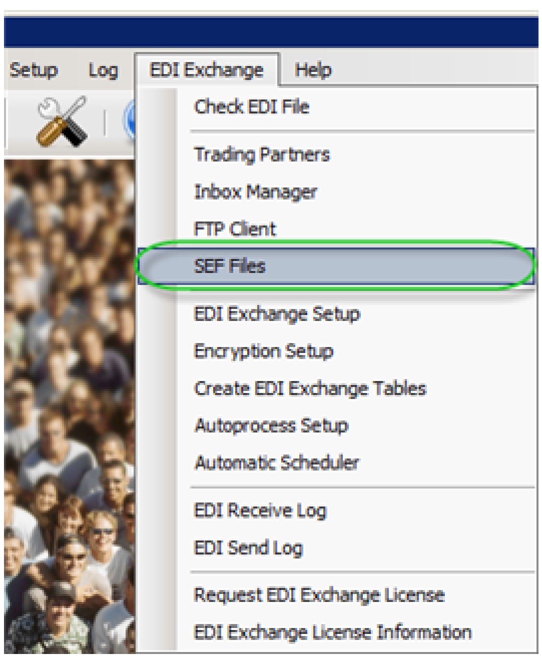
- **Trading Partner Name** — Select a trading partner in the list. If you select "---All---", all trading partners will be included.

4. Click on the "Find Log Files" button to display the list of log files corresponding to your query.

6.7 Listing SEF Files

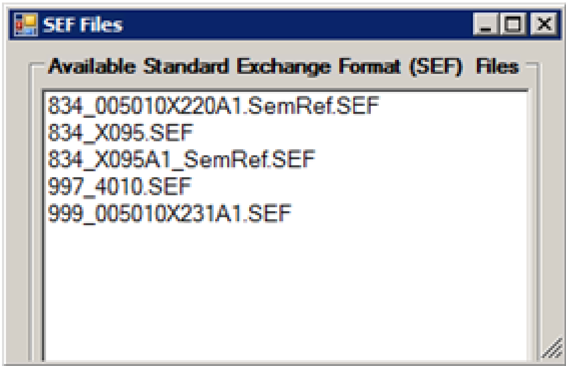
SEF (Standards Exchange Format) files are repositories of standards information that define the format of EDI documents. SEF files are the basis for the compliance check engine that EDI Exchange uses. These files contain all rules of the implementation guide of a transaction. There is a SEF file for each transaction that EDI Exchange is licensed for. For example, for 837 transactions we have SEF files for institutional, professional and dental claims in 4010, 4010A1 and 5010A1 version and the 997 and 999 transactions.

1. To access the list of available SEF Files, select "SEF Files" under the "EDI Exchange" menu.



The "SEF Files" menu item

2. The "SEF Files" window will appear.



A list of SEF files