The HIPAA Claim Status Responder

Table of Contents

1 Introduction

1.1 The HIPAA Claim Status Responder

The status of claim, whether it has been paid, rejected, pended, adjudicated or lost is of eminent importance in the commerce between a health care provider and an insurance company paying for the services of their policy holders. Providers need to be assured that they have a proper cash flow and that problems with claims are quickly identified, rectified and the claims resubmitted. That is the reason why a considerable part of the staff in a hospital or doctors office does billing. If a provider misses payment on a particular claim or has questions regarding the adjudication they will have to contact the payer and ask for the status. Traditionally this has been handled by telephone operators or voice response systems with fax back options. And all too ofter this consists of being on hold large parts of the day to get information on a particular claim. This is time consuming and pushed many doctors to the point of giving up the solo practice.

HIPAA (Health Insurance Portability and Affordability Act) was conceived to bring administrative simplification into the provider-payer relationship and was intended to lower the costs of doing business for payers and facilitate the communications between payer and provider. The HIPAA legislation of 1996 addressed this critical bottleneck of commerce and prescribes the 276/277 EDI transaction set as format for electronic transmissions of claim status requests and responses. The law prescribes this particular transaction set as a mandatory transaction, this means that covered entities have to use it when asked to in order to convey claim status information electronically. Unfortunately 12 years after the HIPAA transaction sets were mandated we have still only spotty performance by payers in their ability to produce meaningful claim status responses.

With the Affordable Care Act, aka Obama Care the CORE Phase II requirements were adopted and it has become obligatory for health plans to provider such claim status responses within seconds using SOAP or MIME communications protocol and as long as this act is not repealed we will see increasing compliance with law by payers and the need for every payer to participate in the electronic exchange of claim status information.

The HIPAA Claim Status Responder gives payers the ability to produce 277 responses to 276 requests

Here its working mechanism in short:

- A provider requests the status of a particular claim and creates a 276 EDI file.
- The file is transmitted via a clearing house, an FTP server or a SOAP or MIME Server

- The HIPAA Claim Status Responder reads each individual request and
  - o Searches the HIPAA Claim Master database for the claims with added status information
  - o Searches a set of Tables that just contains the necessary information for the response
  - o Allows to manually create the response
- The response is packaged into a 277 EDI file
- Returned to the provider

Together with the EDI Exchange module all EDI protocols requirements will be handled such as the Functional Acknowledgment (999), encryption and FTP transport and in conjunction with the HIPAA RealTime Server even CORE Phase II compliance and all the requirements of the ACA can be fulfilled.

Tying in a claim systems into the HIPAA Claim Status Responder for automatic responses is a straight forward job.

1. The claims are coming into the system with the HIPAA Claim Master and are stored in the claim header and detail table. Extra fields are added to those tables to store the status of the claim. The HIPAA Claim Status Responder looks for the claims, looks for the status information and returns it back. If there is no status information a default status is given, if the claim is not found another code is returned. A nightly process updates the table.

2. The claim status information is stored in independent tables that just contain the necessary fields of the claim. A nightly process updates the table.

3. Manual response. Compose the response in a screen by looking up the claim in a legacy system and transferring the information into the claim status response. If the volume of 276 requests is low or even non-existent, then it would be sometimes unwise to spend money and resources on the automatic handling of claim status requests.

1.2 Features

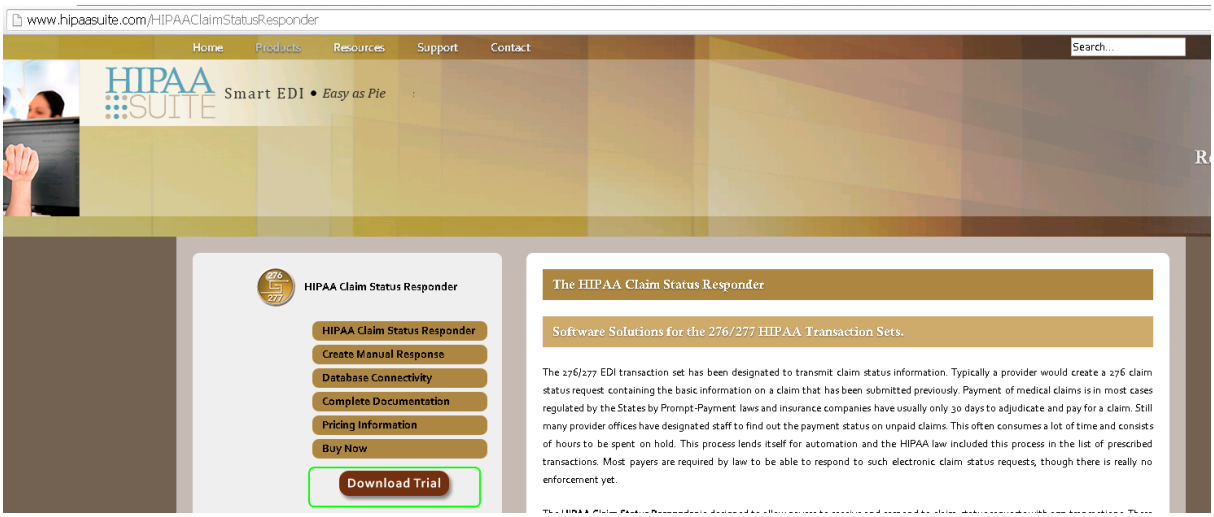
Here a list of the features of the HIPAA Claim Status Responder:

- Takes in X12 276 EDI files
- Parses the whole file and lists each individual claim status request
- Allows one to answer claim status requests sequentially or randomly from the listing
- Option to have default claim status values
- Editable code sets, so you can set the codes used by your company
- Claim status assignment on claim level and line level if the request contains line information
- After status assignment program will create one 277 file that can be returned to the sender
- Export of Claim Status information to any ODBC compliant database
- Tie in to existing claim system and enable automatic response (some interface development necessary)

2 Installation

2.1 Obtaining the software

The HIPAA Claim Status Responder can be downloaded from the HIPAAsuite's website at www.HIPAAsuite.com.



The home page for the HIPAA Claim Status Responder. Click on Download Trial to obtain he software.

The software is in trial mode when first installed and an unlock key has to be used to put

the HIPAA Claim Status Responder into full production mode.

2.2 Installation

The software is packaged in a Zip file with a Microsoft Windows Install Script (msi) file and an file called Setup.exe.

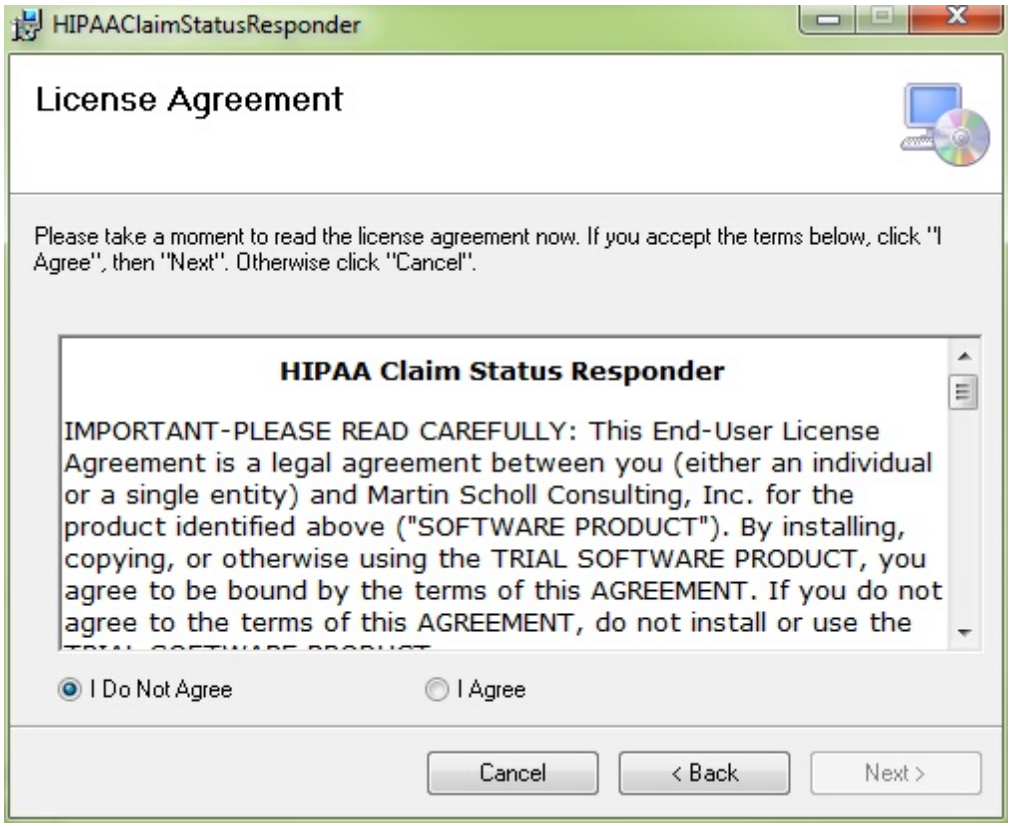
> Make sure to install the program by using the Setup.exe program. This makes sure that all necessary Windows components will be checked and installed if needed.

All the necessary files are contained in the package and the Microsoft Installation engine will sort out merge modules and dependencies of system files and other dll's.

When you execute the installation script file "HIPAAClaimStatusResponder.exe" you will be confronted with the following screen:

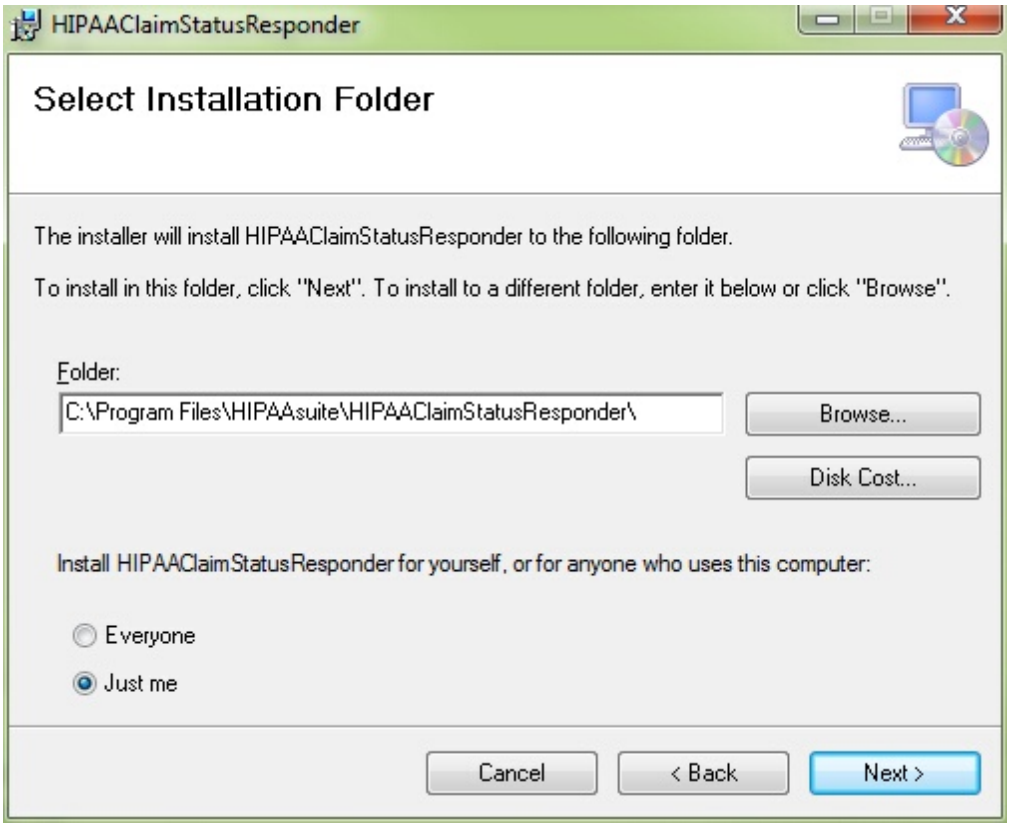
the welcome screen of the Installation wizard

In order to proceed you have to agree to the software license agreement



The software license agreement

After that you have the choice of where to install the program.



Choosing the install directory

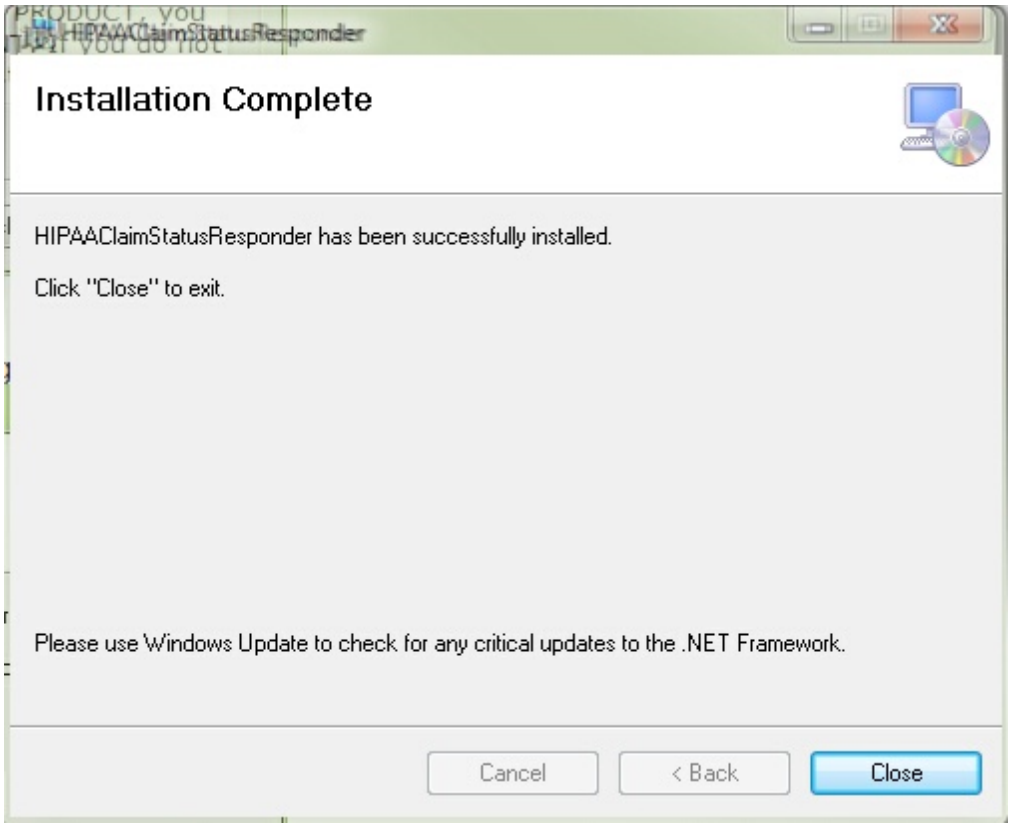
Install Option

Start Menu

Desktop

Quick launch bar

The installation will be proceeding then. After that the program installs and after successful installation you will see the final screen



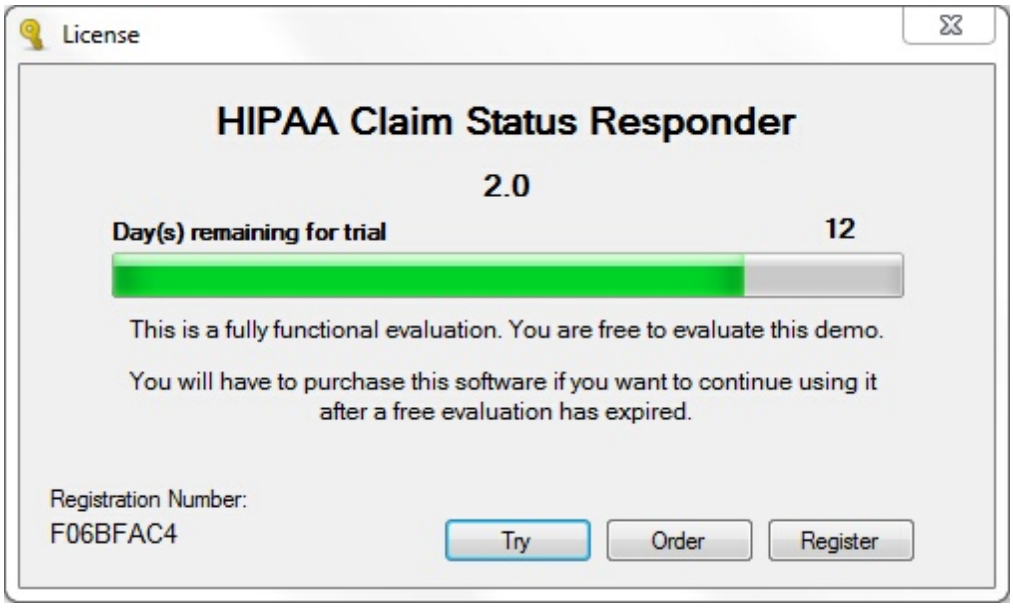
The final installation screen

2.3 Software Trial

The HIPAA Claim Status Responder comes with a free trial of 14 days.

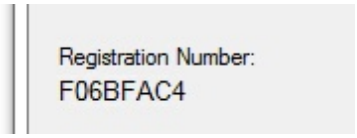
Should your trial time expire and you wish to continue your testing of the software, please send an email to info@HIPAAsuite.com with the Registration number and we will give you a trial extension.

If the product is not registered and you start it, you will see first the trial screen.



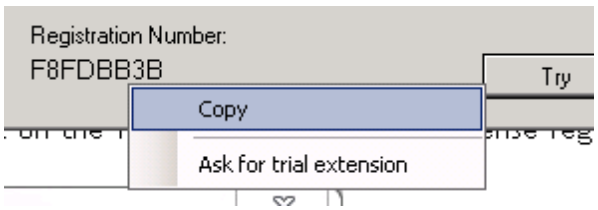
The Trial Screen

You can see clearly the registration number in the lower left hand corner.



The Registration number

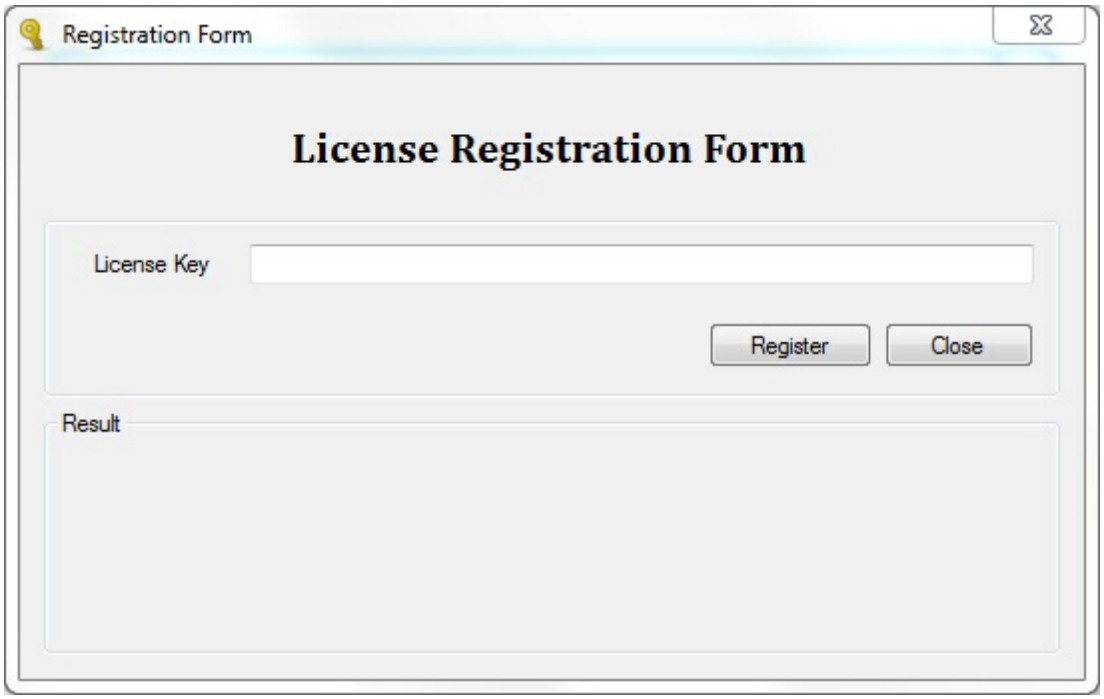
This number is needed for the registration as well as trial extension. It is unique to your computer and hardware. **You can copy the registration number to the clip board, just hover with the mouse over it**, so that you can easily paste it into an email. This avoids human error. (There are no 'O', the letter in the number, only zeros!)



Copy the registration number to the Windows clip board by hovering over the it with the mouse

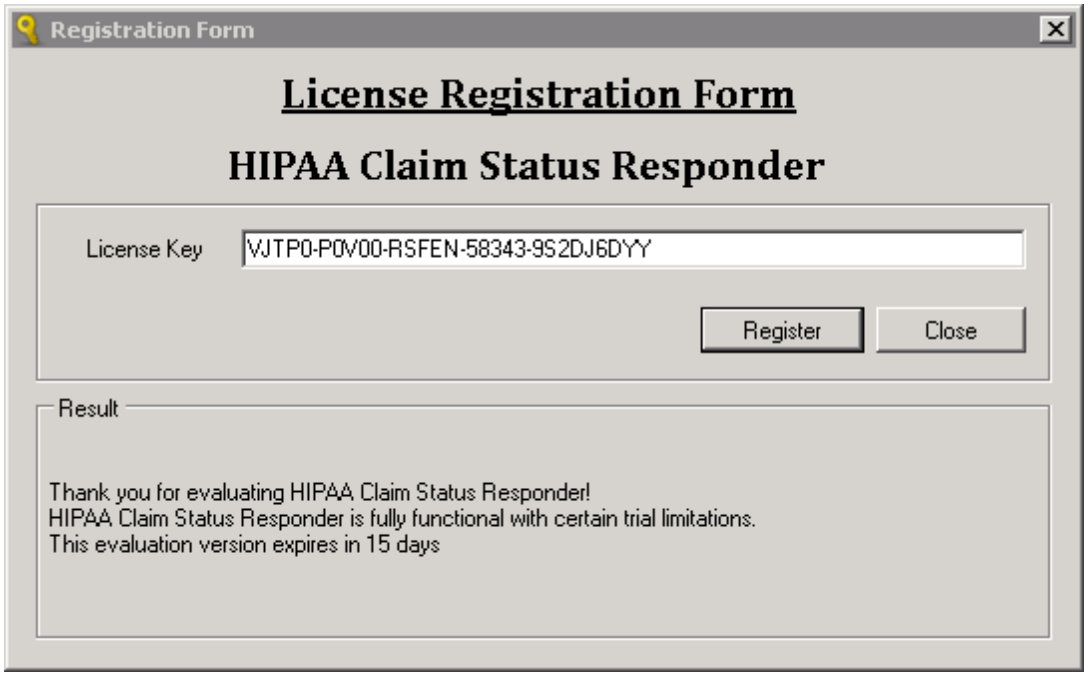
You can even generate an email to us with all the pertinent information as long as a mail application is installed on your computer. When you click "Ask for trail extension" the email client installed pops up with a new message. In this case Outlook.

Once you have received the license key from us you click on the 'Register' button and the license registration form comes.



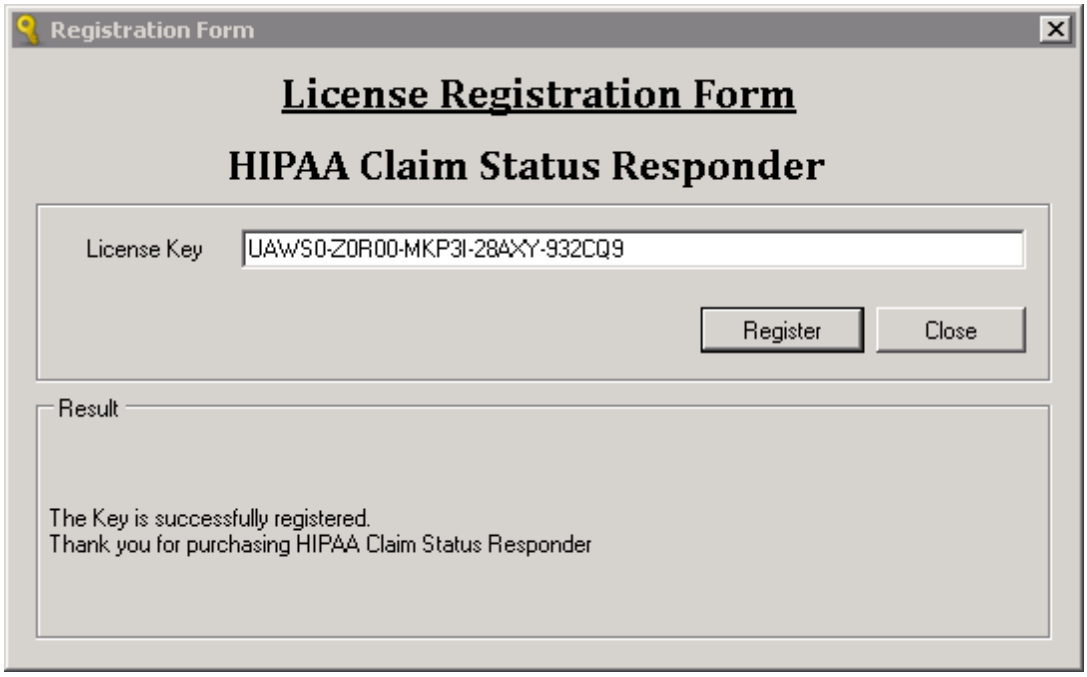
Entering the registration information

Enter the License Key as supplied in our email. The best is to copy and paste the information from our email to avoid typos

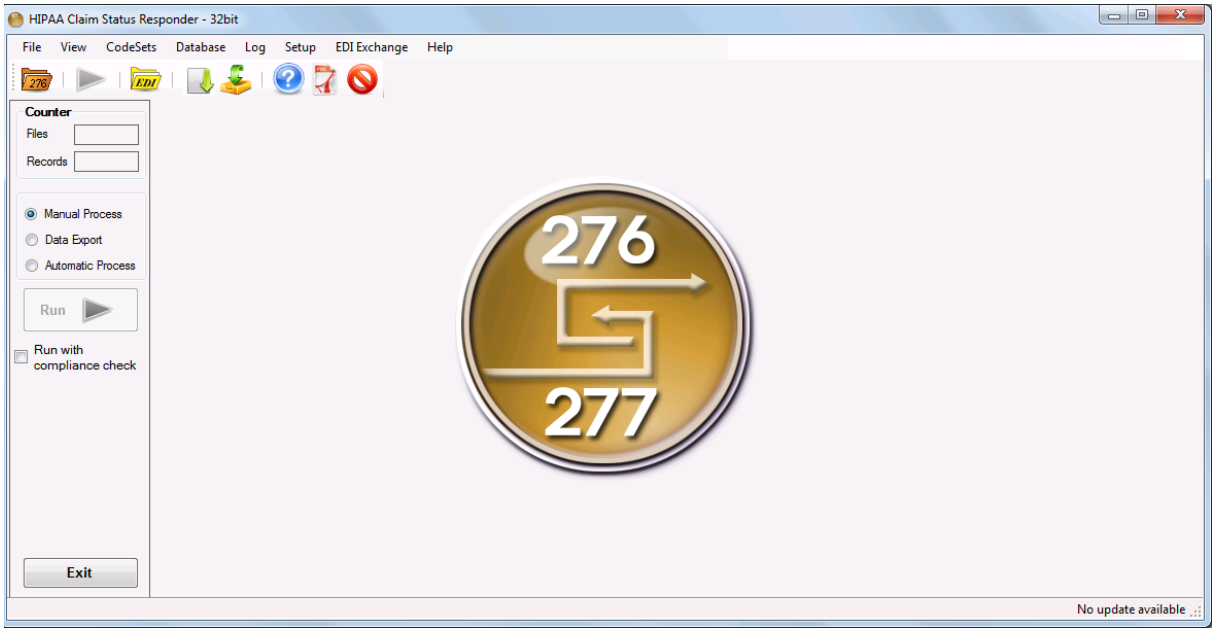


After entering a trial key the software is trial is extended for another 15 days

Once the product is registered with a permanent unlock code, future upgrades will find this key and install without further action necessary.



2.4 Main Window



The HIPAA Claim Status Responder's main screen

In the lower right corner you see the text 'No update available'. When you start the program a process gets started to check HIPAAsuite's website to see if any newer version of the software is available. If there is a new version, you will be presented with a message box asking you to download the newer version. If you decide to do so, the HIPAA Claim Status Responder

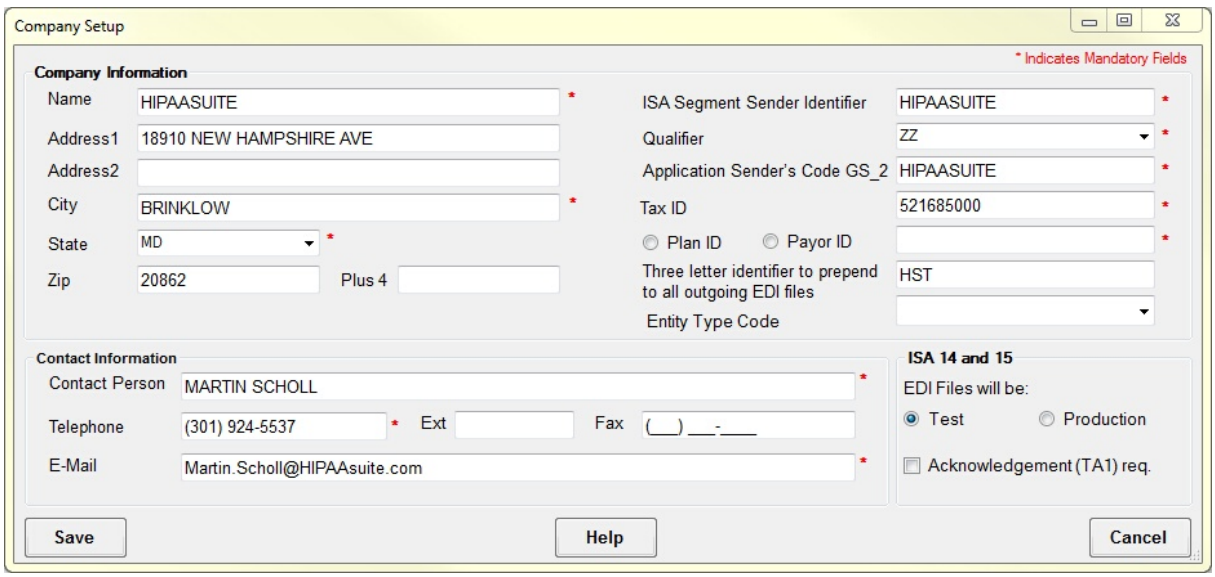
- will exit,
- download the new installation file,
- install it and then
- restart the new version of the program.

3 Setup

3.1 Company Setup

The HIPAA Claim Status Responder needs certain information about you as the sender of EDI transactions so that the software can create a valid EDI file. This information will mainly go into the EDI envelope.

The menu item 'Setup --> Company Setup' will present you with the following screen:



The company setup screen

Fill in the information as far as you know it.

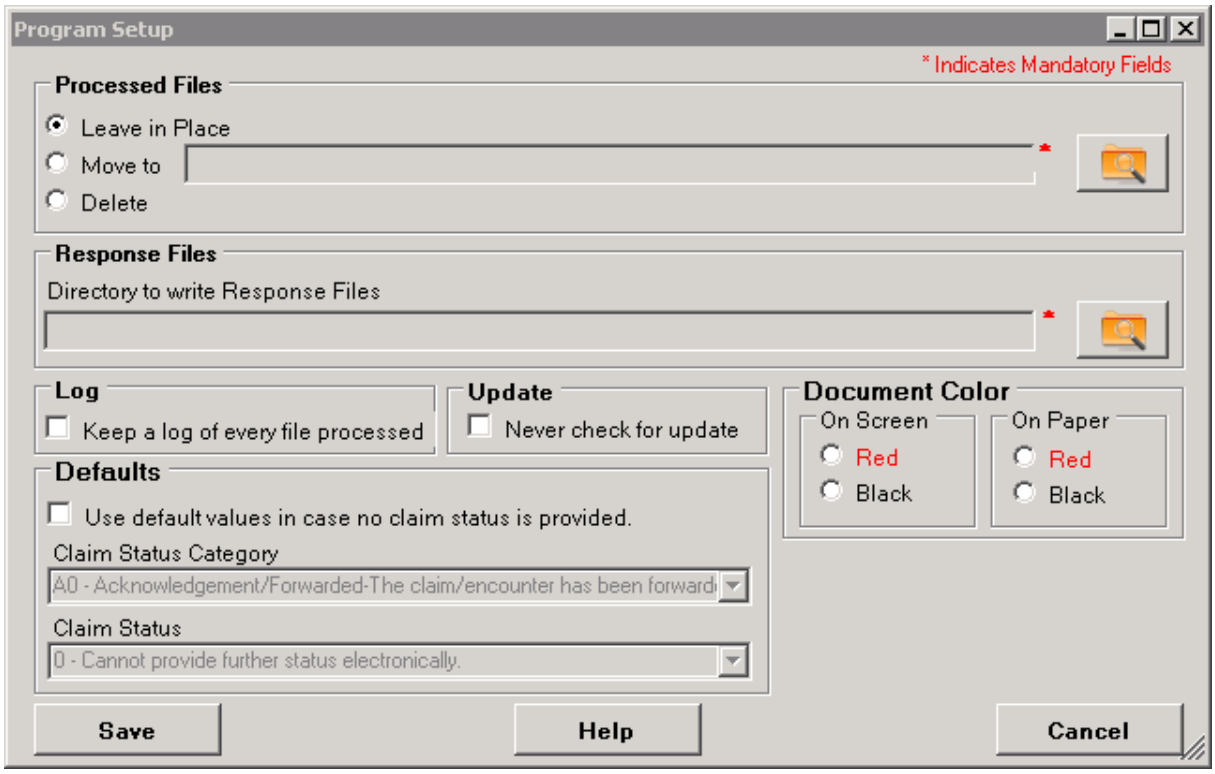
- Name and Address are self explanatory
- The ISA identifiers are needed to create the outer EDI envelope, the ISA segment. You can use any name there with 15 character or less and use the qualifier 'ZZ'. Here a list with all the identifiers and qualifiers

01 Duns (Dun & Bradstreet)
14 Duns Plus Suffix
20 Health Industry Number (HIN)
27 Carrier Identification Number as assigned by Health Care Financing Administration (HCFA)
28 Fiscal Intermediary Identification Number as assigned by Health Care Financing Administration (HCFA)
29 Medicare Provider and Supplier Identification Number as assigned by Health Care Financing Administration (HCFA)
30 U.S. Federal Tax Identification Number
33 National Association of Insurance Commissioners Company Code (NAIC)
ZZ Mutually Defined

- Application Sender's Code is needed for the Group Start segment GS, the second envelope of any EDI transaction. You can repeat here the entry from the ISA sender identifier.
- Tax ID, this is self explanatory
- Plan ID or Payor ID, this information goes into the 277 response file and is the Payer ID for the NM1_09 element in the loop 2100A. Choose Payer ID
- The optional 3 letter identifier to prepend your file names makes it easier for your trading partners to identify your responses as coming from you. This is not a mandatory field
- Entity Type code holds information that goes into the NM1_01 of the 2100 loop and classifies your business. There are about 50 different values to choose from. Select the one that describes your business the closest. This value is also used in STC_01-3, the entity identifier in the status segment. This segment is not mandatory and can be omitted.
- Contact information again is self explanatory.
- The last block of data is again concerned with the first segment of any EDI file, the ISA segment. ISA element 14 determines whether your response is Test or Production data, and ISA 15 indicates whether you expect to receive an acknowledgment for receipt for your files, the so called TA1 transaction.

3.2 Program setup

When you select the menu item 'Setup --> Program Setup' you will see the following screen:



The Setup screen

Here you can select important settings for the application.

- Determine the handling of processed files. When you don't employ EDI Exchange you have the option to leave processed files in place, which is a bad idea since you could process files again and again. You can move the to an archive folder were the processed files we be stored or you can delete the files after processing. We recommend this only when you have secured originals of those files. With EDI Exchange enabled the file we be stored anyway in the trading partner's processed file folder.
- The output directory. That is the folder where response files will be created in. This is very important. Again with EDI Exchange enabled the output folders are sorted by trading partner.
- The next section gives you options about what to do with the original claim status

request files.
  - o You can Leave the files in place. We don't recommend this setting, it will only create confusion to have processed and unprocessed files in the same folder
  - o You can move processed files to their own folder. Indicate in the next field where you want the processed files to move to
  - o You can delete the files after you are done with them. We only recommend this setting if you have a copy of the original file somewhere
- Log:The log usually only gets written to when the program runs unattended through the command line. Checking this option will create entries in the log file for all transactions except viewing on the screen.
- Update: When the program starts, it goes out to HIPAAsuite's website and looks if a newer version is available. If so, it will pop-up a message listing the changes done between your release and the latest available. Some companies will not allow updates to a program without testing. In this case we recommend to check this option and have the program not look for updates.
- Document Color: In the next section you can indicate your color choices for the display of printable forms of the response report. You can have everything in black and white or you can choose to have the form elements such as frames and borders in red to make the document easier to read.
- Defaults: If you want to make your life easier when answering claim status requests, you can select one default value for your answer. For example you can choose **A2**: *"Acknowledgement/Acceptance into adjudication system-The claim/encounter has been accepted into the adjudication system"* as claim status category and **20**:"*Accepted for processing"* as a claim status. Now when you click 'Save' in the response form without filling in any values for status and status category, those values will be filled in.

3.3 Delimiter Setup

EDI is all about delimiters. By describing in the first 106 bytes of any EDI file which delimiters are used in the rest of the document the EDI file is machine readable. There are 4 delimiters used in HIPAA EDI.

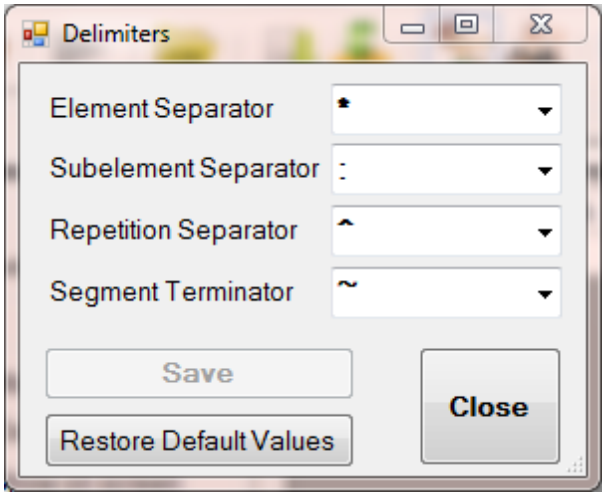
The element separator is the 4th byte of any EDI file. It separates the elements of the segments. All HIPAAsuite products default to * for the element separator.

The sub-element separator is defined in byte 105 and serves to divide elements further. HIPAAsuite default is the colon ':'

The Repetition separator is used since the 5010 version of EDI and indicated in ISA_11. Our default is the caret '^'

The segment separator is byte 106 and used to separate the individual segments of an EDI file. Our default is the tilde '~'.

HIPAAsuite products allow you to set the separators freely to any value that is allowed by the X12 committee. You use the following screen

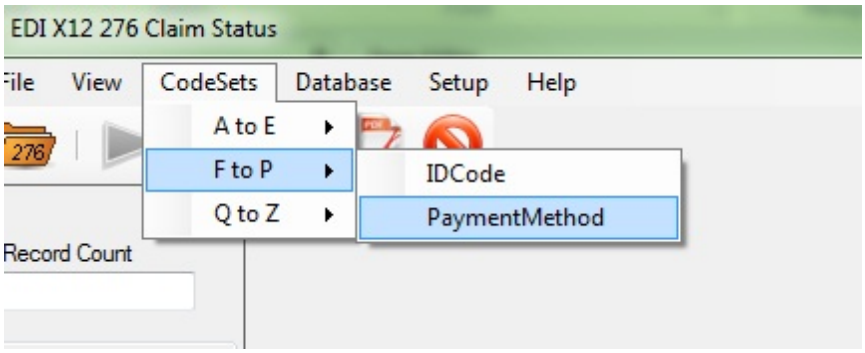


The delimiter screen

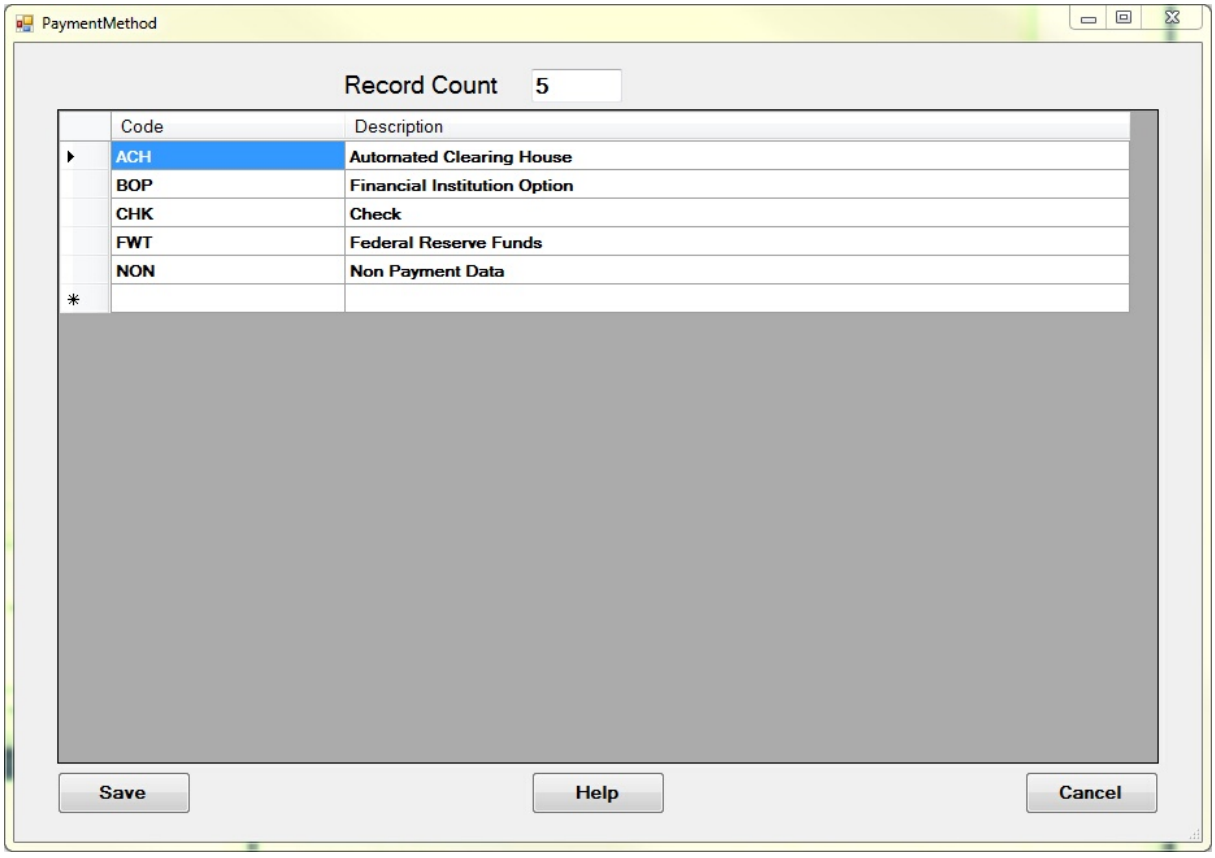
3.4 Code Sets

EDI relies on transaction code sets. These codes represent longer explanations and descriptions. At the onset of EDI one of the main design ideas was to make the EDI files as short as possible and to allow different languages to use the same descriptions by reducing long verbose explanations to 2-3 byte long codes. Computer storage was incredibly expensive and making any file larger than it absolutely had to be was considered wasteful.

The main menu of the HIPAA claim status Responder has the item 'Code Sets'. Click on it and sub menus will lead you to the individual code sets that the HIPAA Claim Status Responder uses. The code sets are stored in the file codesets.xml in the 'Configuration' subdirectory of the Program Data section of the HIPAA Claim Status Responder, usually C:\ProgramData\HIPAAsuite\HIPAAClaimStatusResponder\Configuration\Codesets.xml



The Transaction code sets

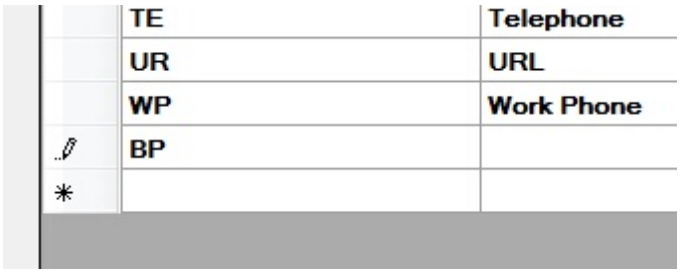


The code set editor

You can add, delete or edit codes.

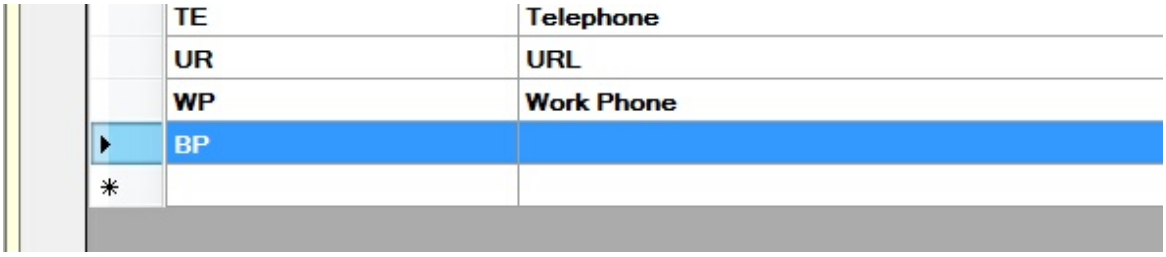
To Add, you type into the last row, and you see the grid change first into selected mode and when you click it again you are in edit mode. Now write your text. Note: Only after you leave this row will the changes take

click into the last row and the cell is high-lighted



Click again and you are in edit mode. See the little pencil symbol

To delete, click into the margin and high-light a row. Now press your delete key on your key board



Highlighting a row by clicking into the left margin

To edit, click into the cell that you want to change and make your changes. clicking or moving outside this cell makes the changes 'stick'

Don't forget to Save your changes by pressing the 'Save' button.

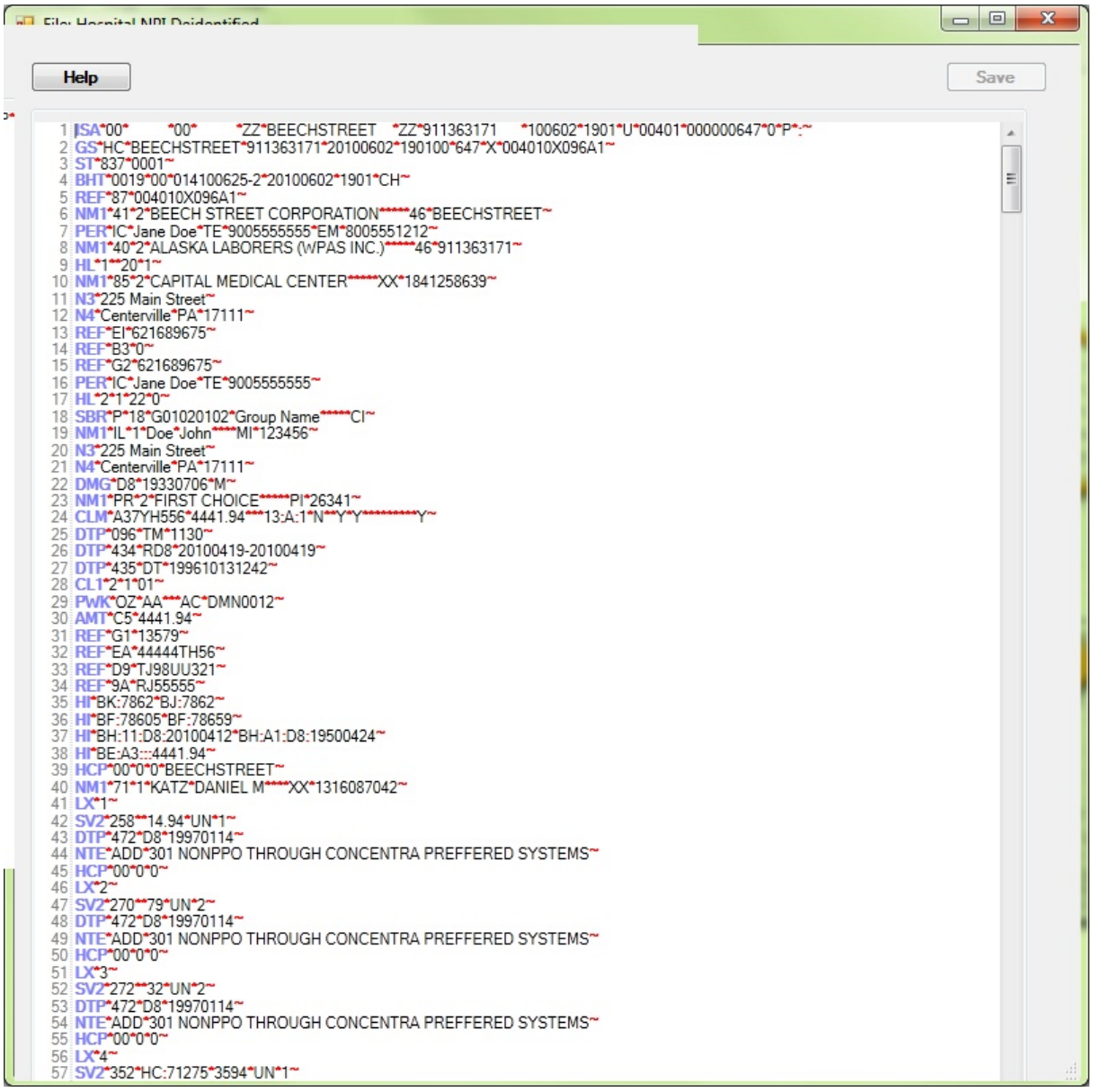
3.5 The EDI Editor

Enter topic text here. Under the menu item 'View' you have the option 'EDI Editor' plus you have the EDI icon on the toolbar to invoke the EDI Editor.

EDI files are often hard to read, especially if they have no carriage returns and line feeds to put each segment on a line of its own.

This option is only enabled when you have Opened an EDI File

When you click this menu option, the following screen will appear



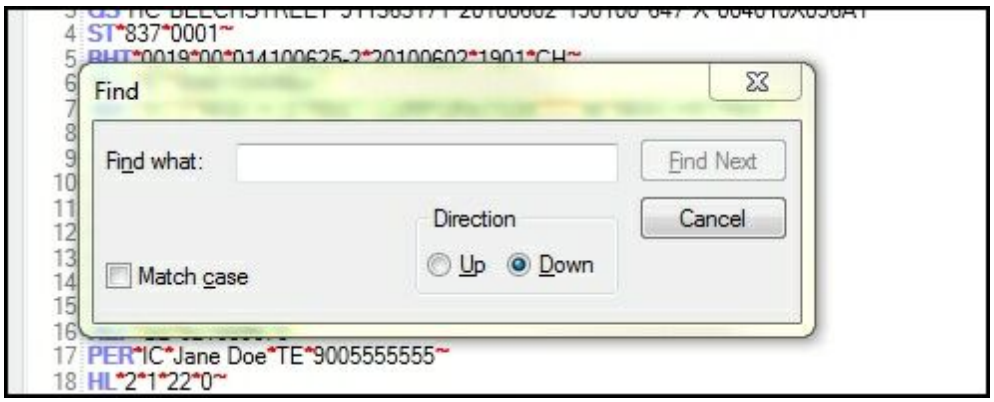
The EDI Editor

This Editor will replace all Element separators with a star '*', all sub element separators with a colon ':' and all segment separators with a tilde '~' even if the original file uses different delimiters. As long as you don't save, there will be no changes to the file.

When you right-click anywhere in the text, a floating menu will appear with typical test edit options such as cut, copy and paste,

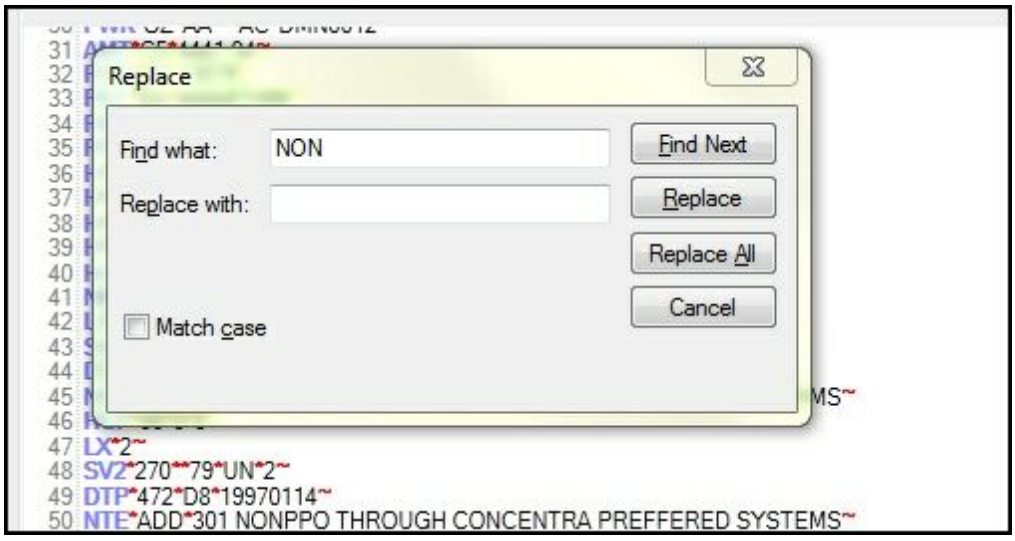
The floating menu of the EDI editor. right-click anywhere in the text to make it appear

Typing Ctrl-F brings up the text search utility



The search utility

Ctrl-H will bring up the replace utility



The Find and Replace utility

If you make changes to the file, the 'Save' button becomes enabled and you can save any changes. The HIPAA Claim Master will further work with those changed files, you don't have to open the file again.

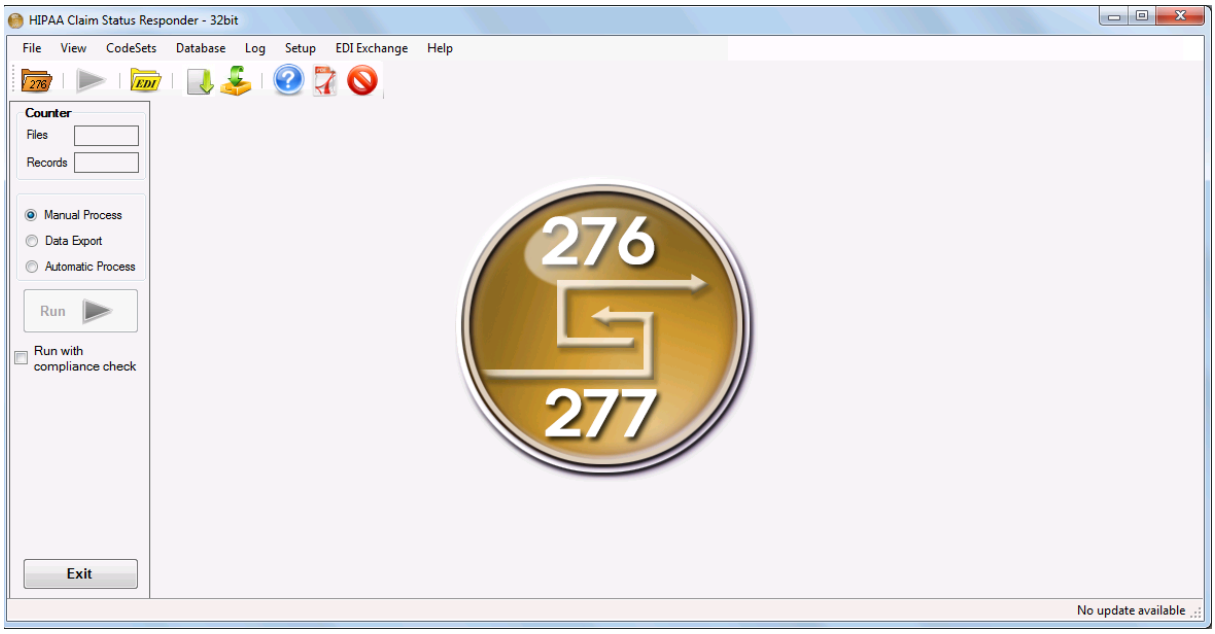
Changing EDI files can be a tricky undertaking. You should be experienced in the format of the 837 and understand that an 837 claim file could be a legal document that should not be altered without the consent of the originator.

4 Manually Processing Claim Status Requests

4.1 Running the program

The installation will add a new group called 'HIPAAsuite' under your Start --> Programs listing. When you click on the HIPAAsuite listing a sub listing called HIPAA Claim Status Responder will show. Click on it and the program will start.

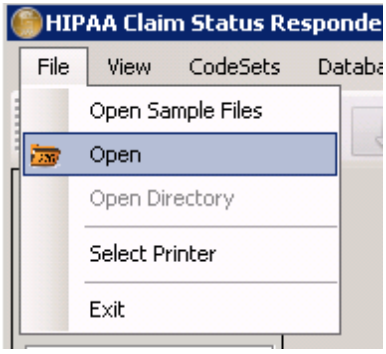
Once you click on 'Try' or when the software is licensed, immediately the main screen shows



The main screen of the HIPAA Claim Status Responder

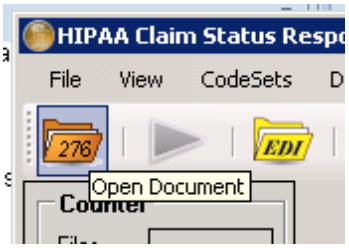
4.2 Opening an EDI file

You can either use the menu 'File' and 'Open'



The File Open menus

or the task bar icon the 'Open Folder' symbol

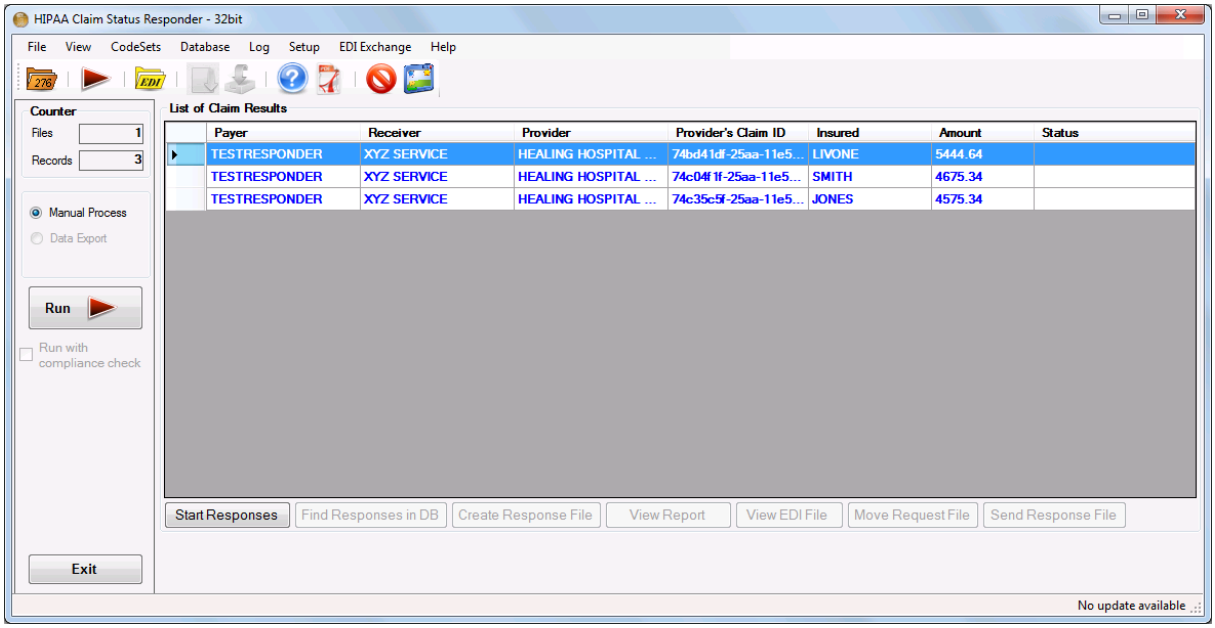


The task bar icon to open a fiel

to bring up the Windows File Chooser

Navigate to your 276 EDI file and select it.

Now you can click on the 'Read File' button and you will see the listing of individual requests in the request grid.



After parsing a 276 request file the individual requests are displayed

We can see that this particular 276 file contained 3 different requests. The spreadsheet lists the payer, the receiver of the response file and the provider and the claim number as well as the insured and the claim amount.

Please note that the last column with the status information is empty.

We can either double-click on a row in the request grid or by clicking on the '*Start Responses*' button. The '*Start Responses*' button will start with request number one. If

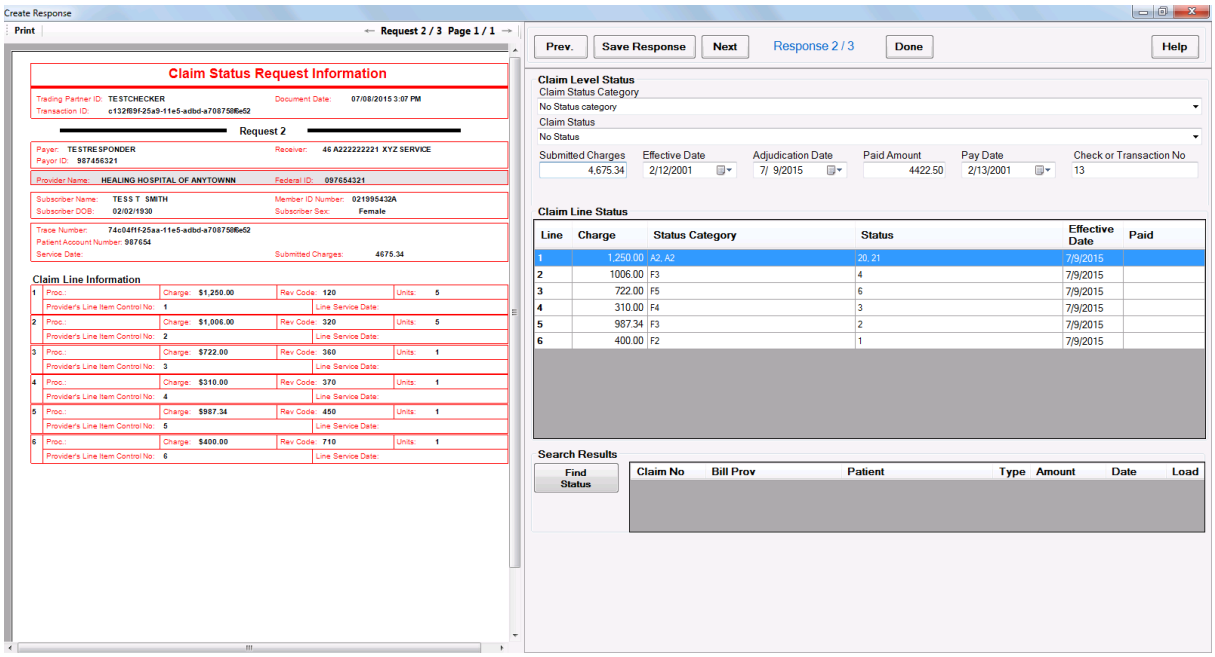
working with DataBase, clicking '*Find Responses in DB*' before starting work on the responses will preload the next step with information from the Database. This can also be done after having clicked '*Start Responses*' in the next window.

Once the status information has been added, one can create the response file by clicking on the appropriate button. Once the file has been created the 'View Report' and 'View EDI File' buttons will be enabled

The 'Move Processed File' button will move the file to the directory that has been specified in the setup.

4.3 Adding Status Information

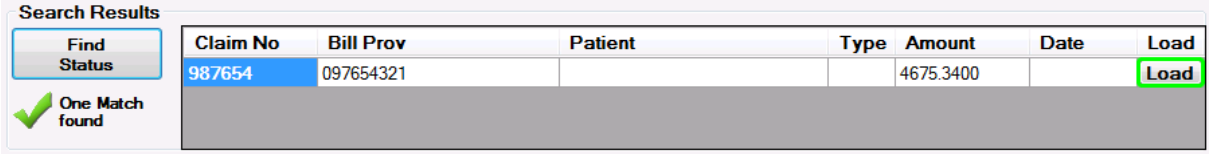
Once we double click a request in the request grid or click the 'Start Responses' button a new screen pops up.



The screen to create the response. In this example the Claim Status and Status Codes are filler meant for demonstration.

The above picture shows us how to work with an individual request. The left side which is also a printable image, gives us all the information contained in the request. These example lines were found by preloading the response data by clicking '*Find Responses in*

DB' in the previous window. The same effect can be had by clicking '*Find Status*' in this window and then loading the claim presented:



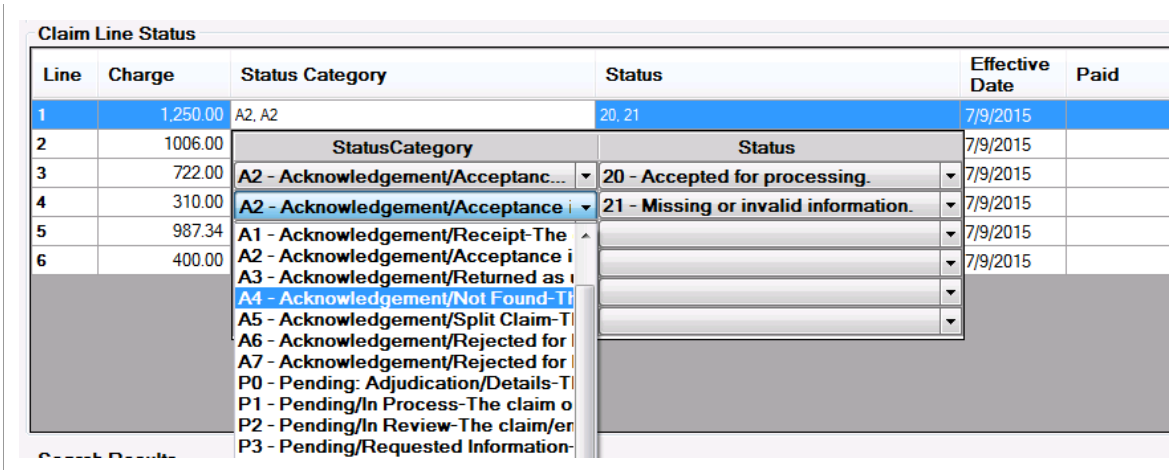
Loading a claim from DB.

In the above case the patient was the subscriber. Otherwise we would see two tabs in the upper right section, one for the subscriber, one for the dependent.

Dependent information in addition to the subscriber's information

The right side of the screen allows a user to enter manually the claim status codes on the Claim or Line level.

> The manual mode of the HIPAA Claim Status Responder allows six pairs of status and status category per claim level or per line level. Category and status information can be selected from six drop-down cells that are generated when the desired Status Category or Status cell to be edited is clicked. To keep these changes, click anywhere else on the *Claim Line Status* grid. To delete one, select the first option of "*no Status Category*" or "*no Status*" or click the grid row and press Delete.



Filling in the Line Level Claim Status for Line 1 of a Claim Status.

The middle part allows us to input the status information on the claim level as well as adjudication dates and payment information. There are two drop down combo boxes that allow you to select a status category and a status on the claim level. Do this only if there is no information for the line level available. Generally you want to put the status information on the service line level.

If there is line information in the request, the lower part of the screen will list this under the "*Claim Line Status*" grid and allow for the input of the status information at the line level. In our database model we allow for six Status Categories and a Status field for each one per Claim Line as each represents a maximum of two STC EDI segments. The data

The Source tables and the Claim Master tables options handle these differently, as the Source tables have a field for each of these six Claim Statuses

	LineItemControlNo	ClaimID	StatusCategory	Status	Status1	StatusCategory2	Status2	StatusCategory3	Status3	StatusCategory4	Status4	StatusCategory5	Status5
1	1C	1	A0	0	1	A2	2	A3	3	A4	4	A5	5
2	IC	2	A0	1	2	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL

Claim Status Codes and Categories in the ClaimStatus Responder's SourceDetail table.

while the Claim Master tables have only one pair of fields which holds all six possible Status Category / Status pairs.

	ID	ClaimID	LineNumber	ClaimStatusCategory	ClaimStatus
1	1	1	1	F1:F2:F3	2:3:4
2	7	2	1	F1:F2	1:2
3	13	3	1	NULL	NULL

Claim Status Codes and Categories in the Claim Master's ClaimDetail table.

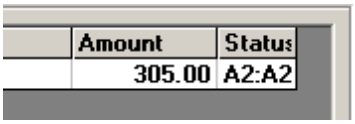
Once the status information has been added, it can be saved by clicking the '*Save Response*' button.

Save button on the top of the Create Response window.

4.4 Creating the Reponse

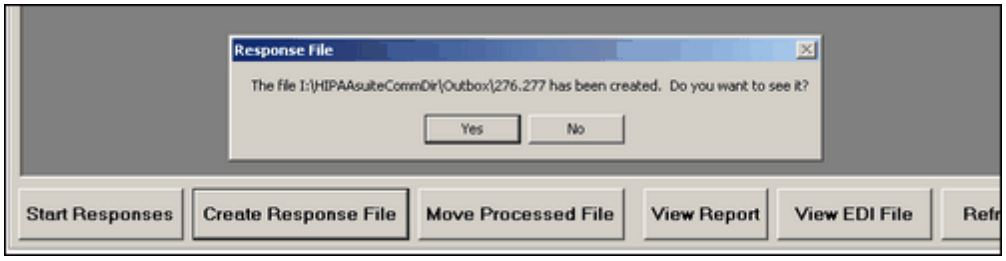
Once all the status information has been added or if you decide to return default status information you can create the response file.

You will see that status information is present in the last column of the request grid.

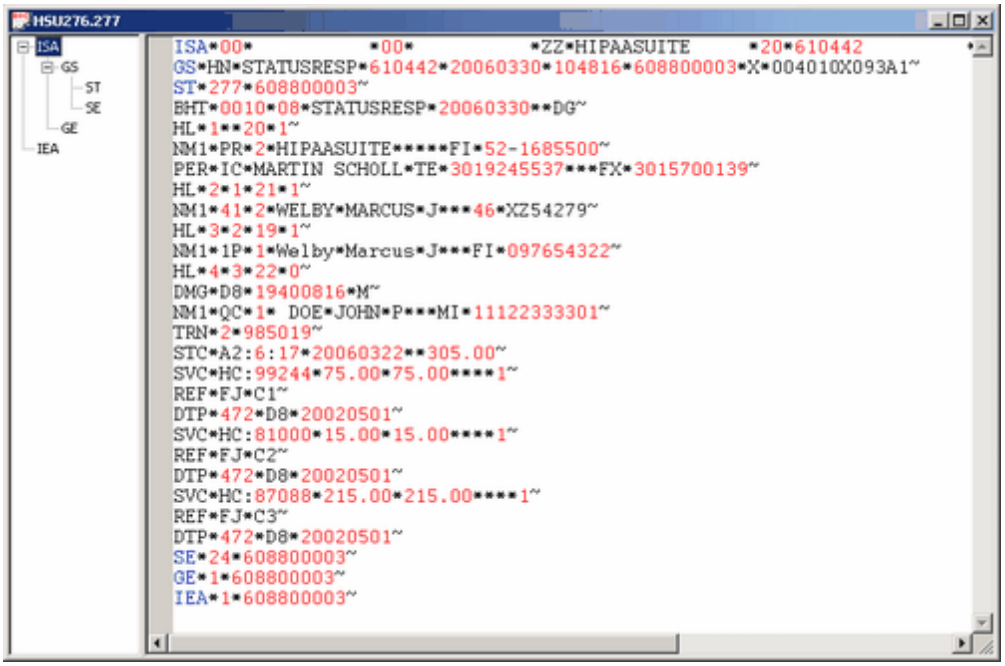


The last column of the request grid contains now a value

If you click the 'Create Response File' button you will get a message that the file was created. The filename of the response is the name of the incoming 276 request file with a ".277" file extension. You have the choice to view it if you have the The EDI Editor installed.



The message that the response file has been created.



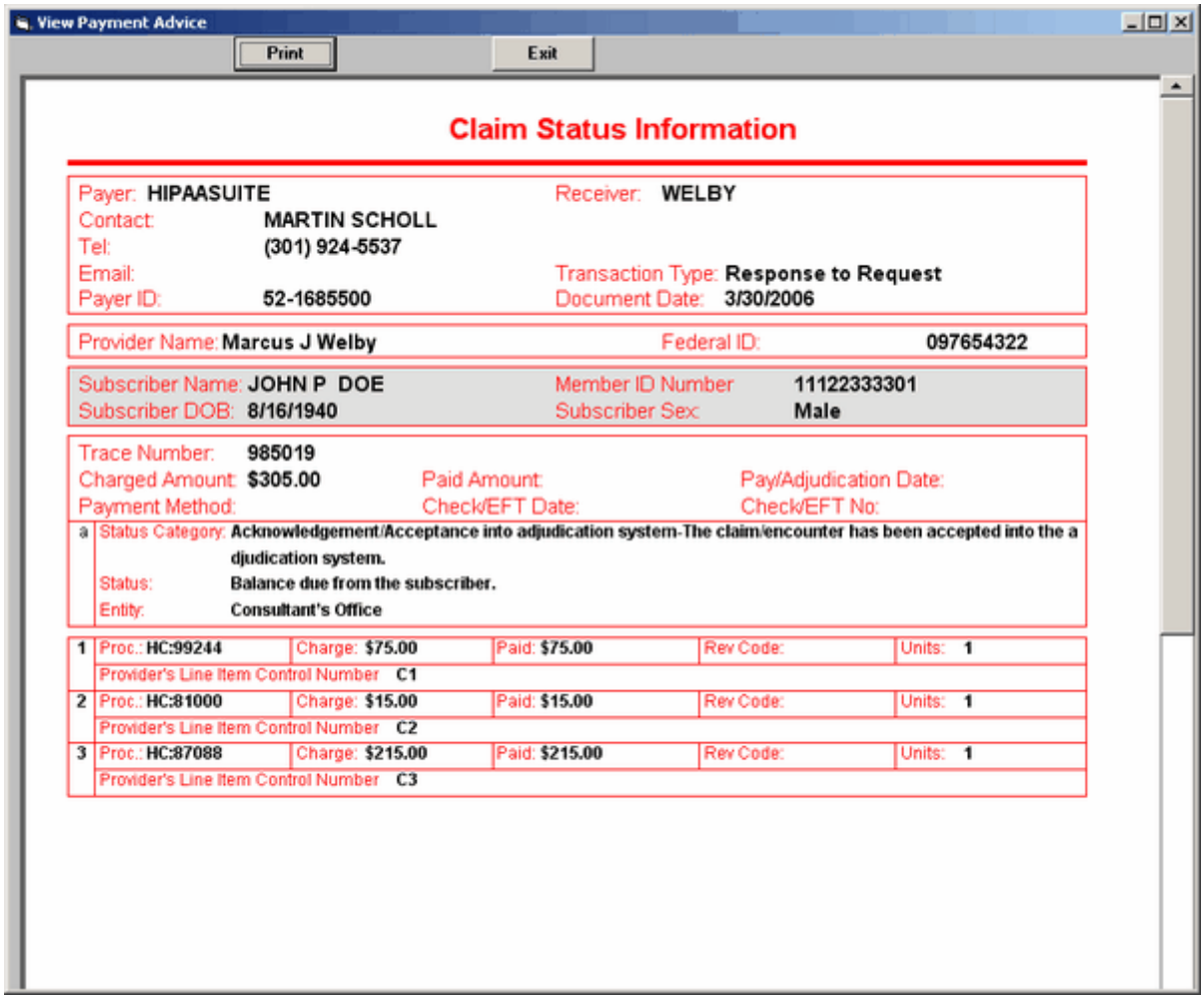
The 277 response file

You might want to move the request file to the processed file folder, to make sure it does not appear again. Just click the 'Move Processed File' button and the file will be moved to the directory that you specified in the Setup screen.

4.5 Viewing the Response as Report

The HIPAA Claim Status Responder has a built-in report generator that translates the EDI document into an easily readable report that can be printed.

If you click on the 'View Report' button you will see a screen like this:



Viewing the response file as report

This report is designed to make the 277 EDI file viewable to the non-EDI specialist. It translates the codes into its descriptions.

You can print this report to your Windows printer by clicking the "Print" button.

5 Database Interaction

5.1 Introduction

The whole idea of EDI is ability of disparate computers to communicate without the

involvement of human being. So while the manual answering of claim status requests is possible, there are certainly limitation on how many request a case worker can handle per shift. And with the introduction of the Affordable Care Act it is now necessary for payers to implement real time interfaces to allow providers instantaneously with responses to their claim status and eligibility requests.

So the real challenge is to connect the HIPAA Claim Status Responder with the back end system and get access to the live data.

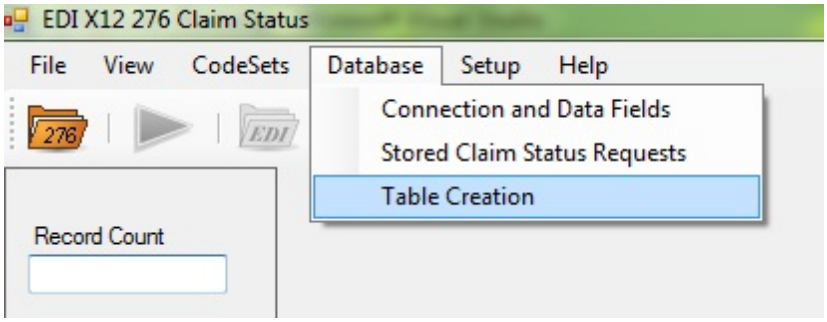
The HIPAA Claim Status Responder has a database interface that allows one to

- export the request data in an SQL compliant database such as Microsoft SQL Server, mySQL, Access or Oracle. The data is placed in two hierarchical tables, EDI_ClaimStatusHeader and EDI_ClaimStatusDetail.
- Write the response given to the request record
- Search in claim tables for the status of a particular claim
- encapsule the claim status into a 277 file.

There are scripts provided and a screen to generate those tables for a few important databases such as Microsoft SQL Server, the open-source database mySQL and Oracle.

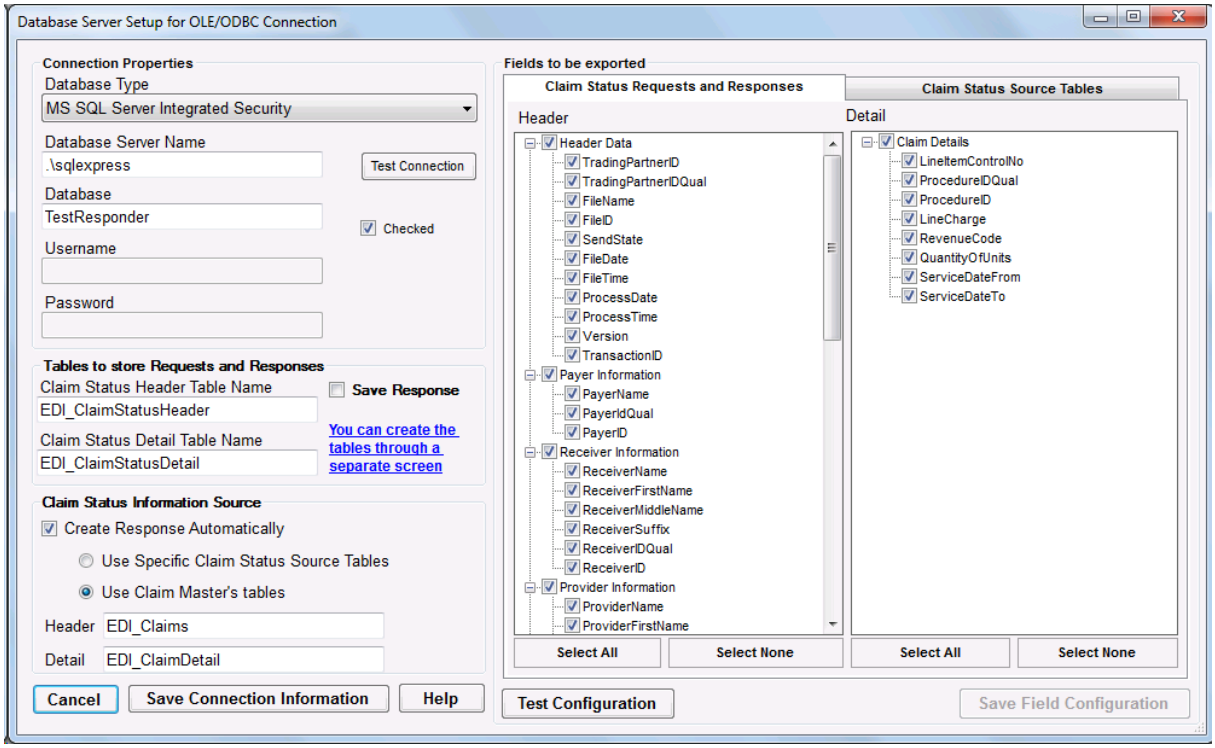
5.2 Database Setup

Under the main menu item 'Database' the first option is "Connection and Data Fields"



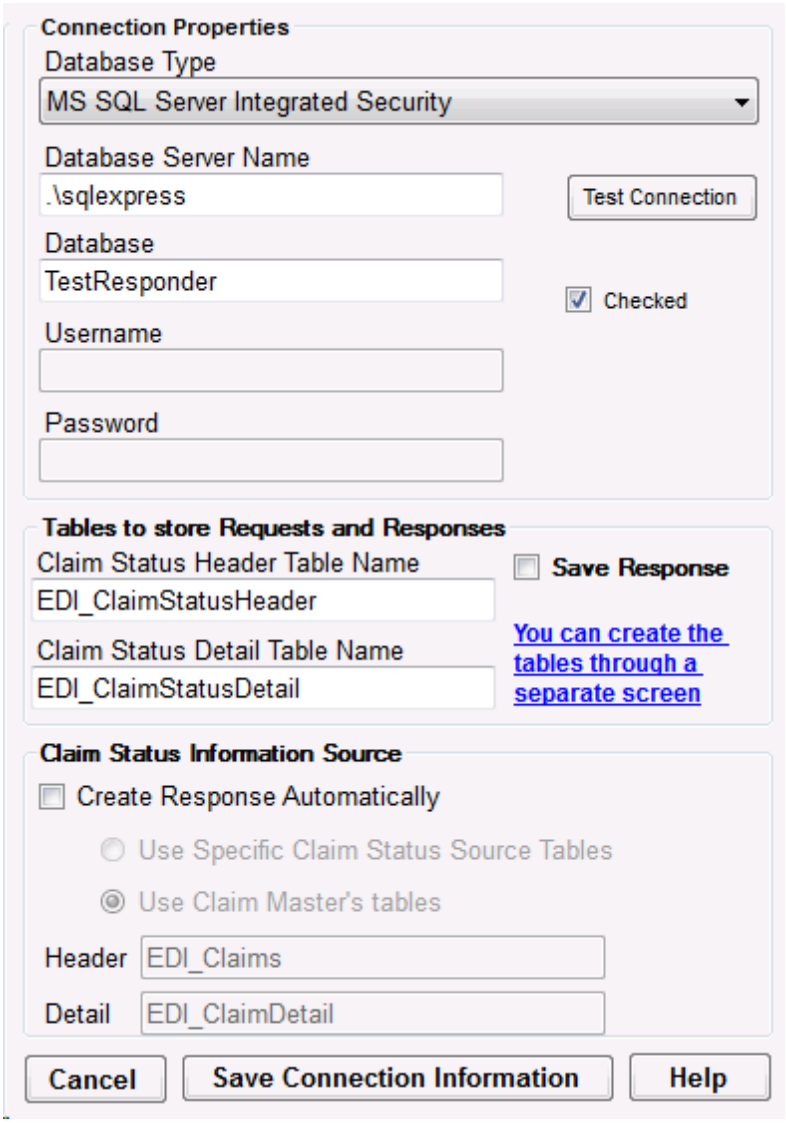
The menu under 'Database'

When you click on it the following screen comes up



Database connection and data fields

On the left side of the screen you see the connection setup, here again in detail



Defining the connection parameters

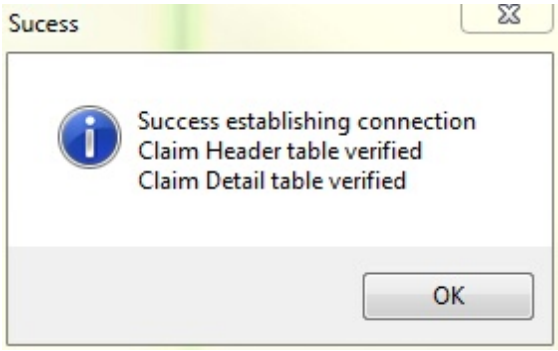
- Database Type --- is either ODBC or Microsoft SQL Server either with Windows Authentication or with explicit credentials (If you need other types, please contact us for customizations)
- Database Server Name or DSN --- In case of SQL server this is the IP address or the name of the database server, for ODBC this is the Data Source Name (DSN) that is defined through the ODBC setup in the Control Panel of Windows
- Database --- This is the database under the above connection, usually not needed in ODBC setup.
- Username --- A defined user that has privileges to the database, usually not needed in ODBC setup
- Password --- Usually not needed in ODBC setup.

- Claim Status Header Table Name --- The name that you give to your Claim Status header table. A default name is suggested but can be changed
- Claim Status Detail Table Name --- The name of the table that contains the line information. A default name is suggested but can be changed

You can create the tables through a separate screen.

After filling in all the information, save the information and test the connection by clicking on the "Test Connection" button.

After establishing a connection and the existence of your tables is verified, you will see a message

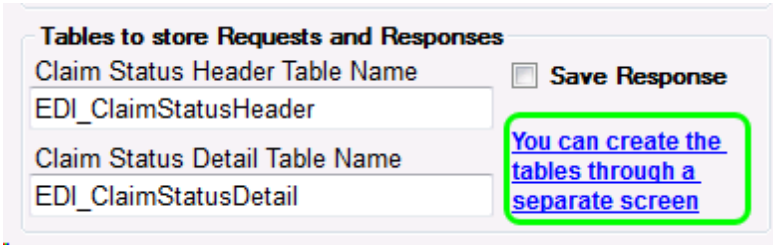


Establishing a connection to the database

You cannot export Claim Status requests before this connection tests successfully.

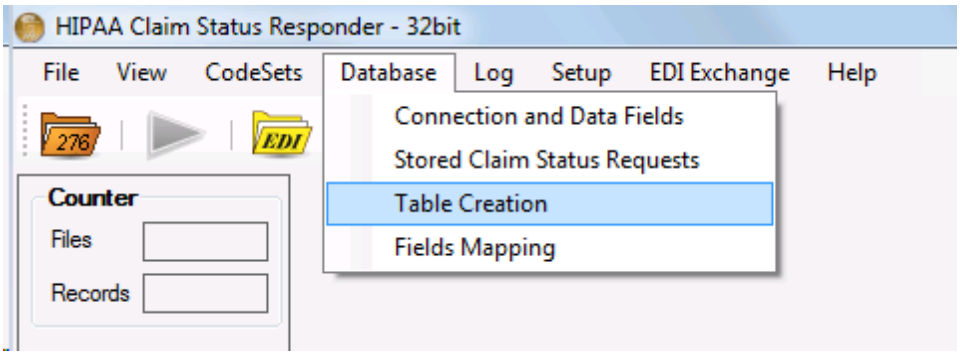
5.3 Creating the Tables

The HIPAA Claim Status Responder can create the tables needed to export data to the database. Once you have the connection to the database configured and tested you can go to the "Create SQL tables" screen by clicking the blue text that reads "*You can create the tables through a separate screen*"



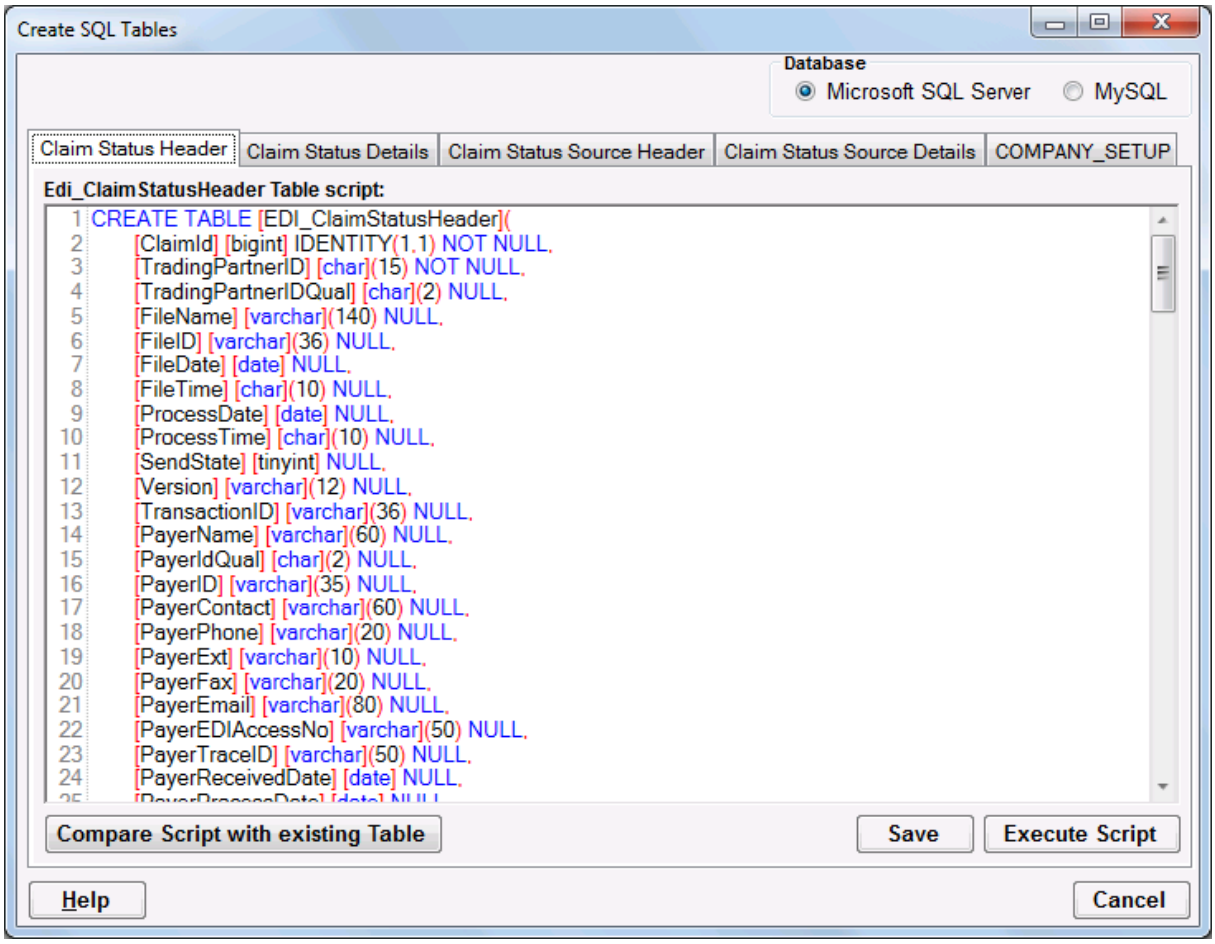
Link to create tables in "Database and Connections" window.

or selecting the "*Table Creation*" option under the "*Database*" dropdown menu.



Clicking "Table Creation" leads to the Create SQL Tables window.

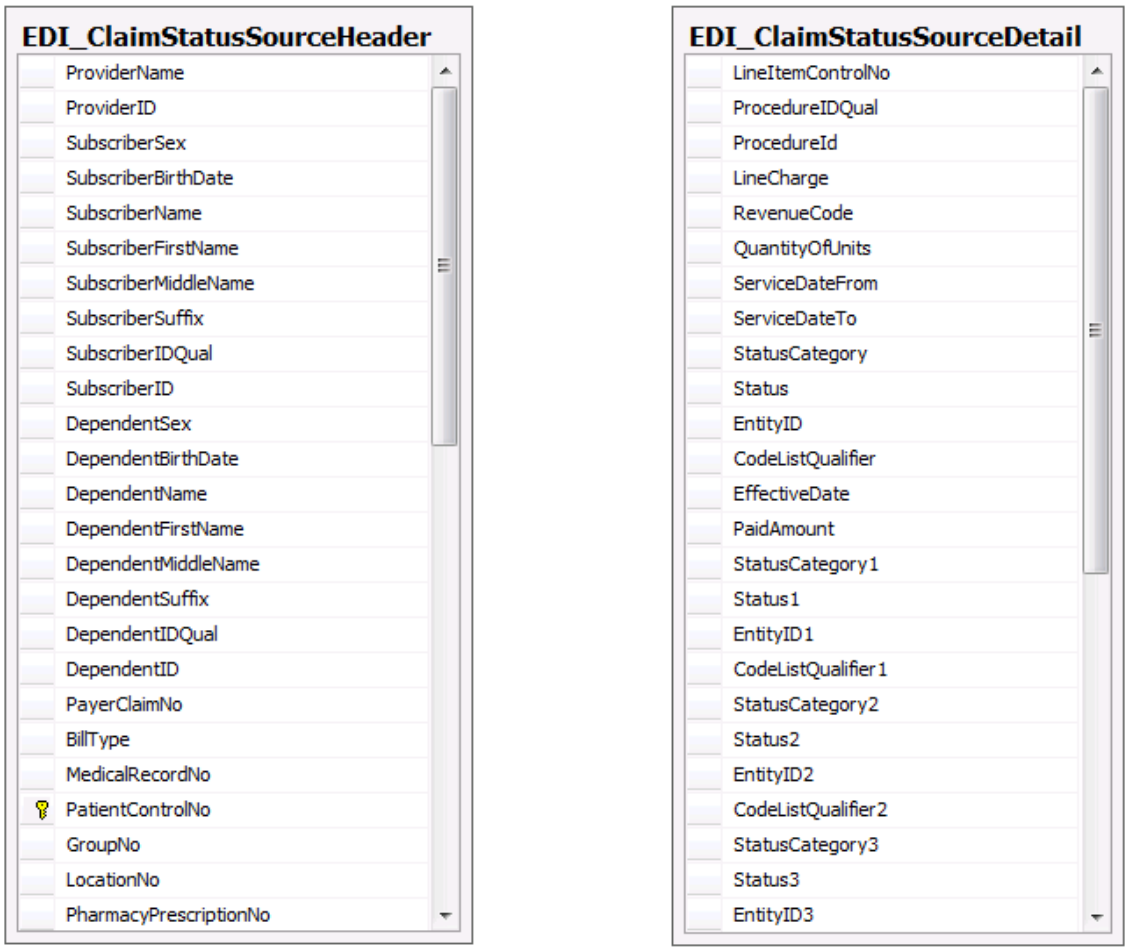
This is the "*Create SQL Tables*" window:



SQL scripts to create the Claim Status tables. Tabs separate the different tables.

What you see is the SQL scripts used to create the tables. The product comes with two versions, one for Microsoft SQL Server, the other for mySQL. If you have a different database you will have to manipulate the scripts until they work. You can change the scripts in this window and save them.

The *Claim Status Source Header* and *Claim Status Source Details* tables are unnecessary if you plan on using the Claim Master to answer Claim Status inquiries.



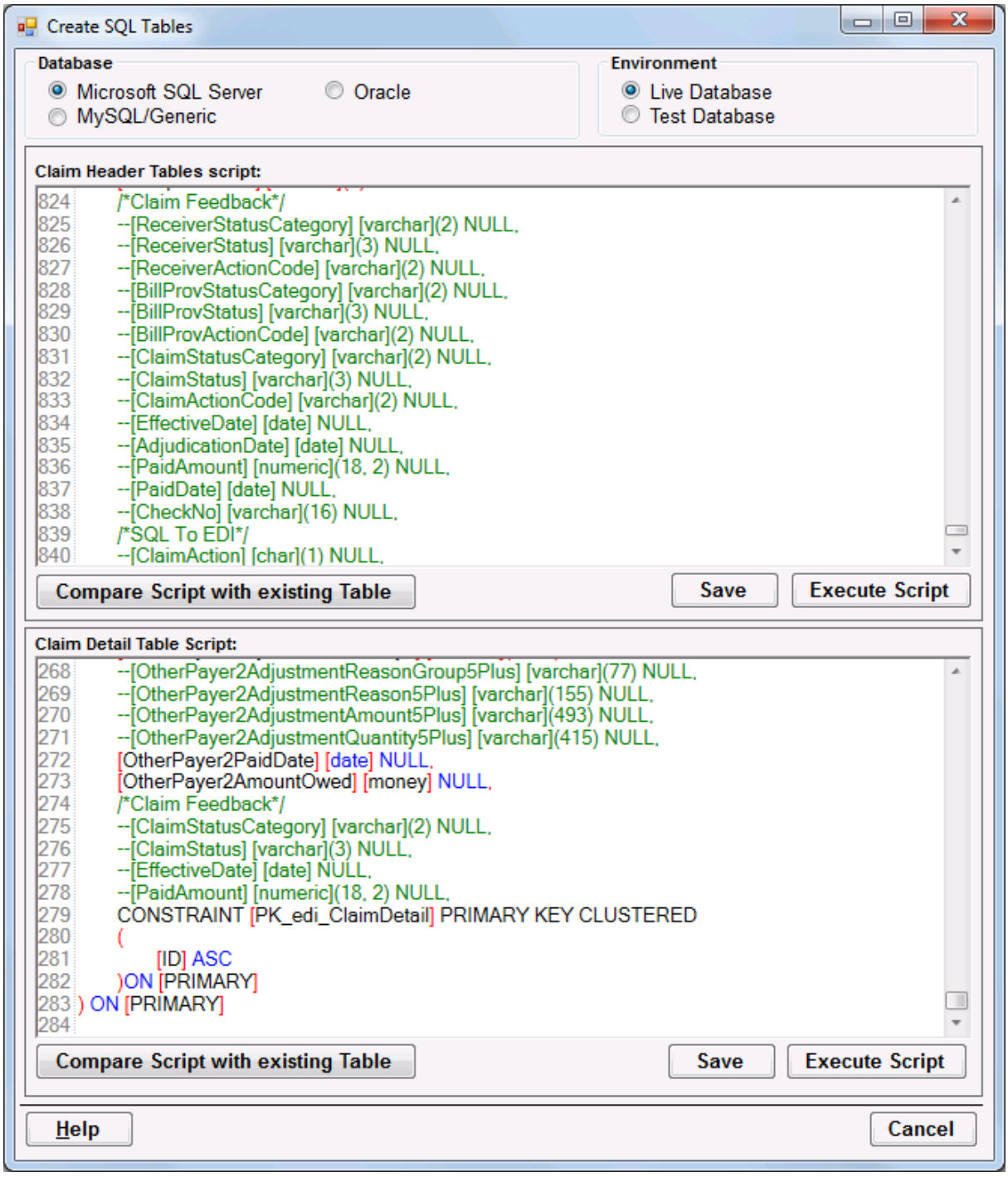
-

Source tables schema.

Using the Claim Master Tables

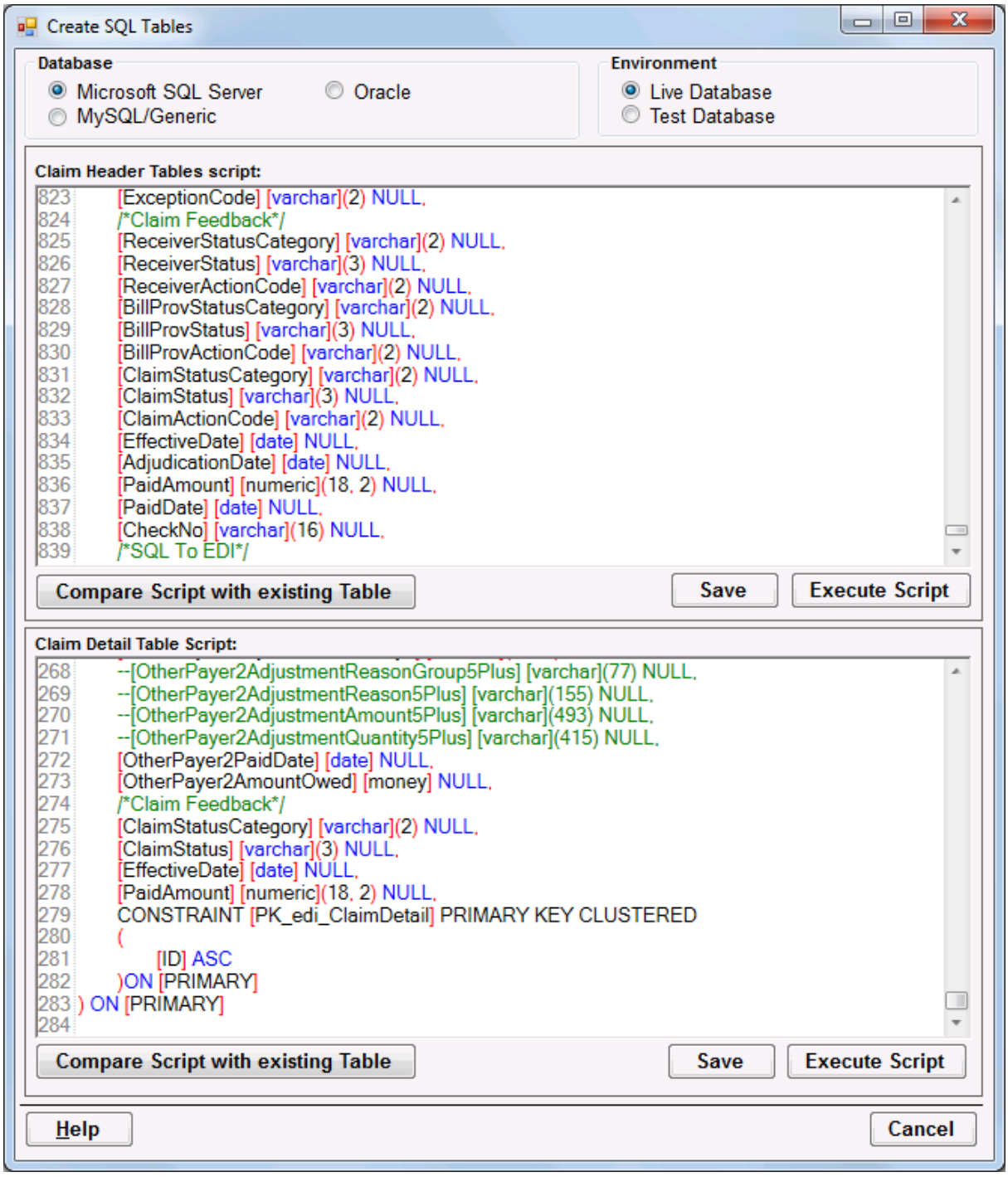
To use the Claim Master tables as a data source for your Claim Status information, some changes need to be made from the HIPAA Claim Master. The following instructions all apply to the HIPAA Claim Master.

Because the Claim Feedback fields are not necessary to operate the Claim Master by itself, they have been preceded by double hyphens ("--") and so are effectively ignored by the database engine.



"--" to write comments in SQL.

To add them to the Claim Master tables, remove the "--" characters preceding the *Claim Feedback* sections of the table creation scripts.



Removing the "--" characters means these lines are no longer comments. Their color changes to reflect this.

If the tables have already been created, click *Save*, then click *Compare Script with existing Table*. This will present you with the changes to be performed on your existing Claim Master tables. Click *Execute Script* to perform the changes. Do this for both the

Claim Header and Claim Detail tables. No data will be overwritten or erased as these are new columns to be added.

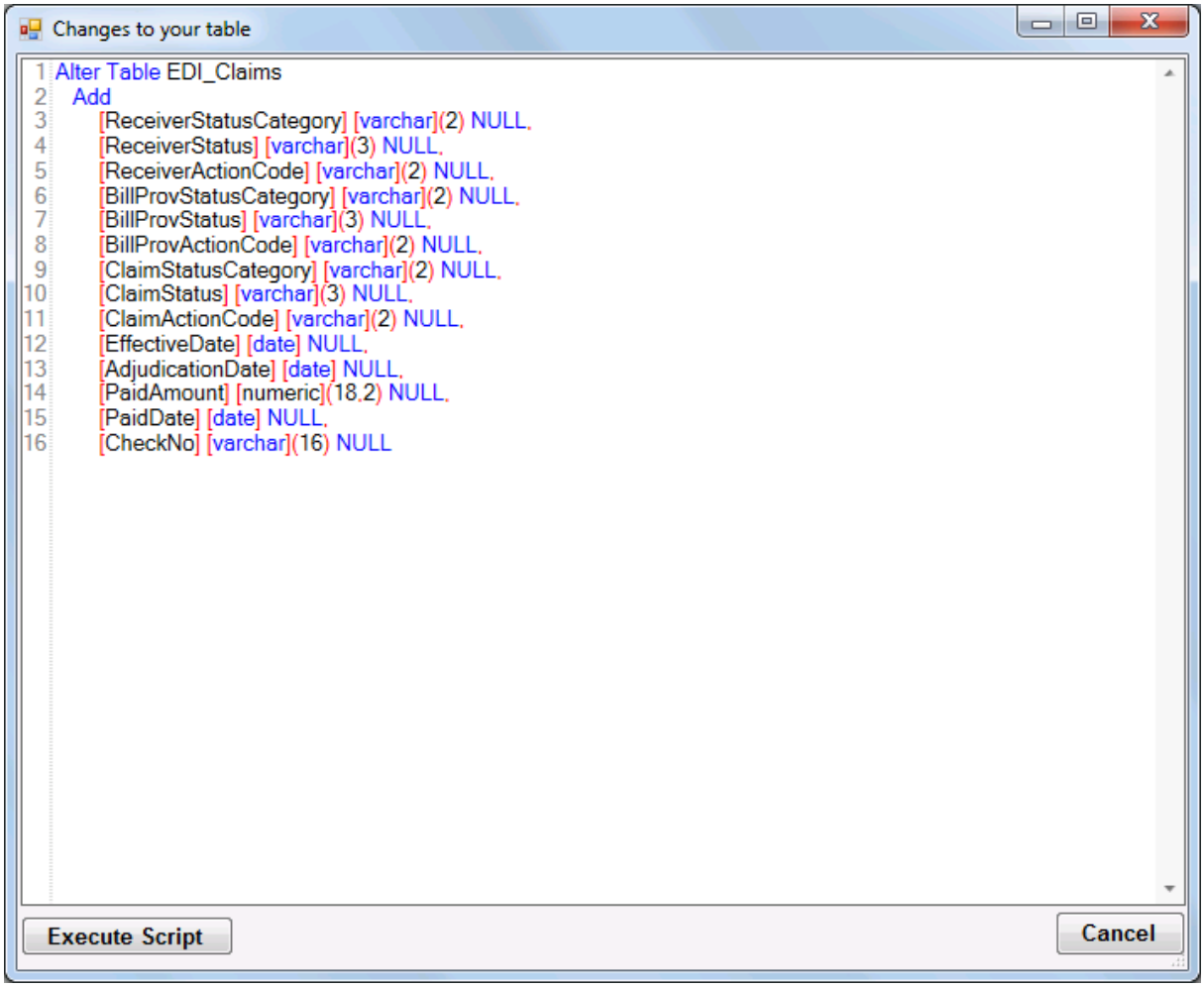
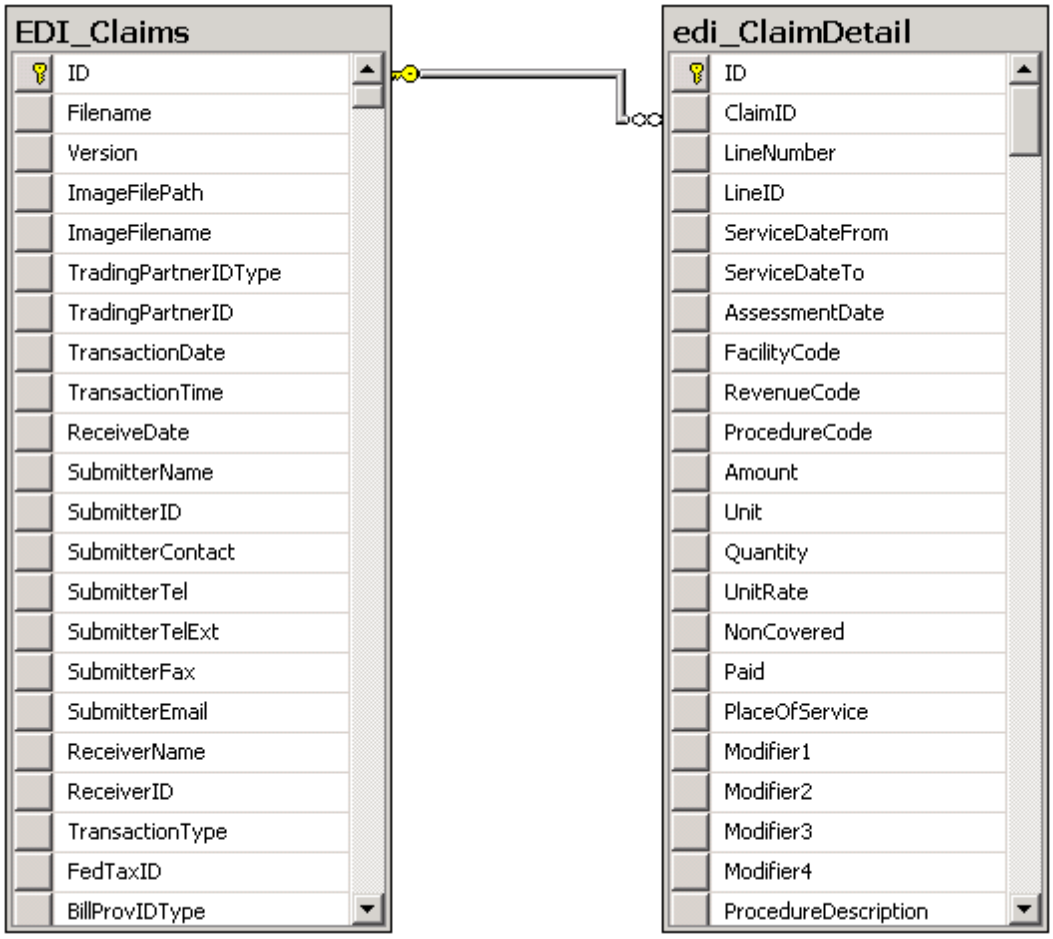


Table changes prompt.

If the Claim Master tables have not yet been created, click *Save*, then click *Execute Script*. Do this for both the Claim Header and Claim Detail tables.

The Claim Master tables now have the requisite data fields to store all necessary Claim Status information to be used as a data source by the HIPAA Claim Status Responder.

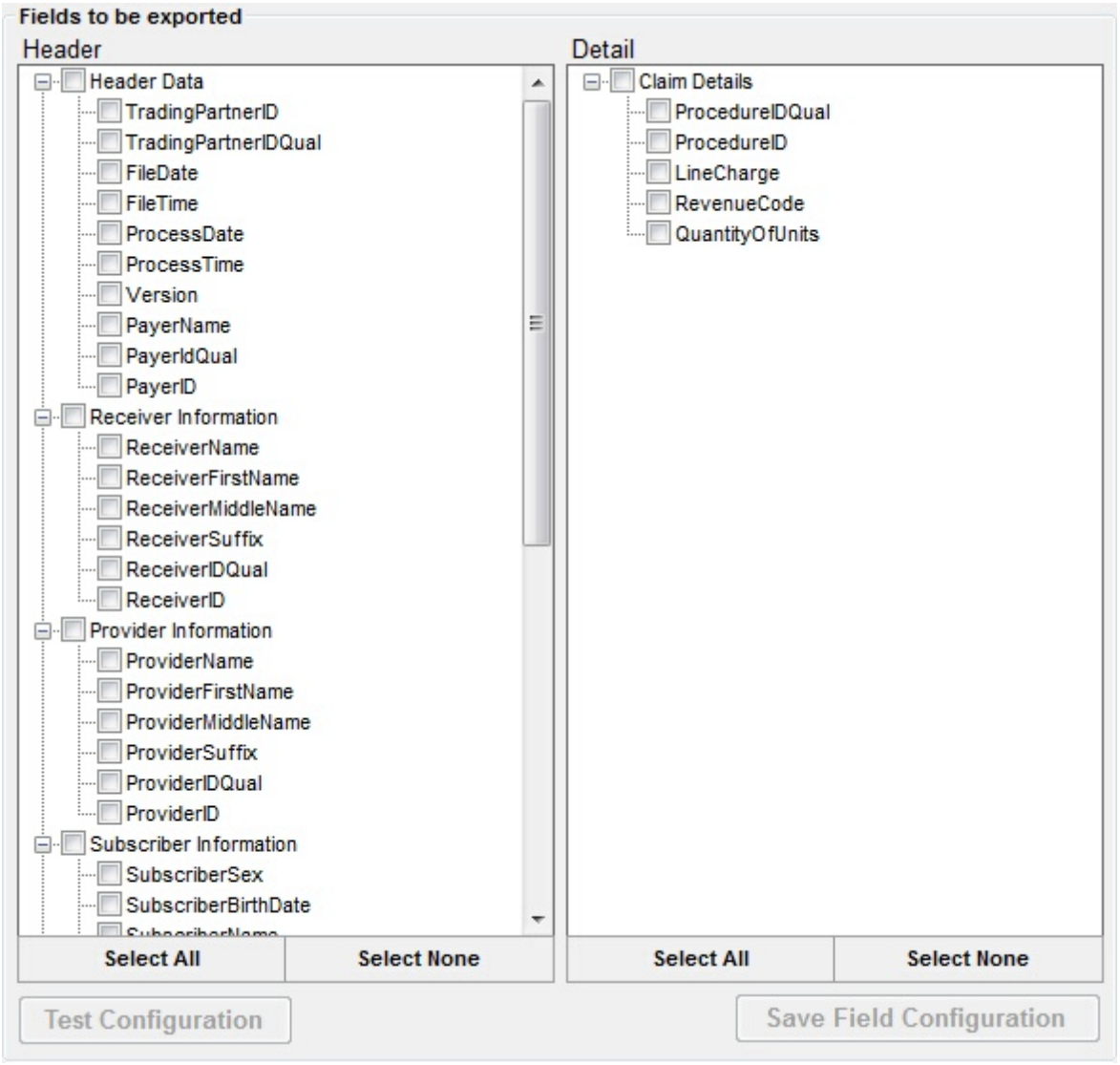


CM tables schema.

5.4 Field Selection

5.4.1 Field Selection

The field selection part of this form lists all the fields that the program works with internally. We recommend selecting all fields; use the "*Select All*" button to save time. You need to test the configuration before you can save it.



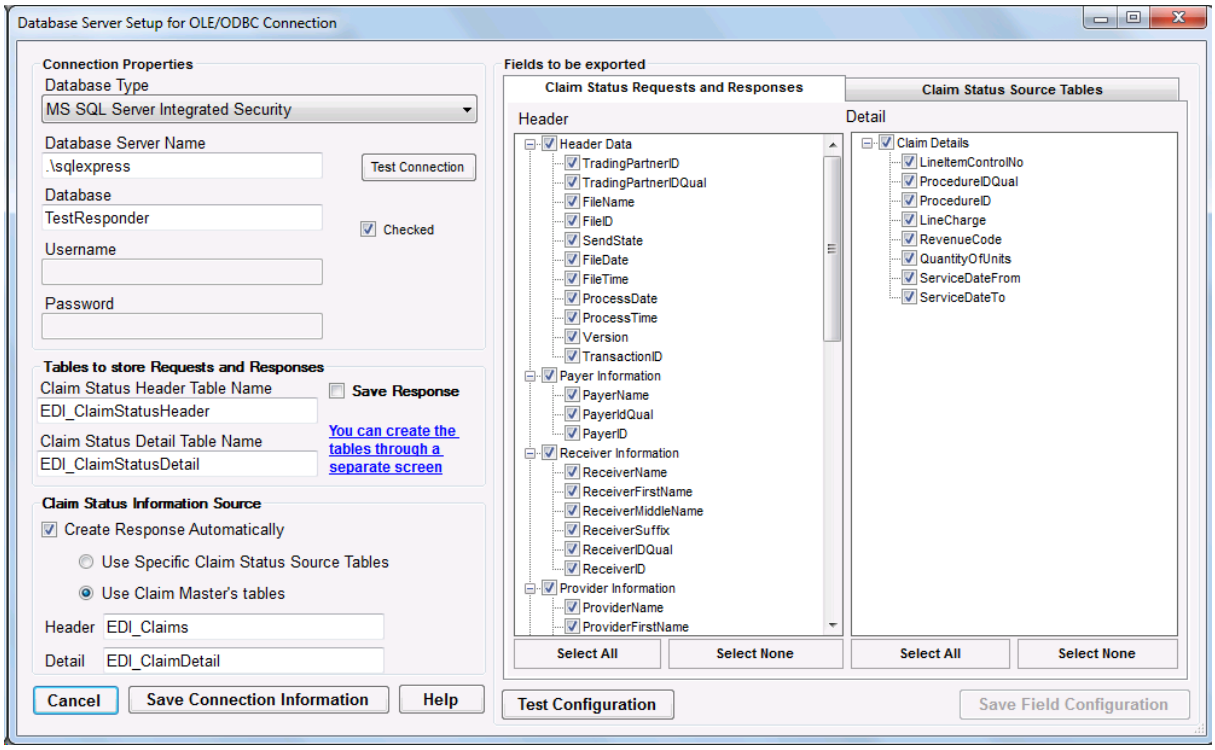
selecting the fields to be exported

If you have errors with individual fields checking out, a screen comes up that lists the fields in error and allows you to deselect them.

5.4.2 Using Claim Master

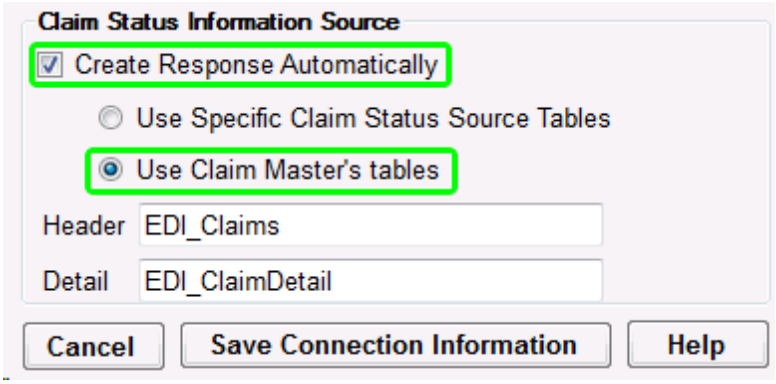
The following steps detail how to use the Claim Master tables as a source for claim statuses:

1. Open the Claim Status Responder Database Connection and Data Fields configuration window.



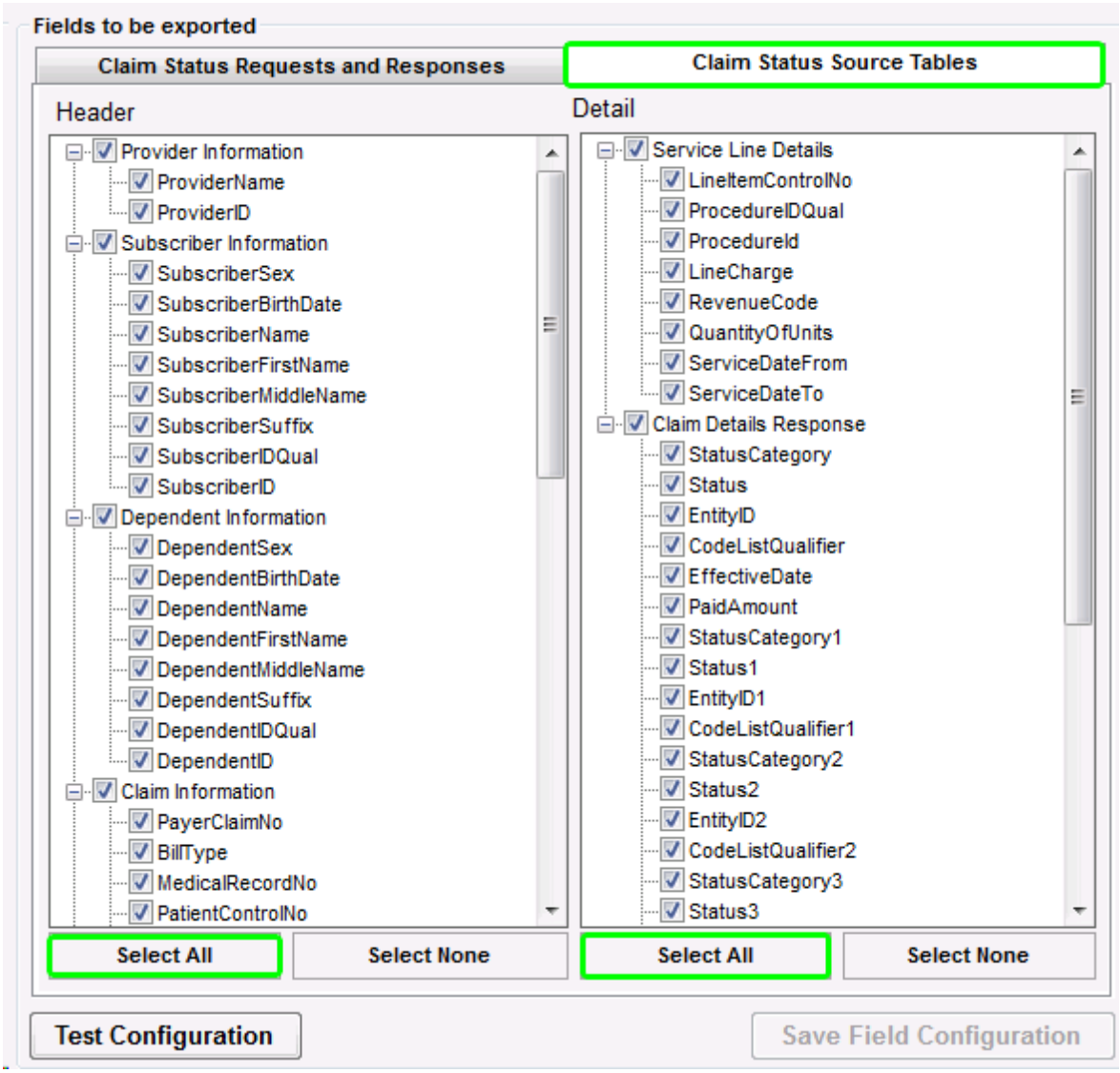
Database Setup form.

2. Check *Create Response Automatically* and select *Use Claim Master's tables* radio button. Verify the Claim Status *Header* and *Detail* fields contain the correct Claim Master Header and Detail table names. Click the *Save Connection Information* button.



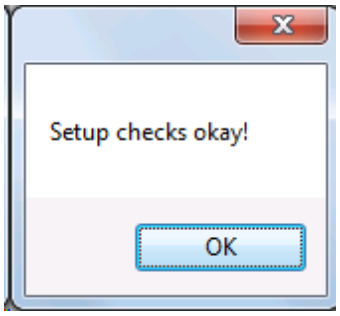
Claim Master tables selected.

3. On the right half of the configuration window, select the *Claim Status Source Tables* tab and check all necessary fields. The ClaimStatus Responder will read these to build a Claim Status response.



All necessary Claim Master fields checked.

4. Click the *Test Configuration* button. This will verify all checked fields for their existence in the Source tables.



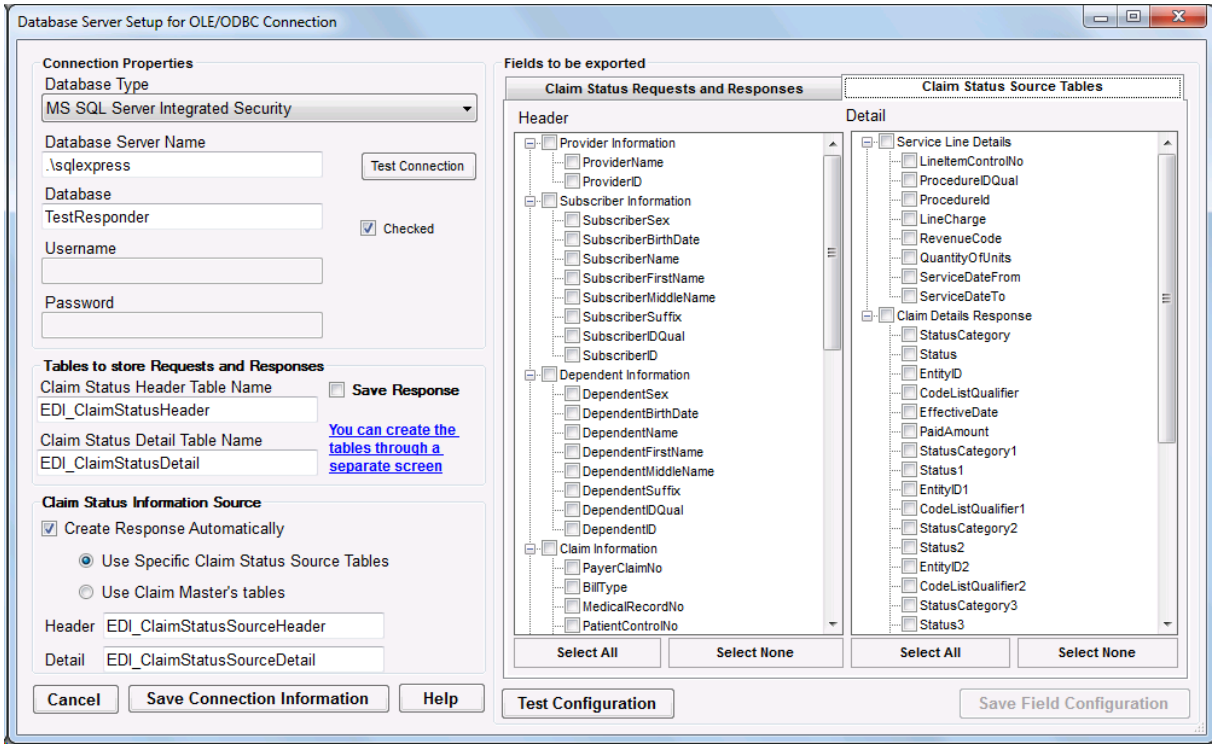
Claim Status Fields tested.

5. Click the *Save Field Configuration* button. The table names and fields are now saved and will be used to look up Claim Status information.

5.4.3 Without Claim Master

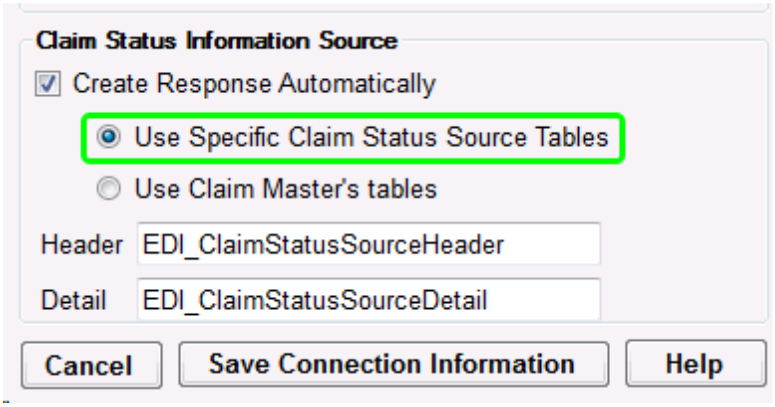
The following steps detail how to use the Claim Status Source tables as a source for claim status information:

1. Open the Claim Status Responder Database Connection and Data Fields configuration window.



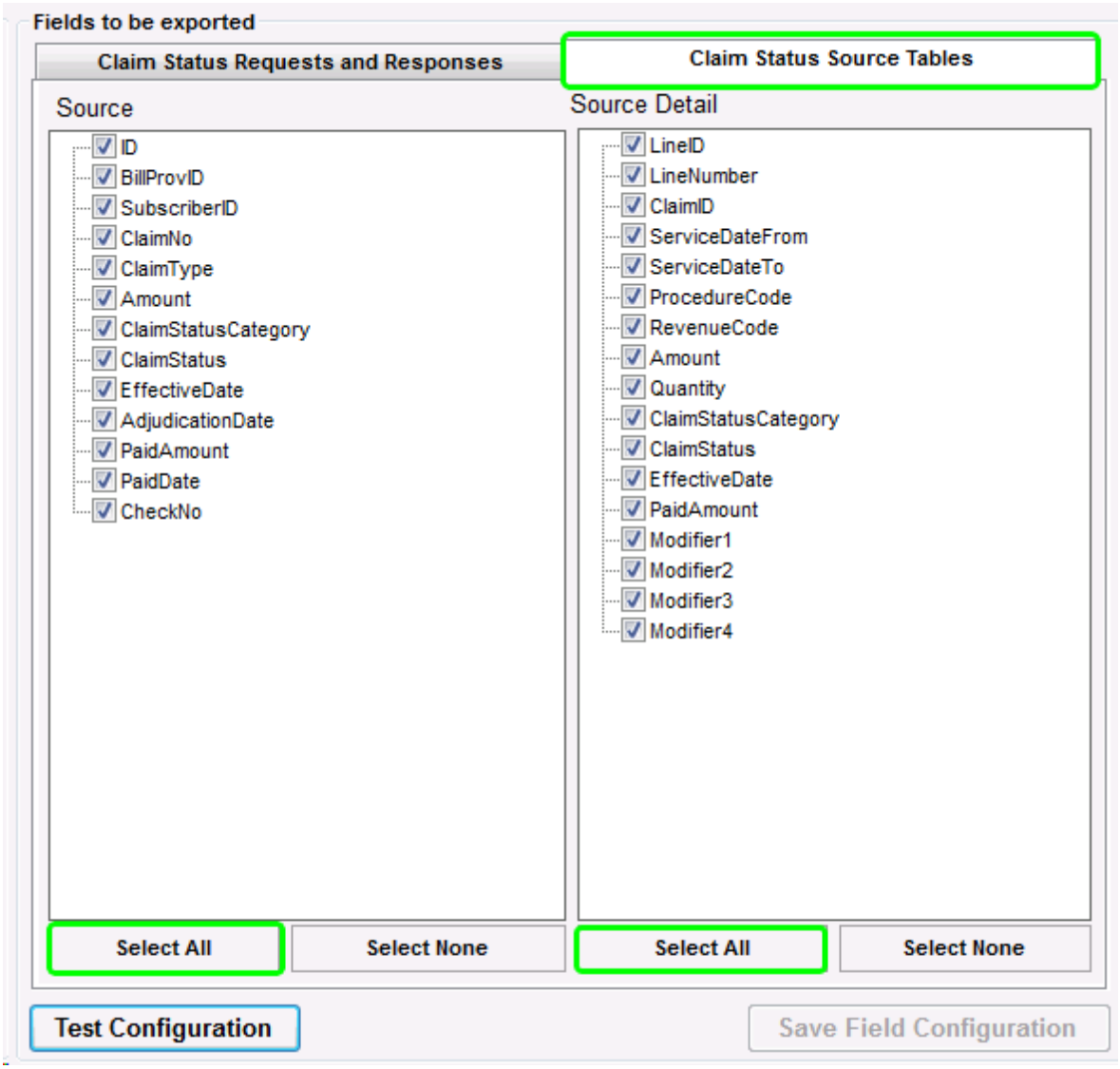
Database Setup form.

2. Check *Create Response Automatically* and select *Use Specific Claim Status Source tables* radio button. Verify the Source *Header* and *Detail* names and click the *Save Connection Information* button.



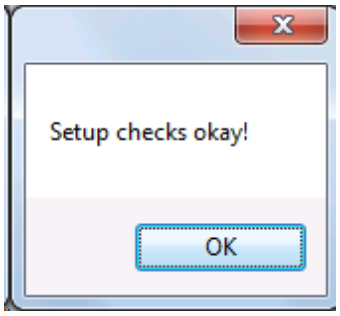
Source tables selected.

3. On the right half of the configuration window, select the *Claim Status Source Tables* tab and check all necessary fields. The ClaimStatus Responder will read these to build a Claim Status response.



All necessary Claim Master fields checked.

4. Click the *Test Configuration* button. This will verify all checked fields for their existence in the Claim Master tables.



Claim Status Fields tested.

5. Click the *Save Field Configuration* button. The table names and fields are now saved and will be used to look up Claim Status information.

5.5 Renaming Fields

You can rename the fields listed for selection. The long field names that the HIPAA Premium Payment Master uses for the data export might be too long for some databases. IBM AS400, Clipper and other legacy databases cannot work with overly long filenames.

For this reason you can change the filenames to any name that you wish, as long as there are **no blank spaces** in the name.

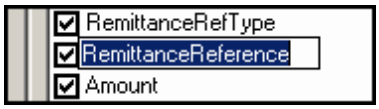
The HIPAA Claim Master lets you change the names of the columns that you select for export. All you have to do is

1. Click twice the field name. Do not double-click, but click slowly twice. You will see that the field name is now editable.
2. Change the name to your value and leave the field by clicking somewhere else
3. Your field name has now been changed
4. Don't forget to save the new settings

Selecting a field

Click again, do not double click, on the label and you see that suddenly there is a frame around the name and the curser is placed at the end of the label. Now you can edit the

label.

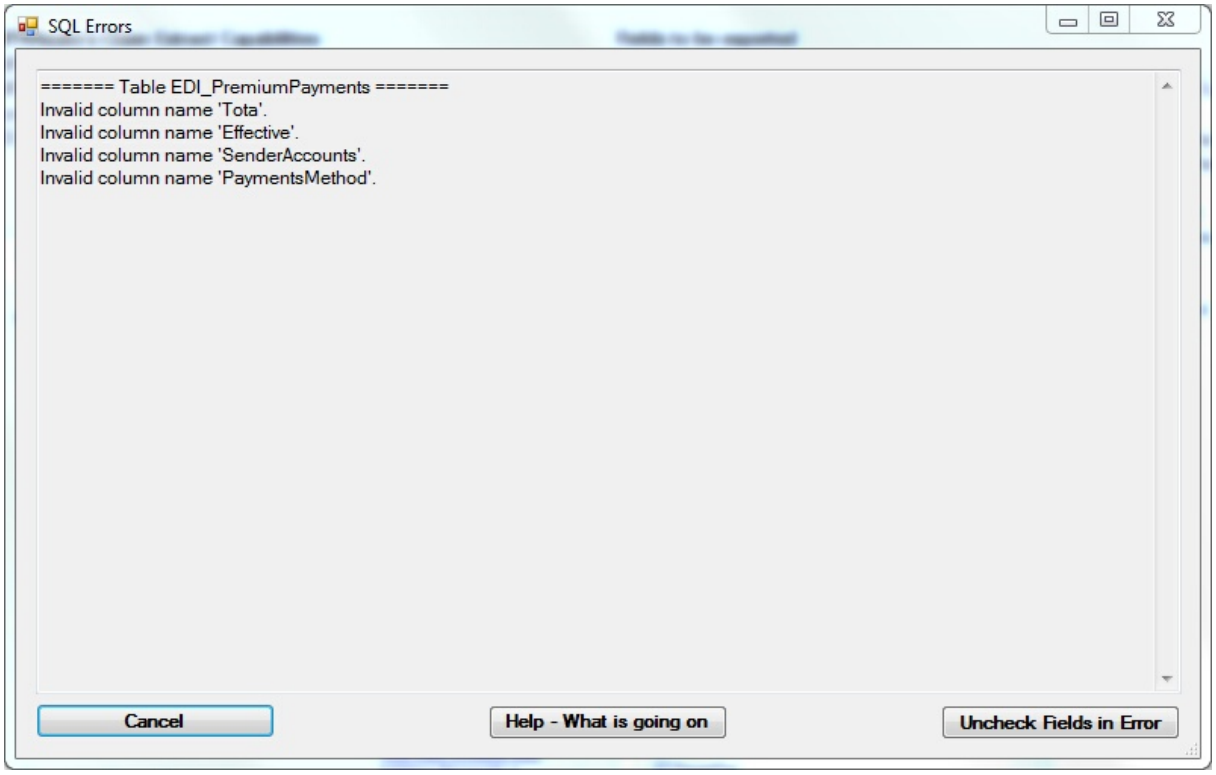


The field name in edit mode

The renamed field

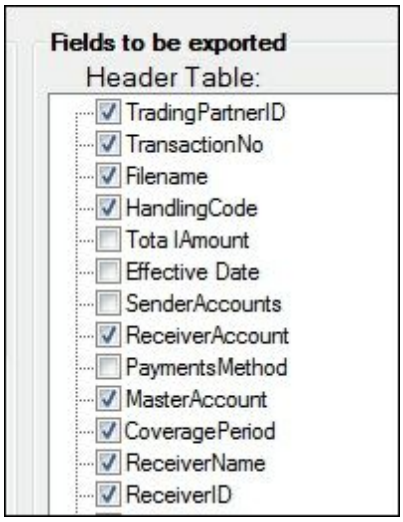
5.6 Field Errors

If fields don't exist in the database that you specified, you will see an error screen



The error screen you will see if the field selection contains non-existing fields.

Study the errors in detail and see what went wrong. In this case for demonstration purposes I changed a few names and of course that caused this error. My best option is to click the "Uncheck the Fields in Error" button and return to the field selection screen.



The fields in error are now unchecked.

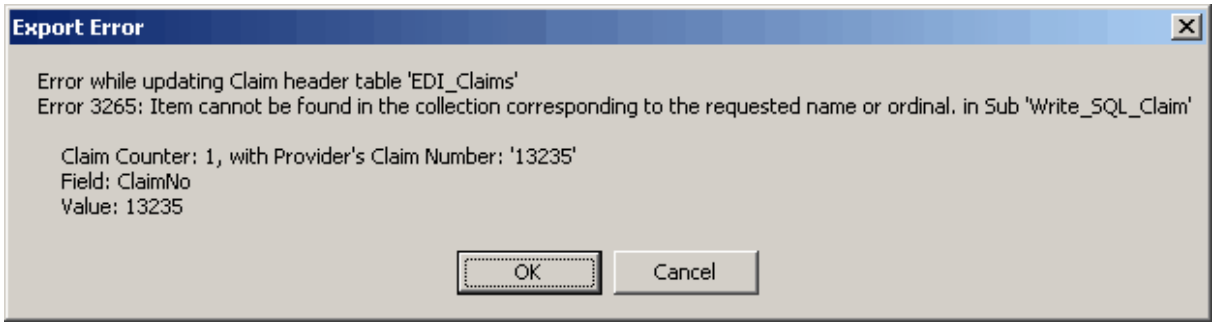
5.7 Database Errors

Enter topic text here.When you start exporting claims into the staging tables you might enconter errors at first. This usually results from table definition issues. The HIPAA Claim Status Responder displays a very detailed error message that tells you which claim failed, at what field and if applicable which line.

This information should help you to trouble shoot the problems. It sometimes takes serious detective work to find and correct errors.

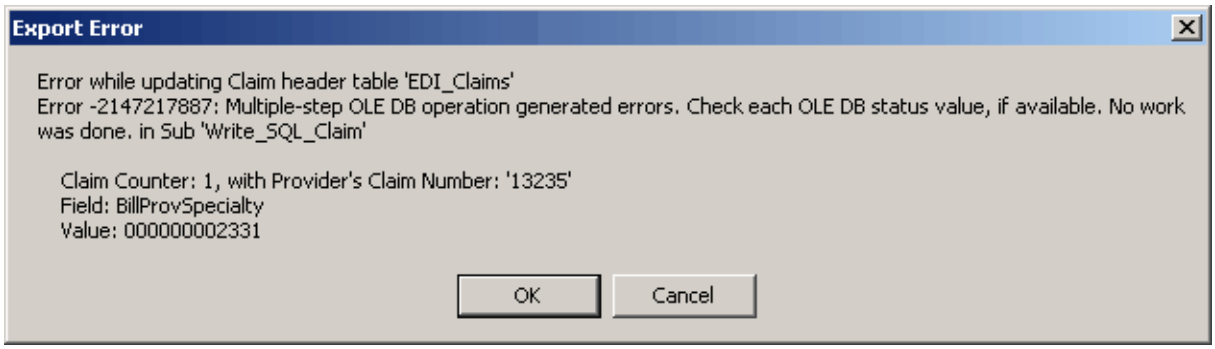
Below are some of the most common errors:

Item cannot be found:



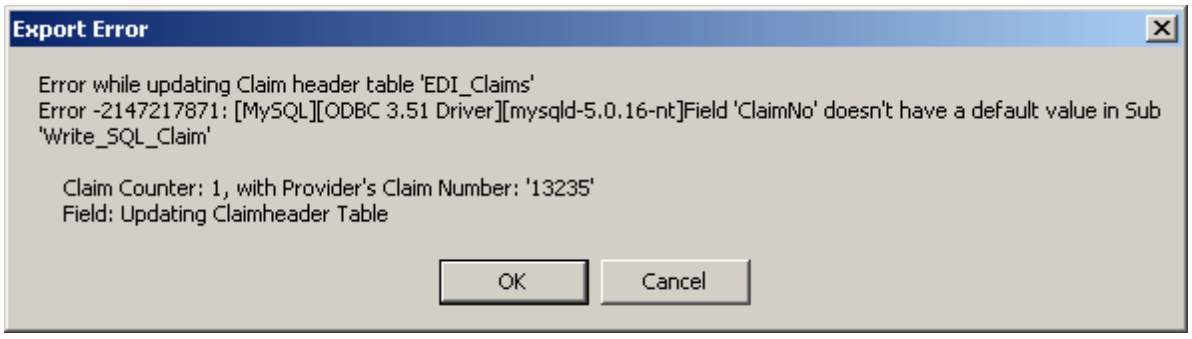
This error happens when a column that was selected for export does not exist in the Header table. In this particular case it is the field 'ClaimNo'. If you receive this error, go back to your table admin tool and check in the field 'ClaimNo'

Multi-step OleDB Operation generated errors



This is typically the message when the field definition in the database is different from the data. Here we see that the error occurred with the billing provider's specialty. The field definition in the table was set as varchar(10) and the value here:000000002331 has 12 digits, causing the error message.

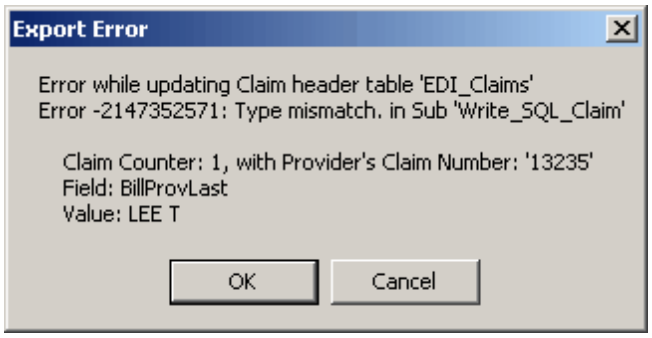
Field doesn't have a default value



The field 'ClaimNo' is defined as 'Not Null'. But somehow this data was not present and

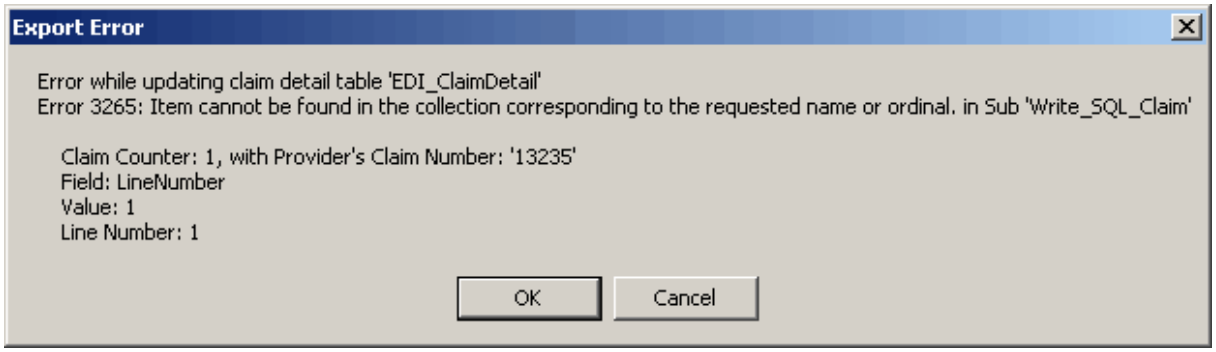
HIPAA Claim Master tried to update the table with a null ClaimNo.

Type mismatch:



This error occurrs when the HIPAA Claim Master tries to write a letter to a field that is defined as 'Integer,' for example. The data type of the column does not match the data type of the value.

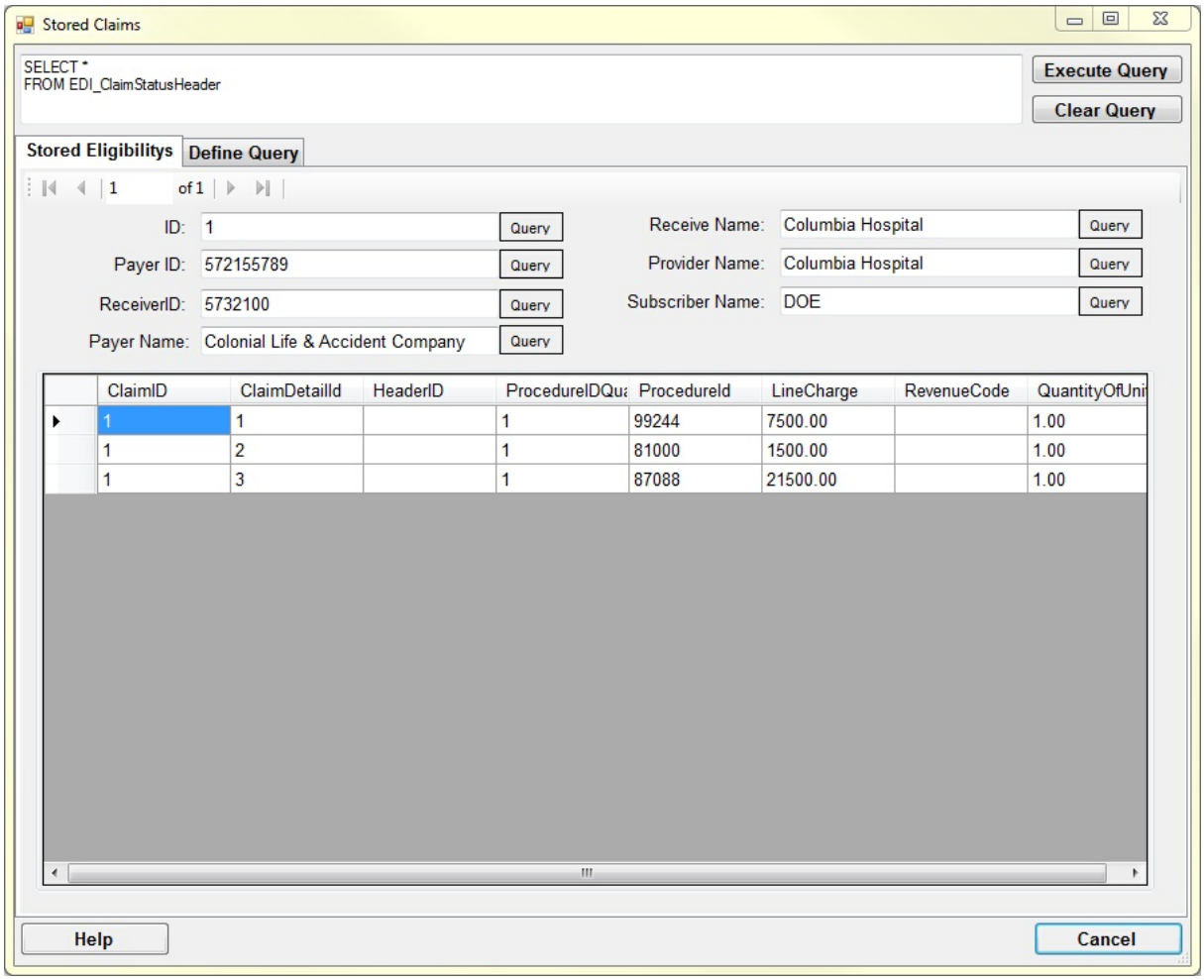
Claim Detail Errors



The errors with the claim detail table are similar, only that the error message indicates also at which line number it occurred.

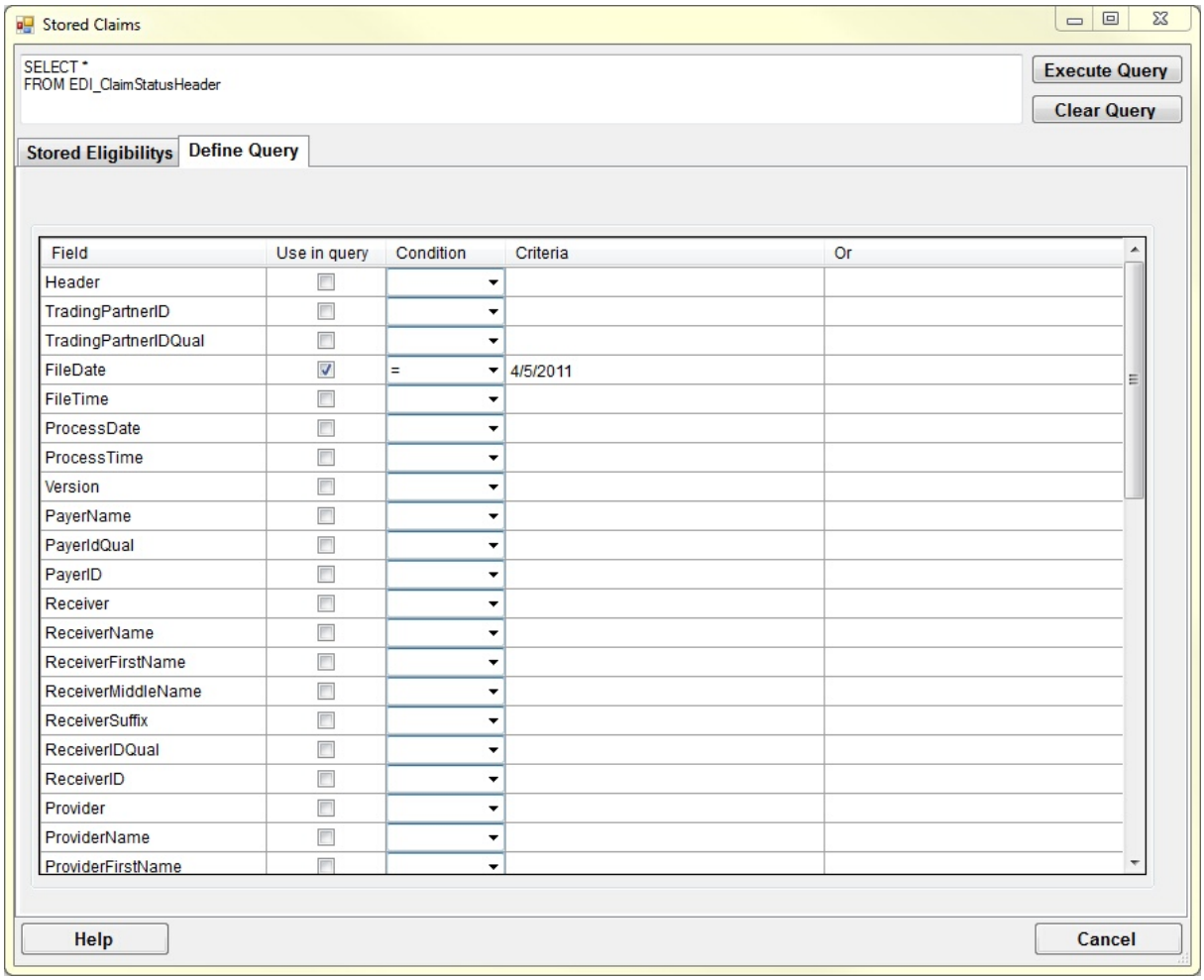
5.8 Exported Requests

You can work with the data in the Claim Status tables through the 'Stored Claim Status Requests" screen.



Stored Claim Status Request records

When you open the screen it shows you the first record in the database and the screen will let you scroll through all the records. You can also enter your own SQL query to select certain records only either as free form query if you are experienced in the database query language or through the 'Define Query' tab



Build your query

Here you can compose your query using the fields in the database and conditions that you select

6 Populating Claim Statuses

6.1 Concepts

The 277 Claim Status response is built from request/response data in the *EDI_ClaimStatusHeader* and *EDI_ClaimStatusDetail* tables and a pair of Source tables that can be filled from the HIPAA Claim Master or built from the HIPAA Claim Status Responder and filled externally.

Claim Master as Source

Every row in *EDI_Claims* represents a single claim and every row in *EDI_ClaimDetail* represents a billable event or instance. The Claim Master stores all data pertaining to a claim. The Claim Master can also store Claim Status information under the fields labeled as "*Claim Feedback*" in the HIPAA Claim Master Database Connection Fields nodes and Claims and ClaimDetail table creation scripts. Since the HIPAA Claim Master already fills in all of the Claim information, the "*Claim Feedback*" fields are all that is necessary to provide a Claim Status on a claim. These fields are:

Claim Status Source Tables

If the HIPAA Claim Master tables cannot be used, the HIPAA Claim Status Responder provides scripts for an independent set of information source tables which contain all fields necessary to provide Claim Status information. The *EDI_ClaimStatusSourceHeader* is to be used to store information about a specific claim; a claim's line items are stored in *EDI_ClaimStatusSourceDetail*.

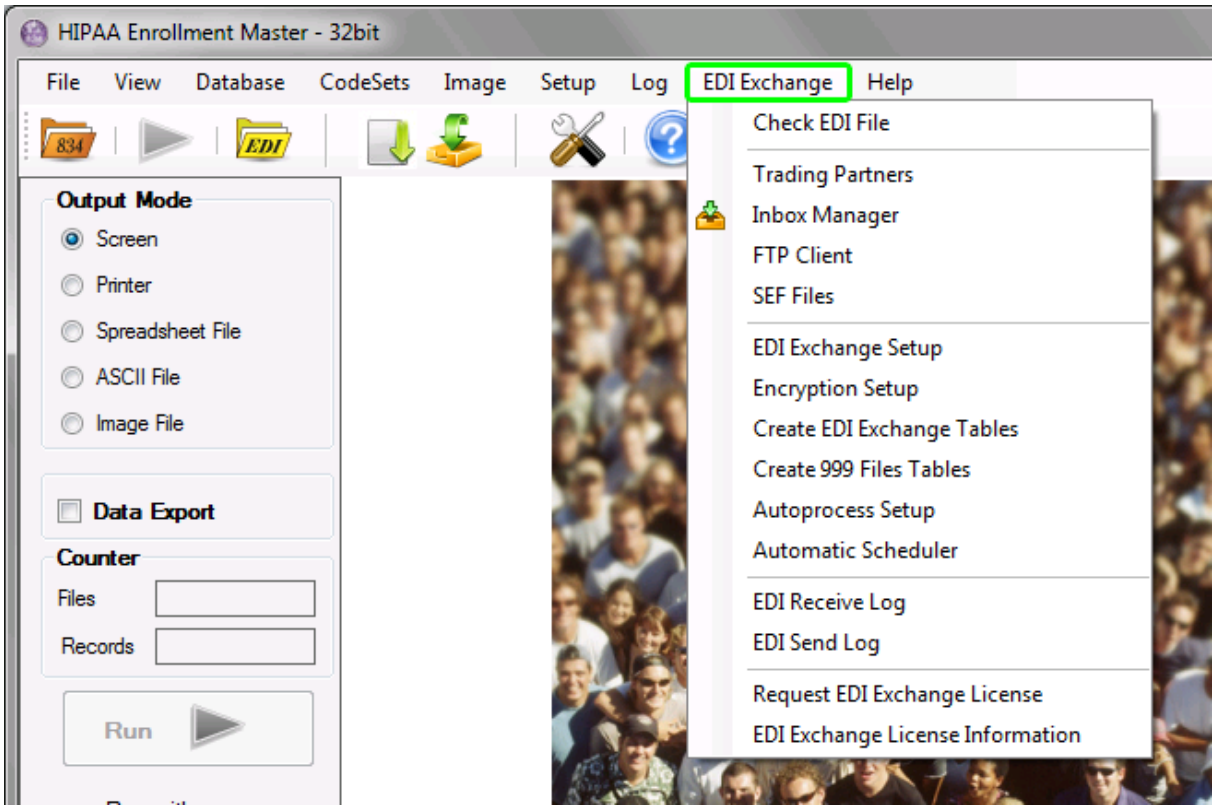
7 EDI Exchange

7.1 Getting Started

7.1.1 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. Some of our products, such as HIPAA Claim Master, process EDI files but do not receive 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 the 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, CORE-Compliant server addresses and credentials, 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**

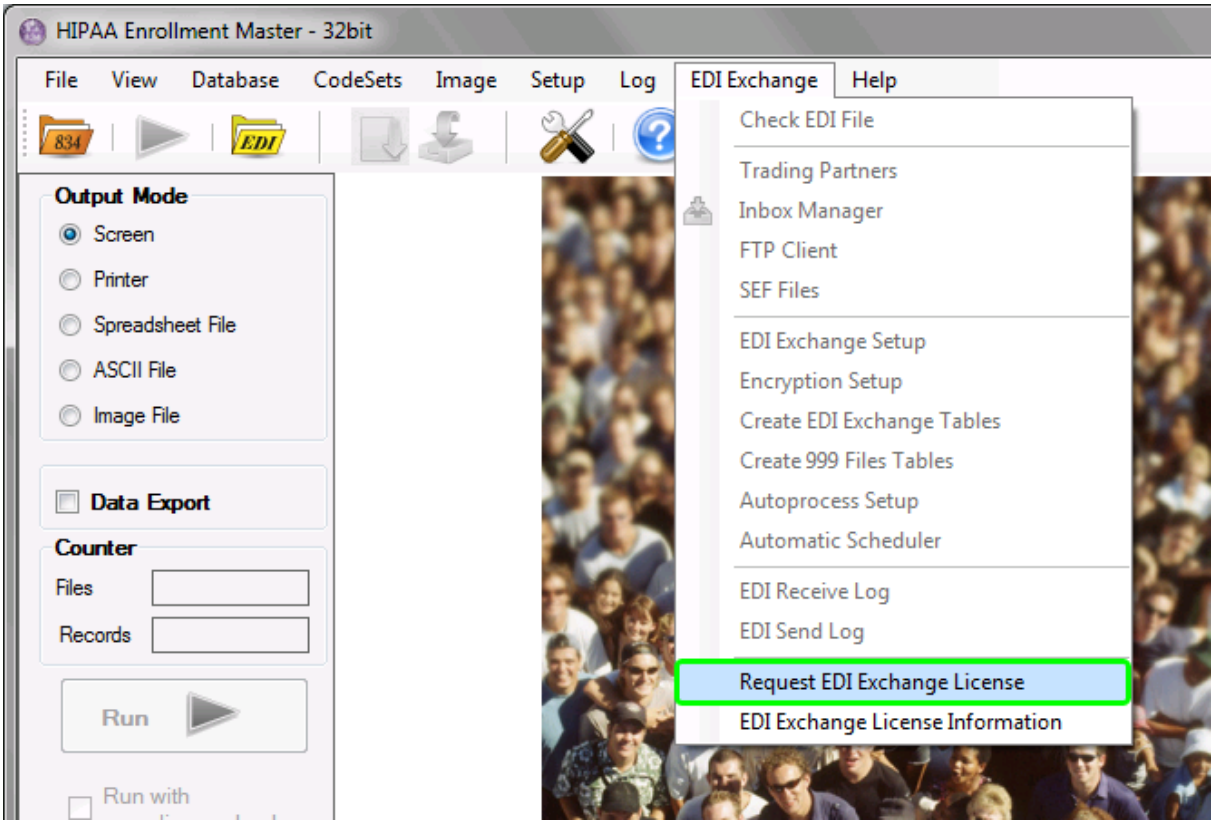
7.1.2 Requesting EDI Exchange License

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.

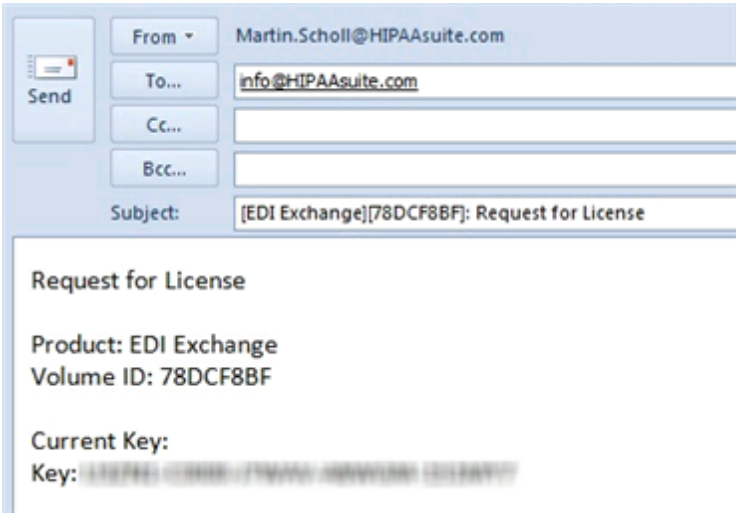
Follow the instructions below to request a trial or final license key.

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



A menu item to request a license key

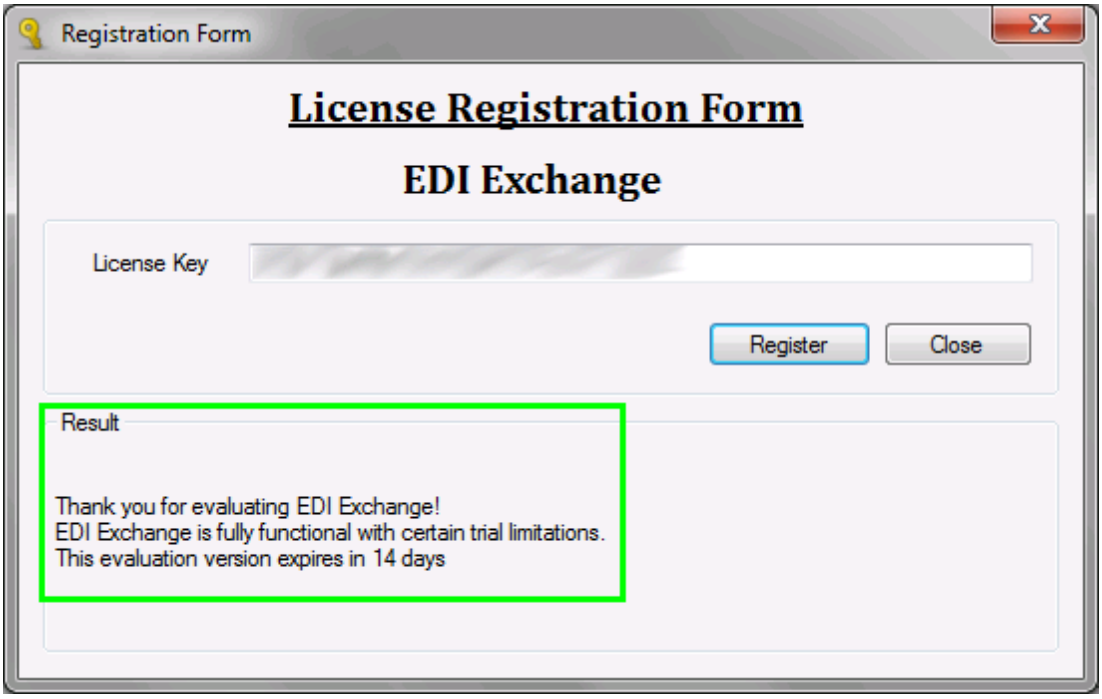
2. Once you have clicked this menu item, your default email application appears. In our case, it is Microsoft Outlook. All information necessary to produce the key is automatically filled out.



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.

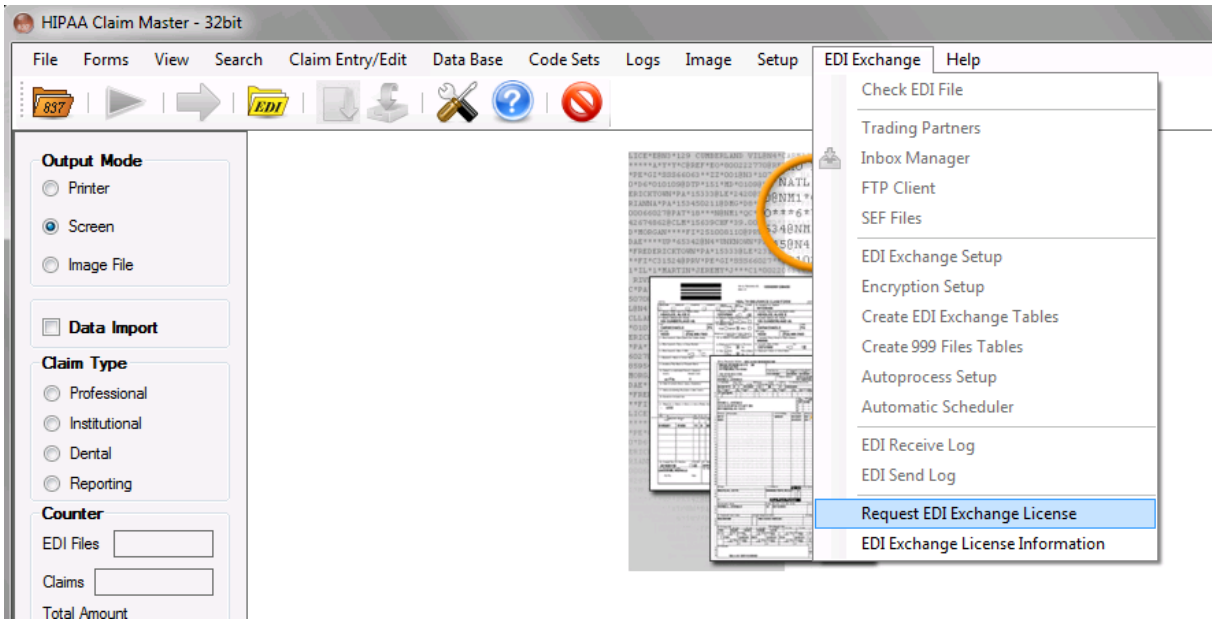


Entering the license key

7.1.3 Registering EDI Exchange

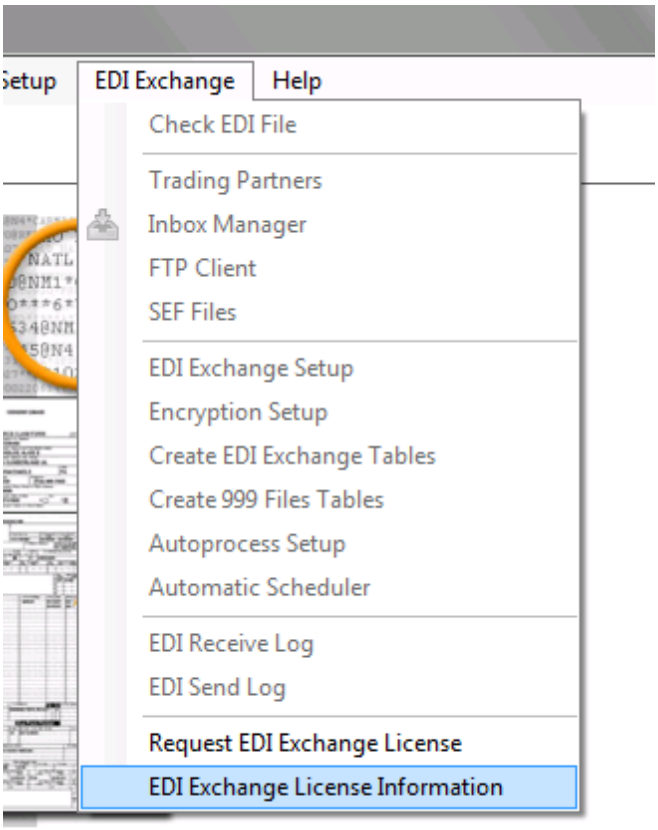
EDI Exchange is licensed separately from the host application, HIPAA Claim Master, for example. The reason is that EDI Exchange will work on all HIPAAsuite Products that are installed on your particular computer. For example, if you have HIPAA Claim Master and HIPAA Enrollment Master licensed, only one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

When you first install a HIPAAsuite product of your choice, a 15-day EDI Exchange trial is included. 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.



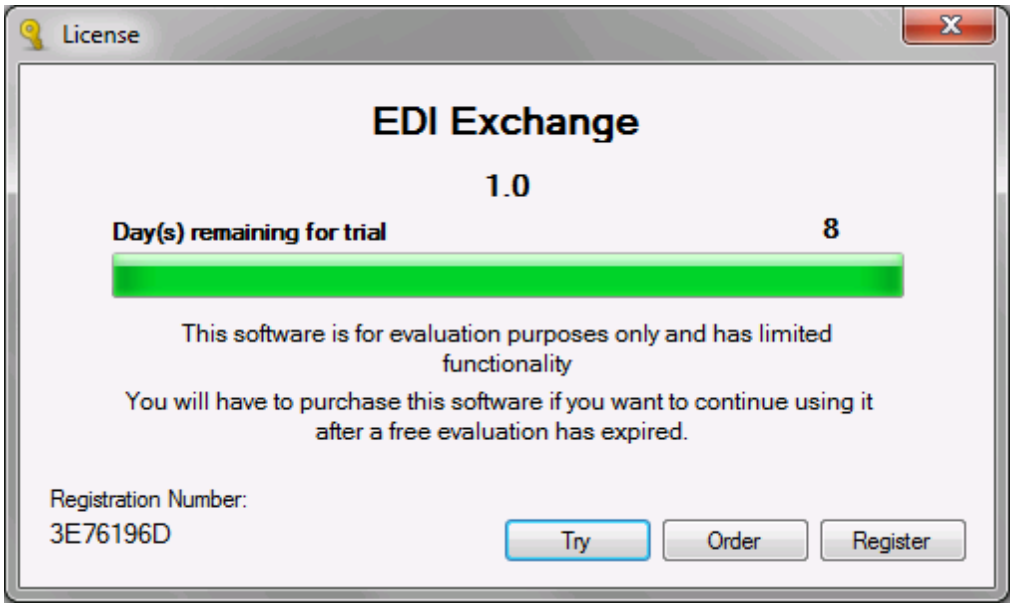
The "EDI Exchange" menu with menu items disabled

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



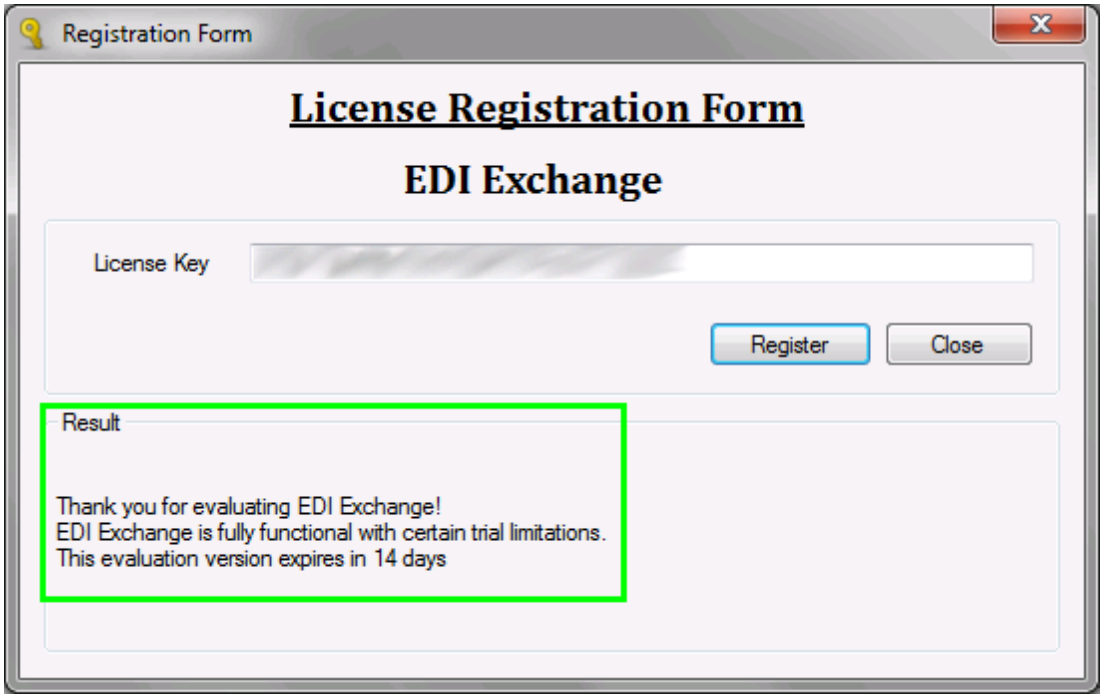
"EDI Exchange License Information" option under the "EDI Exchange"

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.

7.2 Configuring EDI Exchange (Obligatory Settings)

7.2.1 1 Setting up Database Connection

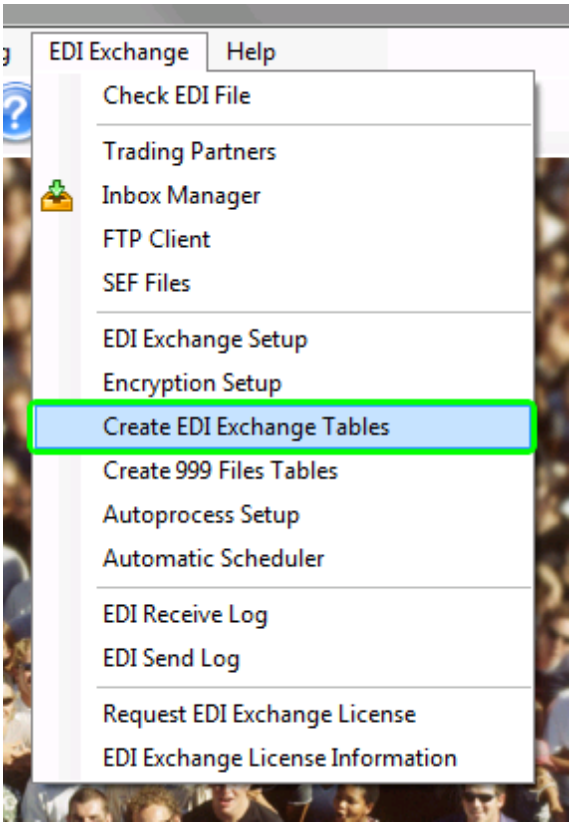
EDI Exchange work is based on the database connection that you define under *Database ▸ Connection and Data Fields* in the main menu of the HIPAA host application. Make sure the connection has already been set up and tested before proceeding with EDI Exchange.

Then proceed to the next step: Creating Database Tables.

7.2.2 2 Creating Database Tables

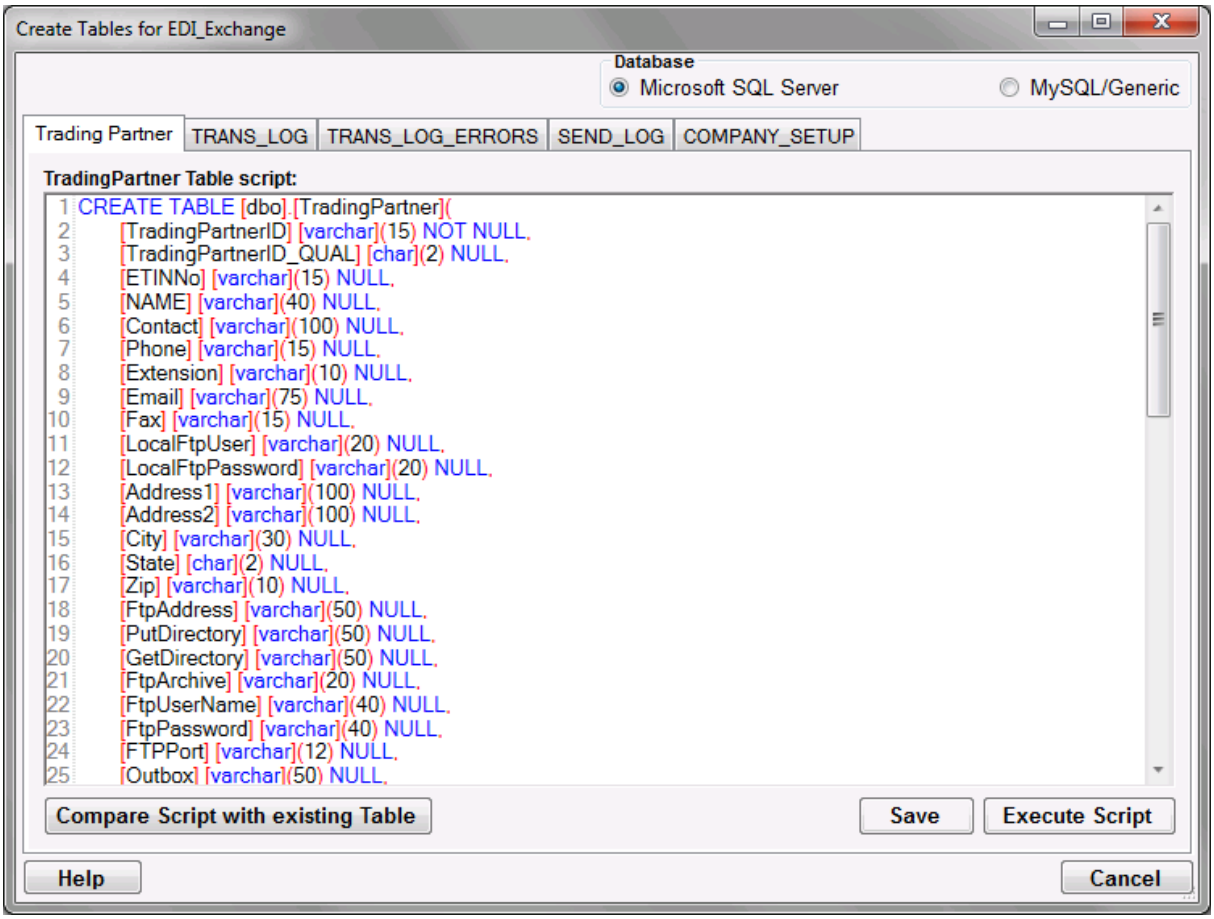
Once you have configured the database connection (Setting up Database Connection), follow the instructions below.

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



The menu item to create the necessary tables.

2. The "Create Tables for EDI_Exchange" screen will appear. Table creation and/or modification for your database is handled here.



The screen to create the tables

3. Select the database type you use for your host HIPAA application.
   - **Database**
     - **Microsoft SQL Server** (SQL Server 2008 and above)
     - **MySQL**

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

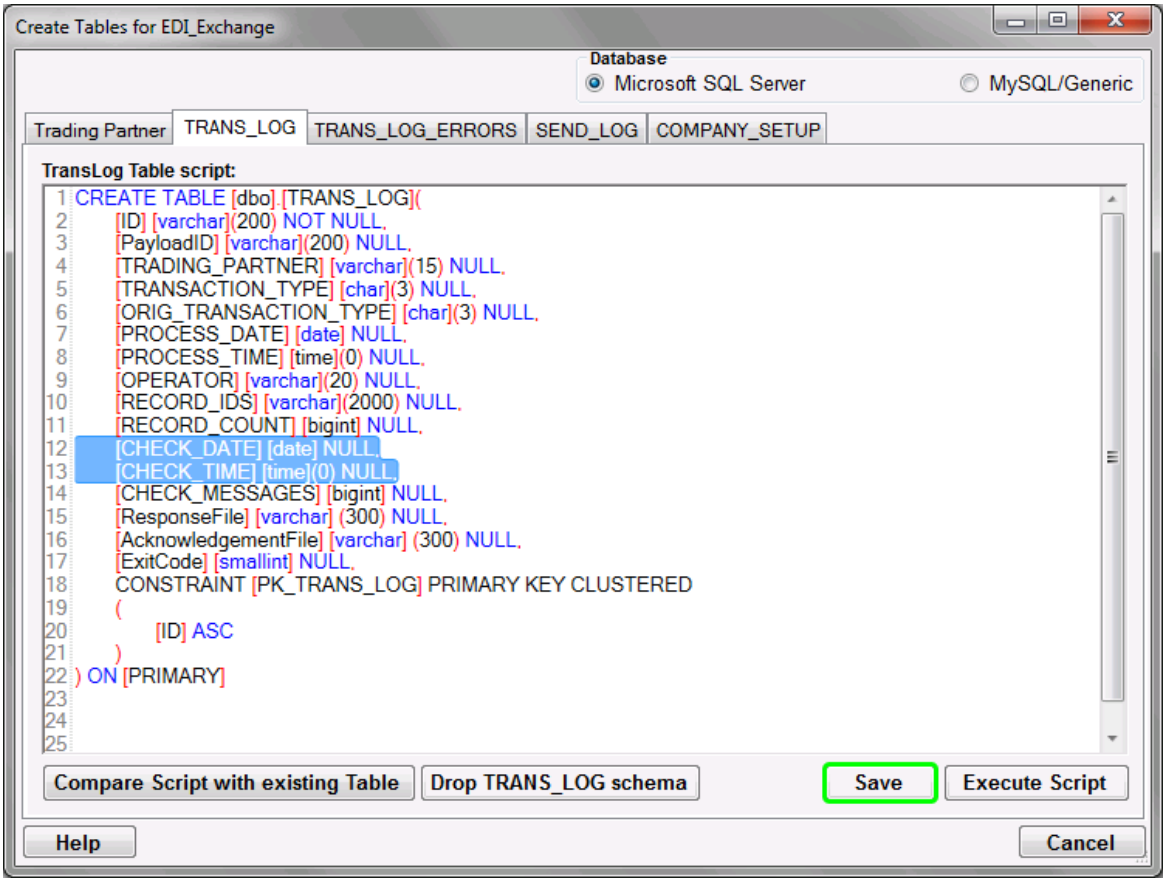
4. The following tables are part of EDI Exchange:
   - **TradingPartner** — SQL statements to create the "TradingPartner" table in your database. This table contains information about trading partners.
   - **Trans_Log** — SQL statements to create the "TRANS_LOG" table in your database. This table contains 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.

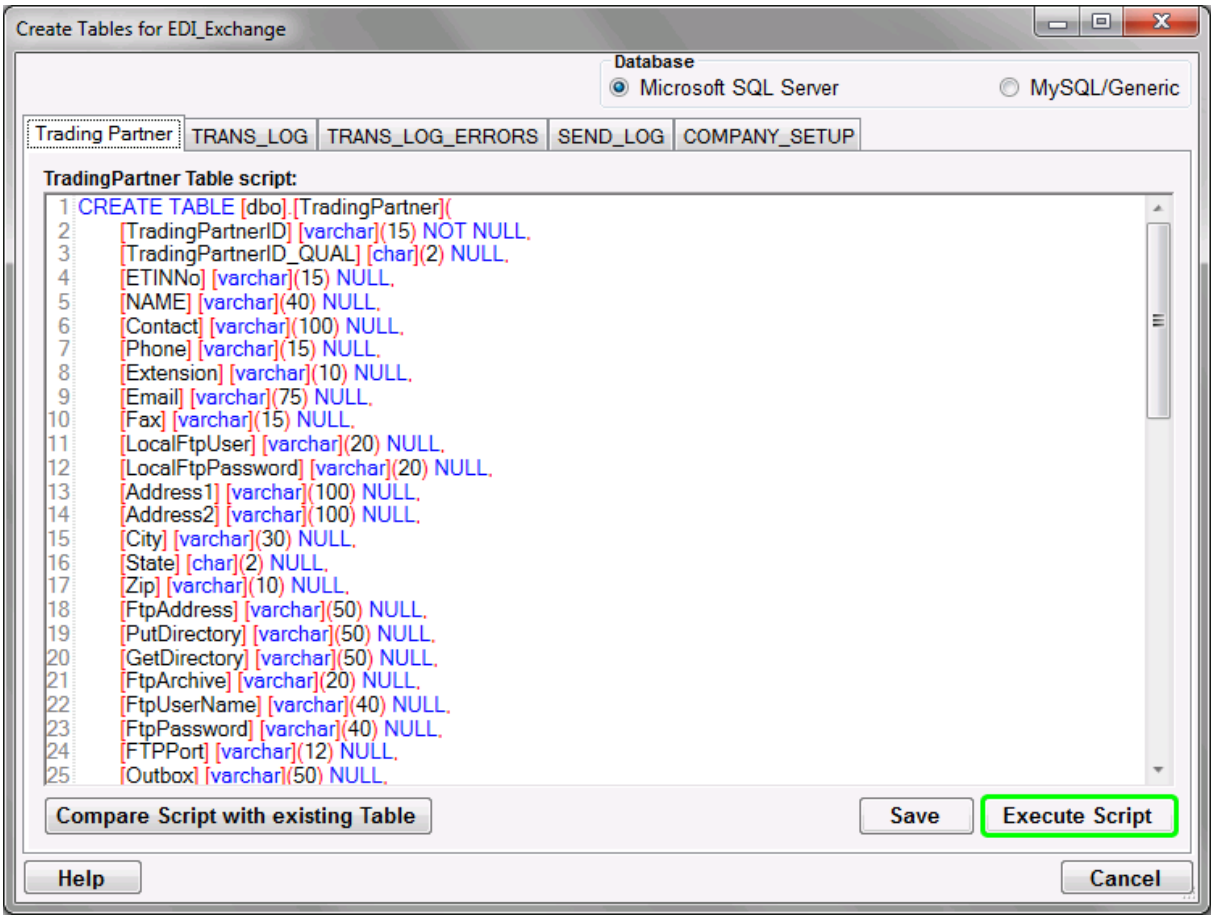
5. You can modify the scripts so that they run on your specific database. Once you have you modified the script, click "Save."

> 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. One example are 'date' and 'time' or 'money' data types that do not exist in SQL Server 2005. You can just rename those types to 'datetime' and save you script and it will run fine.



The "Save" button

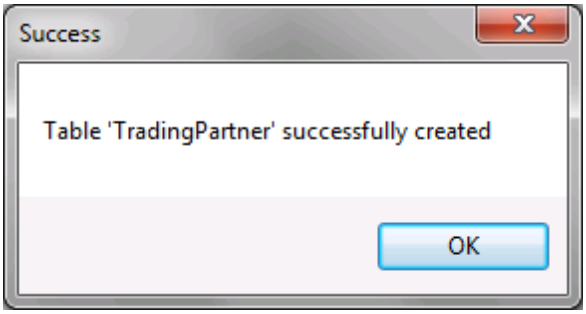
6. For **each** script on every tab, click "Execute Script" to create the corresponding table in the database.



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.

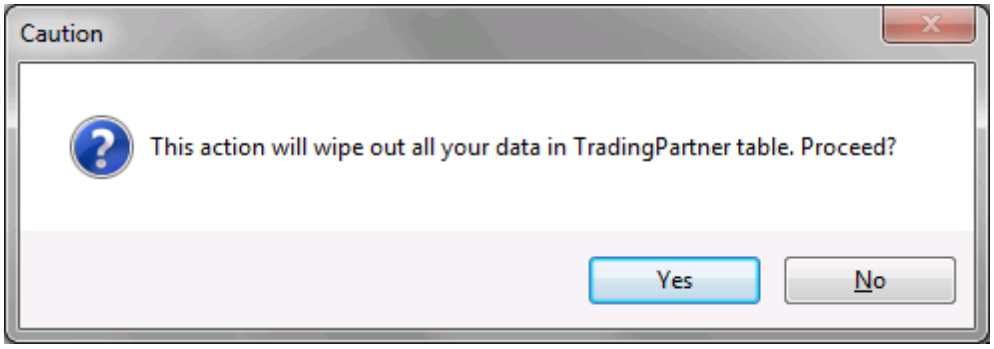
7. Once the table has been created successfully, you will see the following notification:



The Create Table script success message

> **Warning: Double-execution of a script wipes out the previous table you have created. A prompt will warn you before deleting an existing table. To Add/Remove fields use the "Compare Script..." button. Remove the script files once you have created the tables so nobody can destroy the tables**

by accident.



The double-execution warning message.

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

Compare Script with existing Table

HIPAAsuite products go through continual development and improvements. Often these changes lead to new fields in the database. While it is easy to drop a table and regenerate it with the new fields, you will loose all the data in the table. To avoid this trouble there is the button "Compare Script with existing Table". I you click this, the table structure in your database will be compared with the script. There are two possible outcomes. Your table is up to date

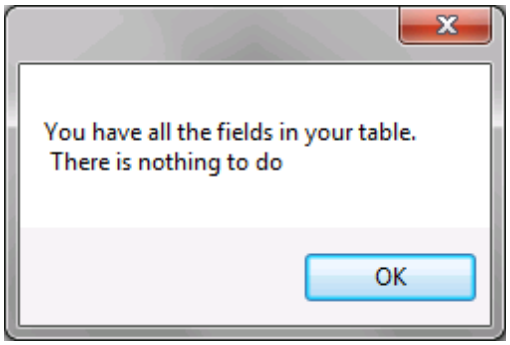
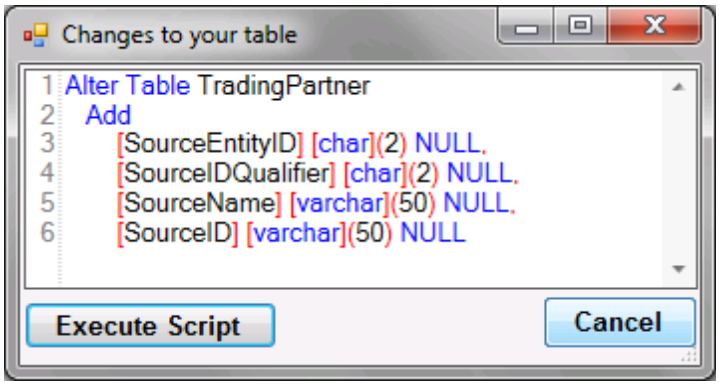


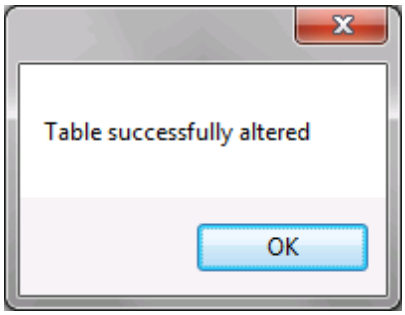
Table is up to date

or if your table is missing recently added fields, you will see a window pop up that shows an 'Alter Table' script with which you can add those fields to the table without interfering with existing data.



The 'Alter Table' script that shows as a result of missing fields

You can now click the "Execute Script" button and the field will be added and a message will confirm your changes



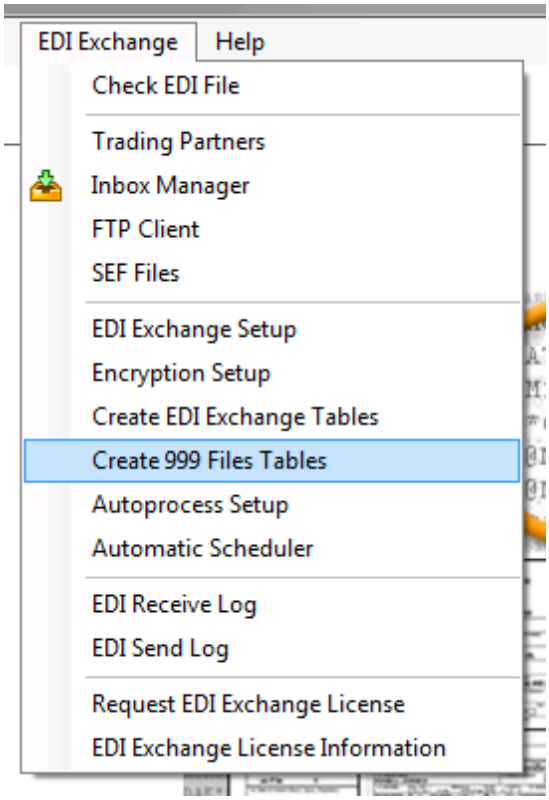
Alter Table statement successfully executed.

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

7.2.3 2b Creating 999 File Tables

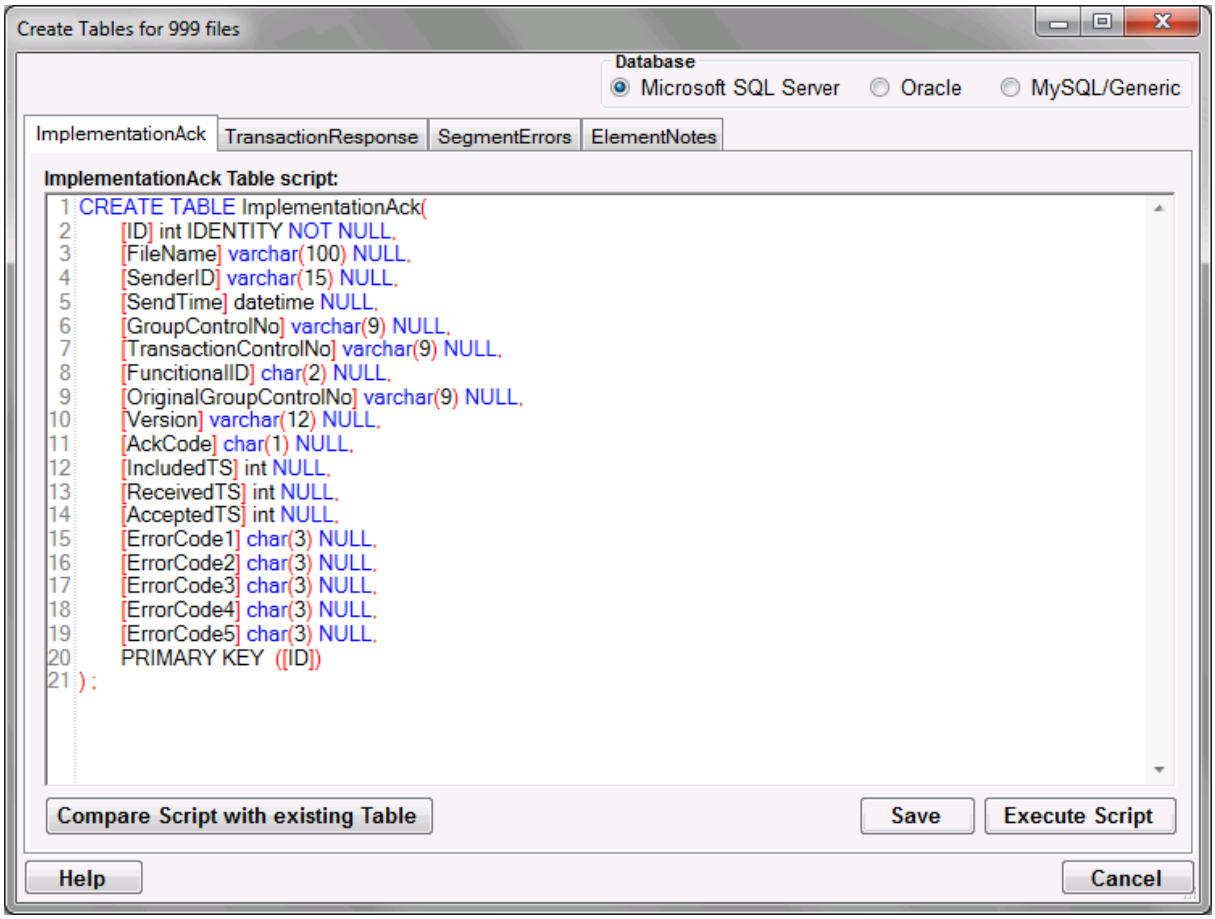
Once you have configured the database connection (Setting up Database Connection), follow the instructions below.

1. Select *EDI Exchange* ▸ *Create 999 Files Tables* in the main menu.



The menu item to create the necessary tables

2. The "Create Tables for 999 Files" screen will appear. Table creation and/or modification for your database is handled here.



The screen to create the tables

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

- **Database**
  - **Microsoft SQL Server** (SQL Server 2008 and above)
  - **Oracle**
  - **MySQL**

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

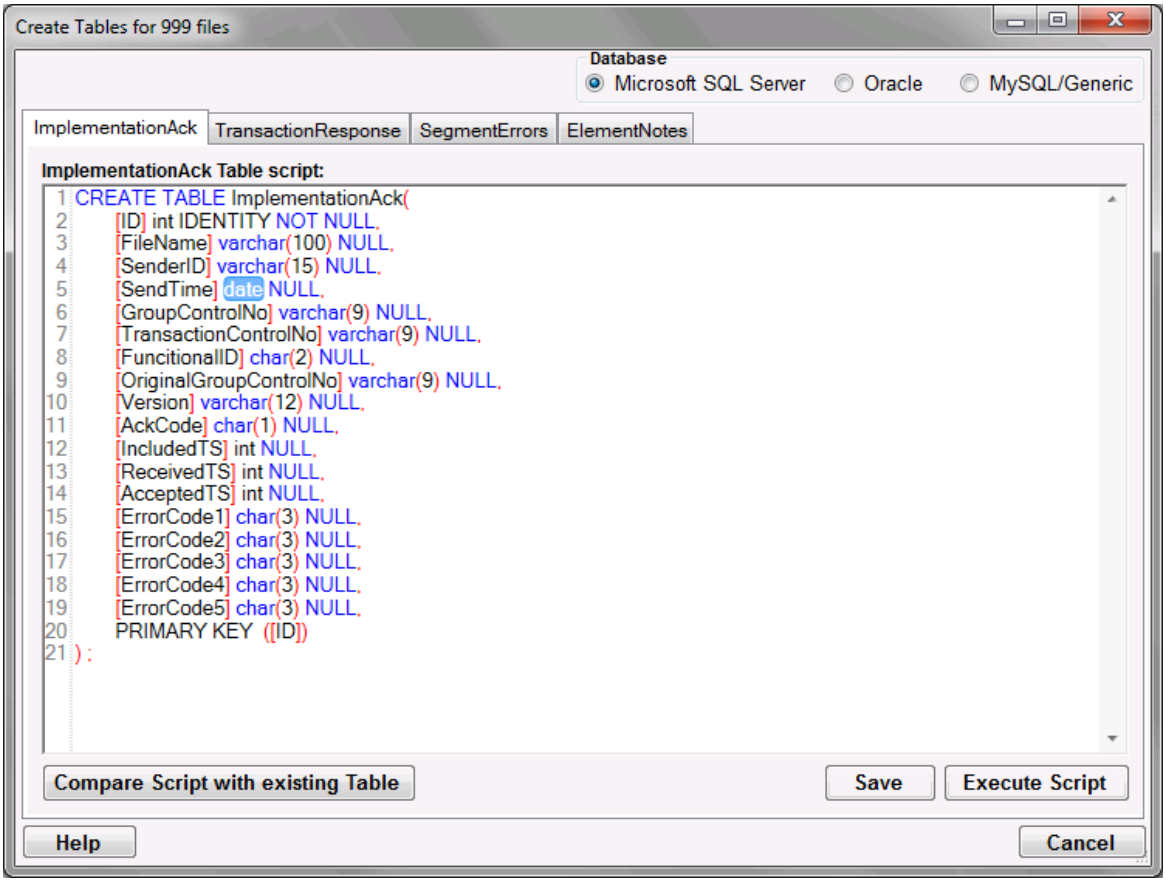
1. The following tables are part of EDI Exchange:

- **ImplementationAck** — SQL statements to create the "ImplementationAck" table in your database. This table contains information about Acknowledgments.
- **TransactionResponse** — SQL statements to create the "TransactionResponse" table in your database. This table contains individual transactions contained in 999 files.

- **SegmentErrors** — SQL statements to create the "SegmentErrors" table in your database. This table contains individual segments in error contained in 999 transactions.
- **ElementNotes** — SQL statements to create the "ElementNotes" table in your database. The table contains the elements in error in a specific segment.

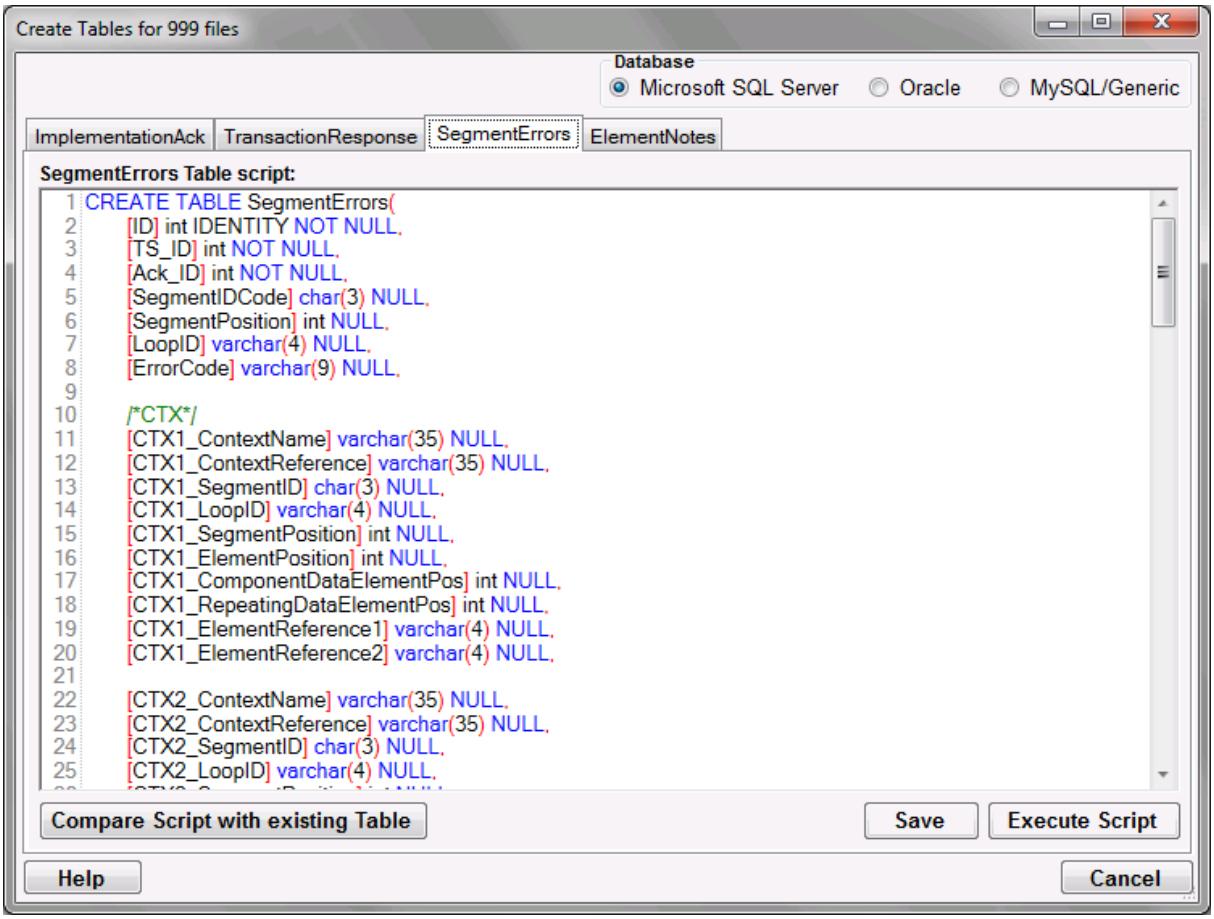
5. You can modify the scripts so that they run on your specific database. Once you have you modified the script, click "Save."

> 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. One example are 'date' and 'time' or 'money' data types that do not exist in SQL Server 2005. You can just rename those types to 'datetime' and save you script and it will run fine.



The "Save" button

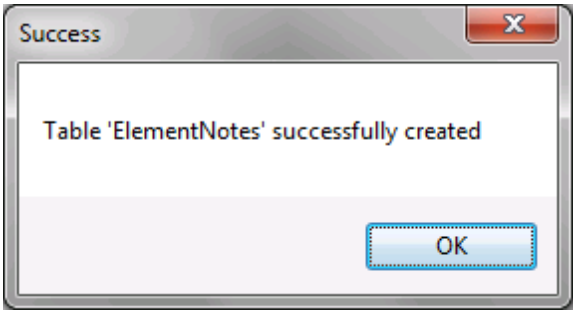
6. For **each** script on every tab, click "Execute Script" to create the corresponding table in the database.



The "Execute Script" button

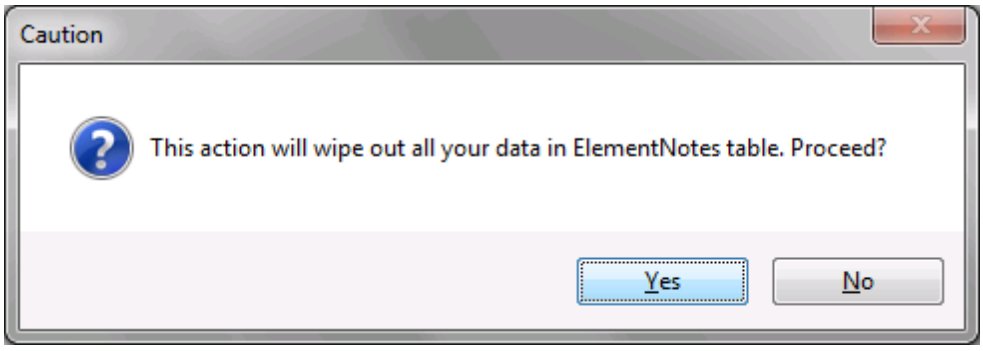
> Notice: Creating tables means clicking the "Execute Script" button in all four tabs of the "Create Tables for 999 Files" window. Then close this window.

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



The Create Table script success message

> **Warning: Double-execution of a script wipes out the previous table you have created. A prompt will warn you before deleting an existing table. To Add/Remove fields use the "Compare Script..." button. Remove the script files once you have created the tables so nobody can destroy the tables by accident.**



The double-execution warning message.

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

Compare Script with existing Table

HIPAAsuite products go through continual development and improvements. Often these changes lead to new fields in the database. While it is easy to drop a table and regenerate it with the new fields, you will loose all the data in the table. To avoid this trouble there is the button "Compare Script with existing Table". I you click this, the table structure in your database will be compared with the script. There are two possible outcomes. Your table is up to date

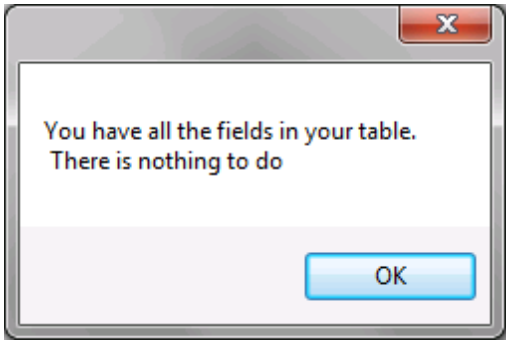
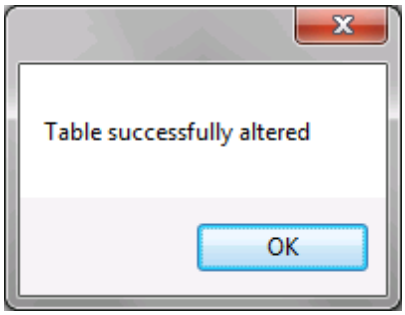


Table is up to date

or if your table is missing recently added fields, you will see a window pop up that shows an 'Alter Table' script with which you can add those fields to the table without interfering with existing data. In the latter case, you can click the "Execute Script" button and the field will be added and a message will confirm your changes

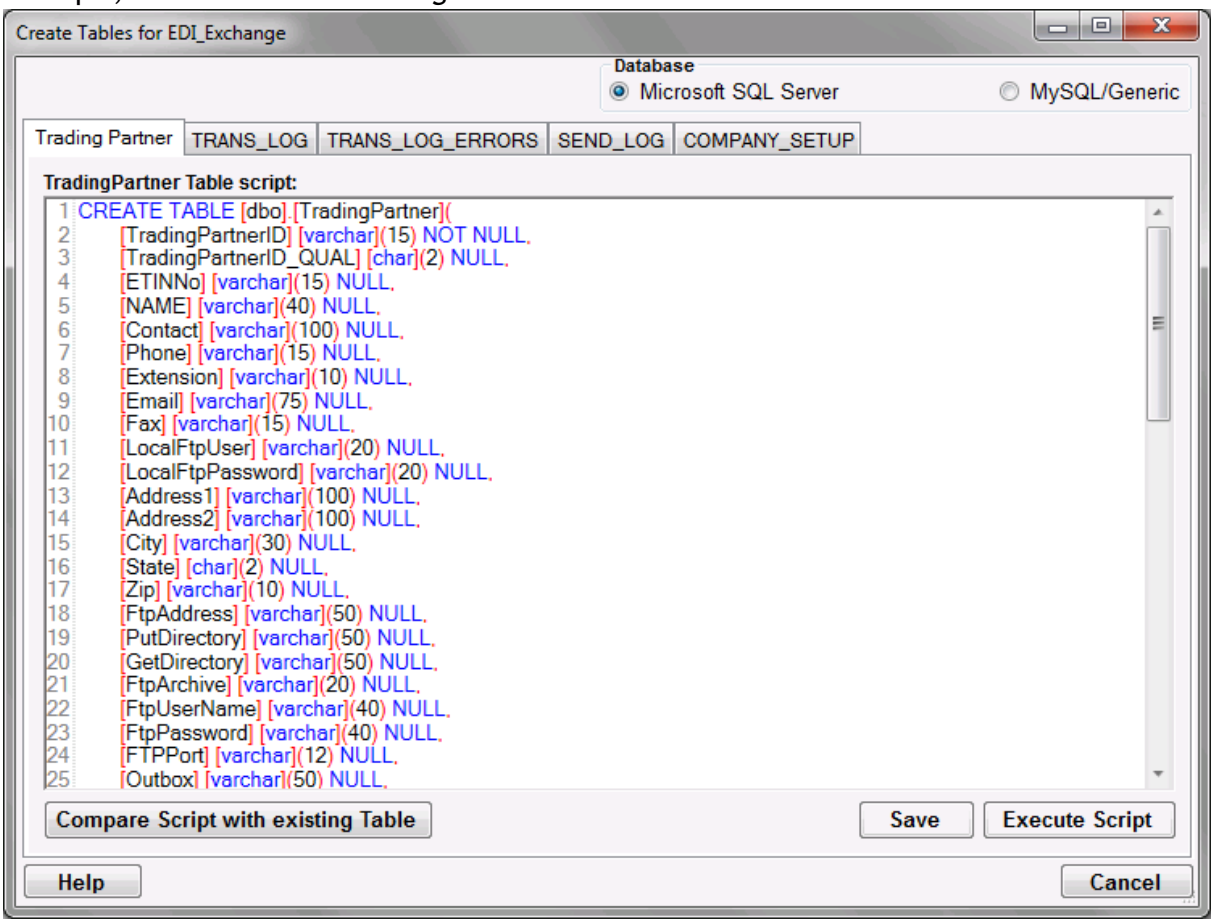


Alter Table statement successfully executed.

7.2.4 2c Updating Database Tables

To update an existing table (in the event of an update, for example), follow the instructions below.

1. Start with the table creation script window of the table you want to update. In this example, we will use the *Trading Partner* table.



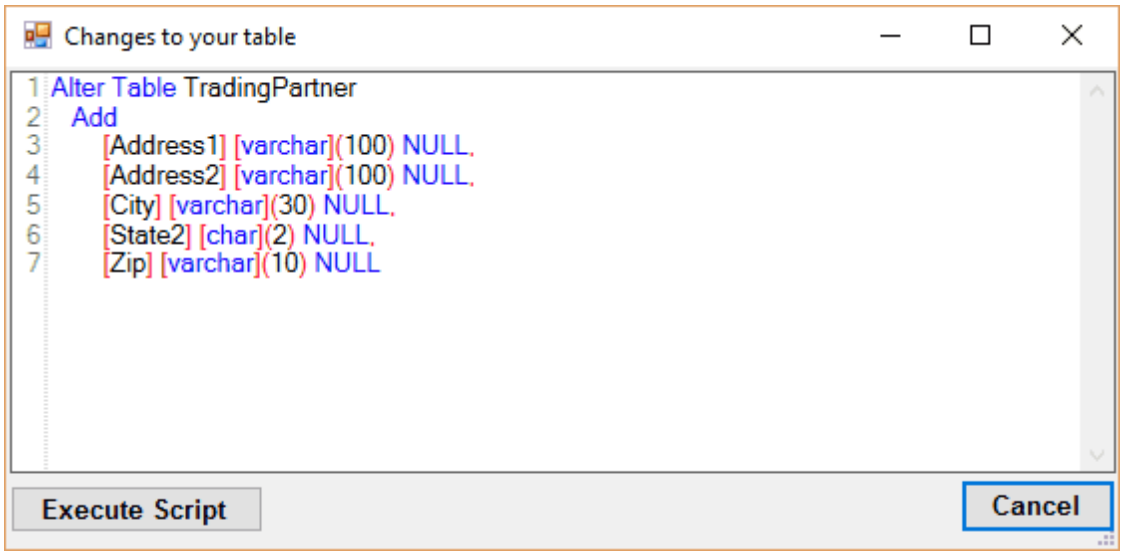
The table creation script for the Trading Partner table.

2. In the case of modifying a table to include/exclude/change a field or fields required by

a program update, the script will have been updated for you and clicking the *Compare Script with existing Table* button will bring you to the next step. To modify the table yourself in order to conform to your particular database, first edit the script text to suit your database system, click the *Save* button, then the *Compare Script with existing Table* button, and proceed to the next step.

> 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. One example are 'date' and 'time' or 'money' data types that do not exist in SQL Server 2005. You can just rename those types to 'datetime' and save you script and it will run fine.

3. Having clicked *Compare Script with existing Table*, the script will be compared to the existing table and any additional fields will be presented. In this example, the Trading Partner table's Address fields will be added.



Changes to be made to Trading Partner table.

4. Click *Execute Scipt*. This will perform the additions/changes stated in the alter table script and a prompt will appear informing you of the change. The table has now been modified.

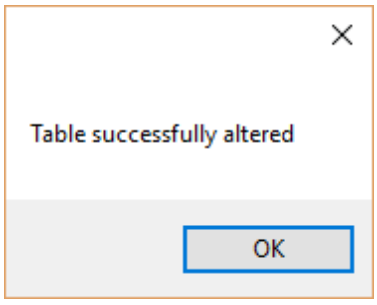


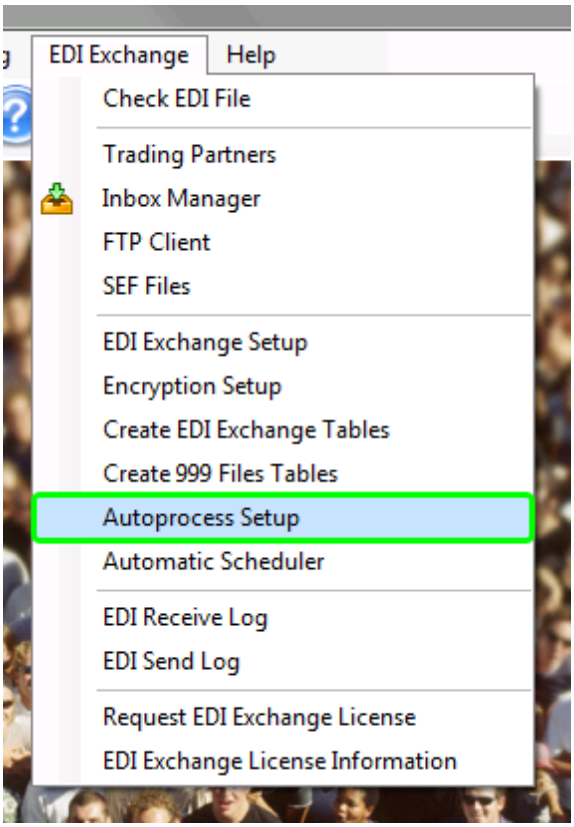
Table has been altered.

7.2.5 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.

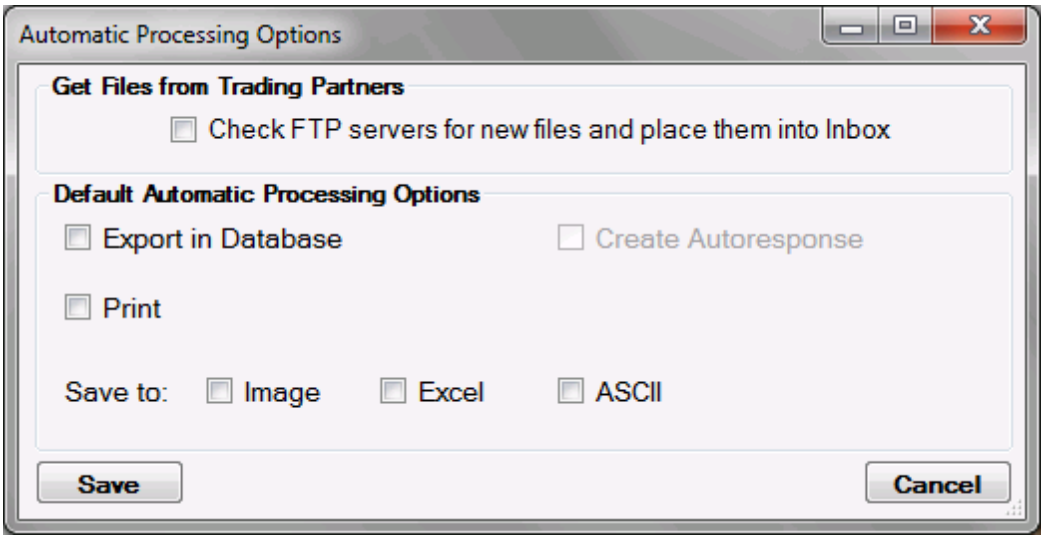
Follow the instructions below to specify the Auto Process Options.

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:

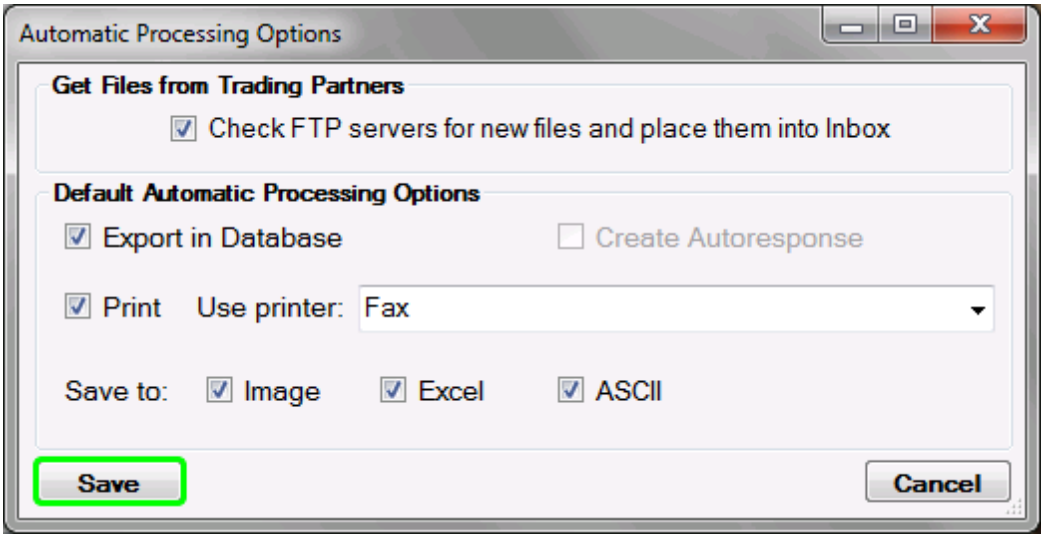
Check Path Options

- **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.

7.2.6 4 Defining Communications Directory

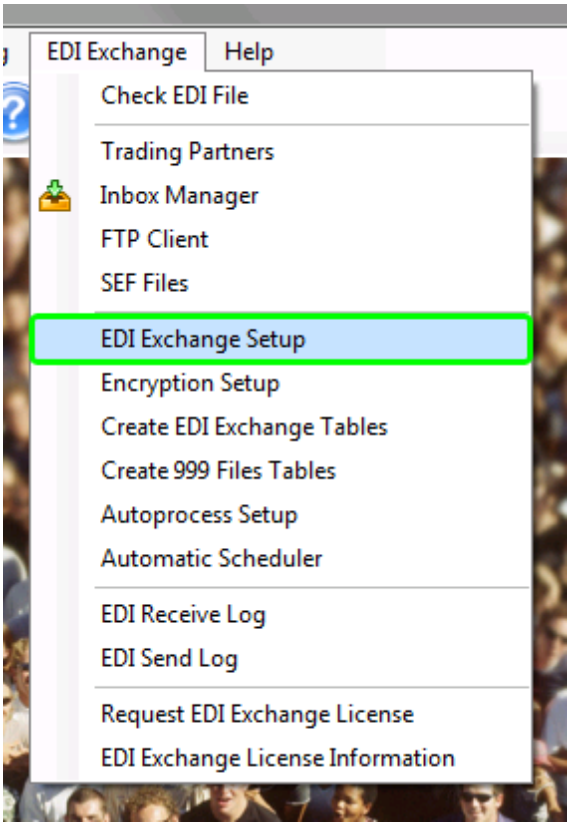
EDI file directory is an obligatory setting you need to set up before starting using the EDI Exchange. In order to keep track of the thousands of EDI files that accumulate over time, EDI Exchange uses a folder structure which we call the "HIPAAsuite Communications Directory" or "HIPAAsuiteCommDir" in 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 transaction. The location and names of the sub-folders are handled in the "Trading Partner Setup." See Setting up Trading Partners.

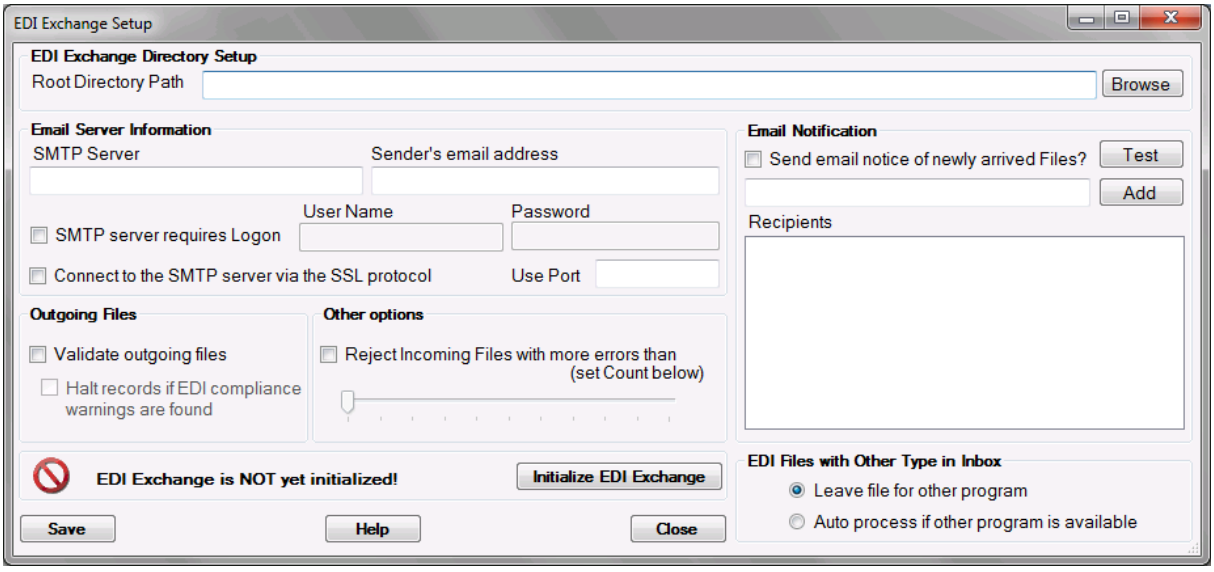
Follow the instructions below to specify EDI communications root directory.

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



The "EDI Exchange Setup" menu item

2. The following window will appear.

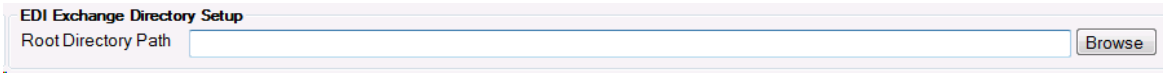


The "EDI Exchange Setup" window

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

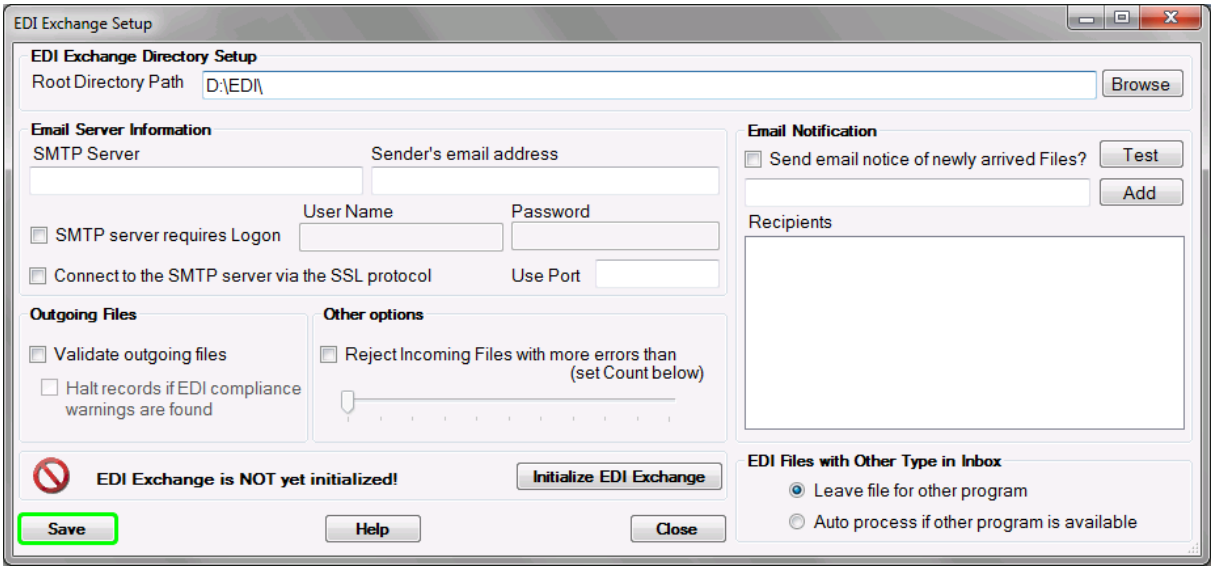
3. Under "EDI Exchange Directory Setup" specify the following setting:

- **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."



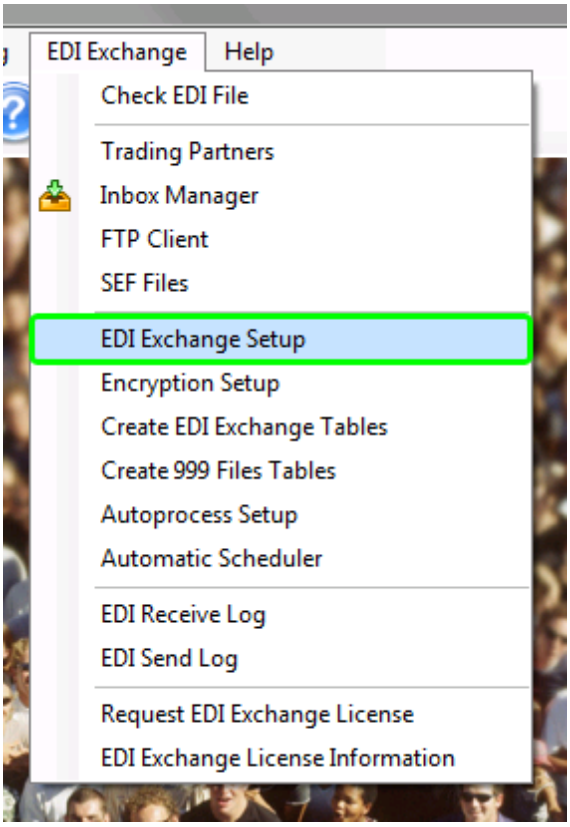
The "Save" button

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

7.2.7 5 Initializing EDI Exchange

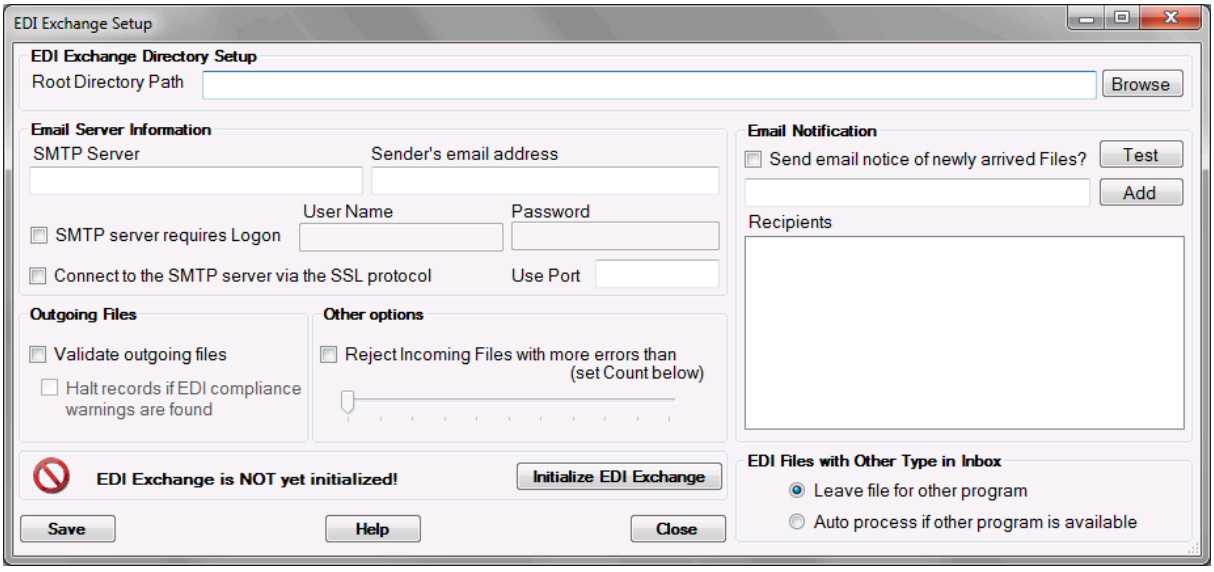
Before you can use EDI Exchange, and after you have configured the obligatory settings, you have to perform the initialization. Follow the instructions below.

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



The "EDI Exchange Setup" menu item

2. The following window will appear.

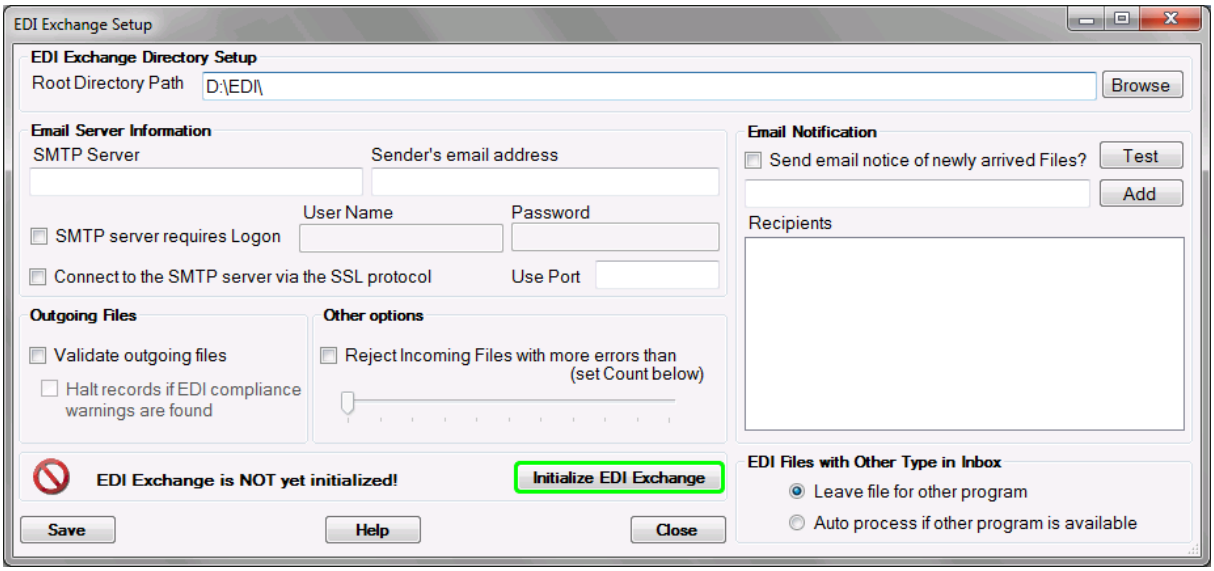


The "EDI Exchange Setup" window

> 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

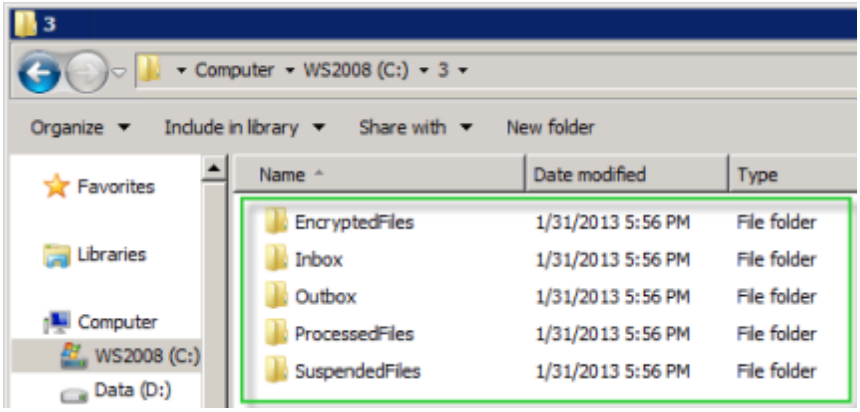
Read more in Setting up Database Connection.

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:

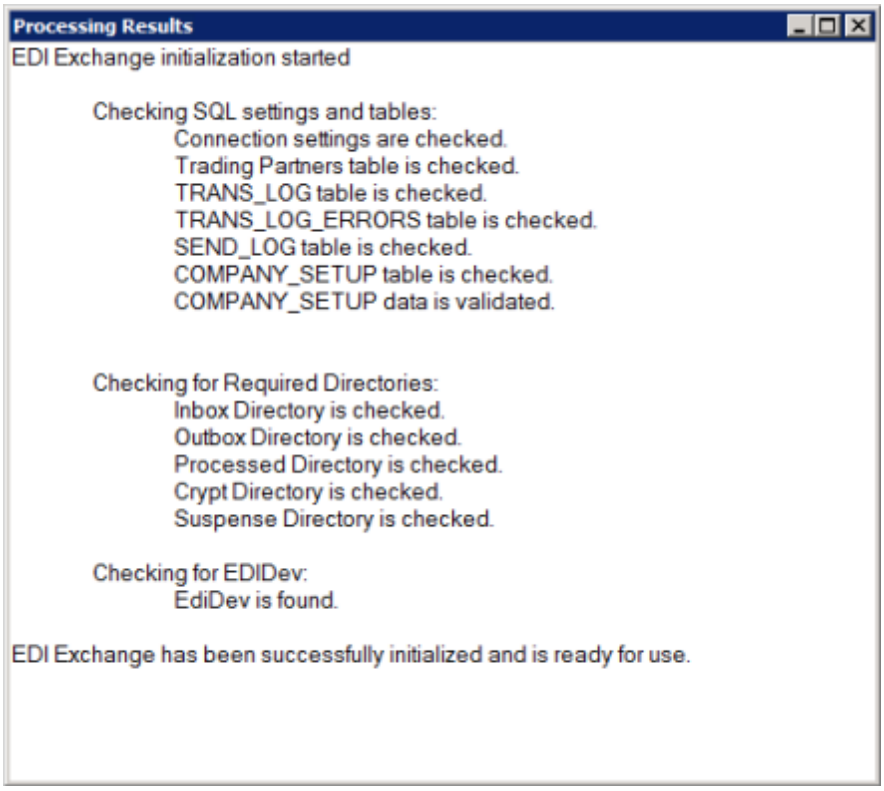


The directory structure of EDI Exchange

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

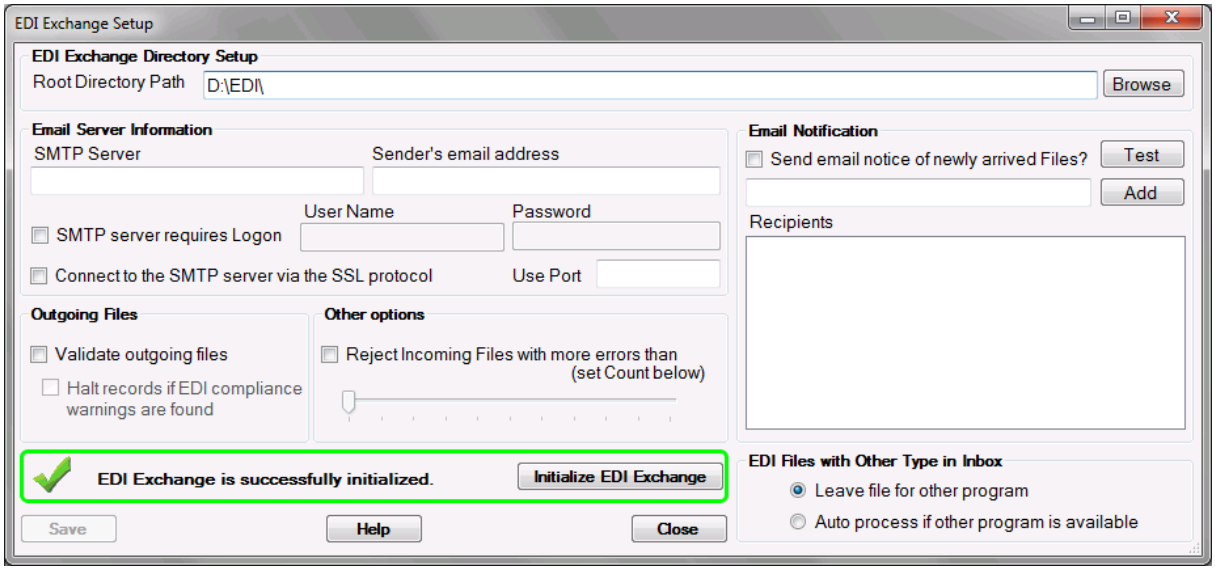
5. The last thing checked by the system is if the Automatic File Processing options have been set up. Read more in Defining Auto-Processing Options. The options are important for the hand over from EDI Exchange to the other HIPAAsuite program that hosts EDI Exchange.

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.

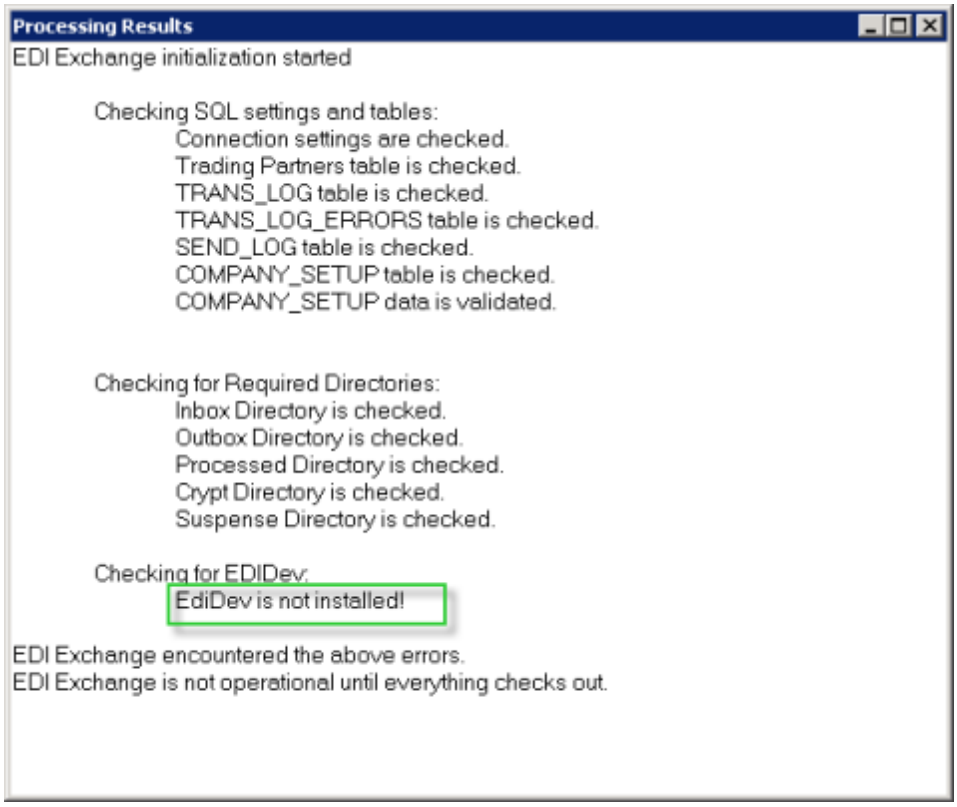


The "EDI Exchange is successfully initialized" message on the bottom of the "EDI Exchange Setup" window

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:

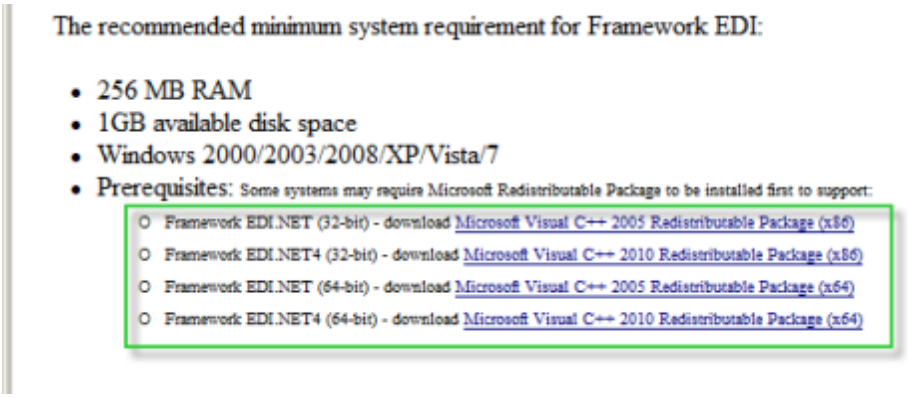
```
Checking for EDIDev:

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.


The recommended minimum system requirement for Framework EDI:

- 256 MB RAM
- 1GB available disk space
- Windows 2000/2003/2008/XP/Vista/7
- Prerequisites: Some systems may require Microsoft Redistributable Package to be installed first to support:
  - Framework EDI.NET (32-bit) - download Microsoft Visual C++ 2005 Redistributable Package (x86)
  - Framework EDI.NET4 (32-bit) - download Microsoft Visual C++ 2010 Redistributable Package (x86)
  - Framework EDI.NET (64-bit) - download Microsoft Visual C++ 2005 Redistributable Package (x64)
  - Framework EDI.NET4 (64-bit) - download Microsoft Visual C++ 2010 Redistributable Package (x64)

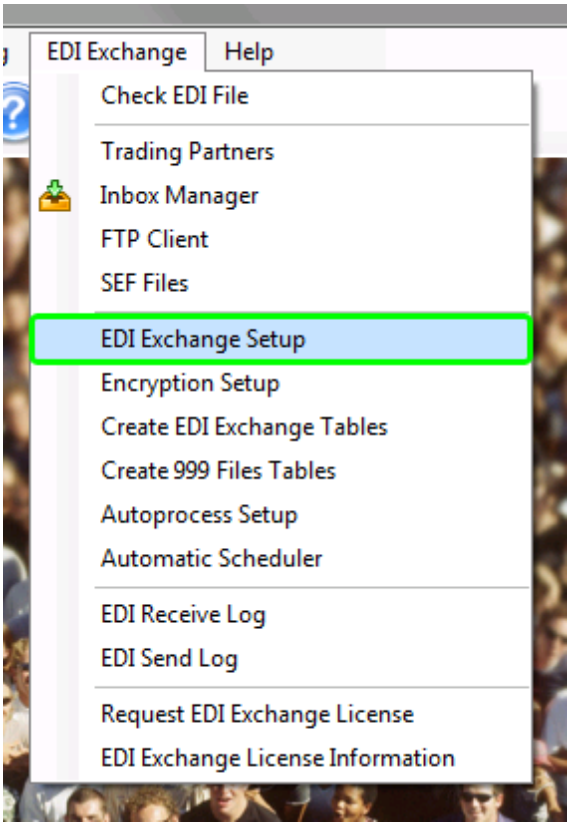
3. Download one of the following components you need according to your OS' bit depth:
   - Framework EDI Enterprise evaluation 32-bit
   - Framework EDI Professional evaluation 64-bit
4. Install downloaded components and start again the EDI Exchange initialization procedure.

7.3 Configuring EDI Exchange (Optional Settings)

7.3.1 Setting up Email Notifications

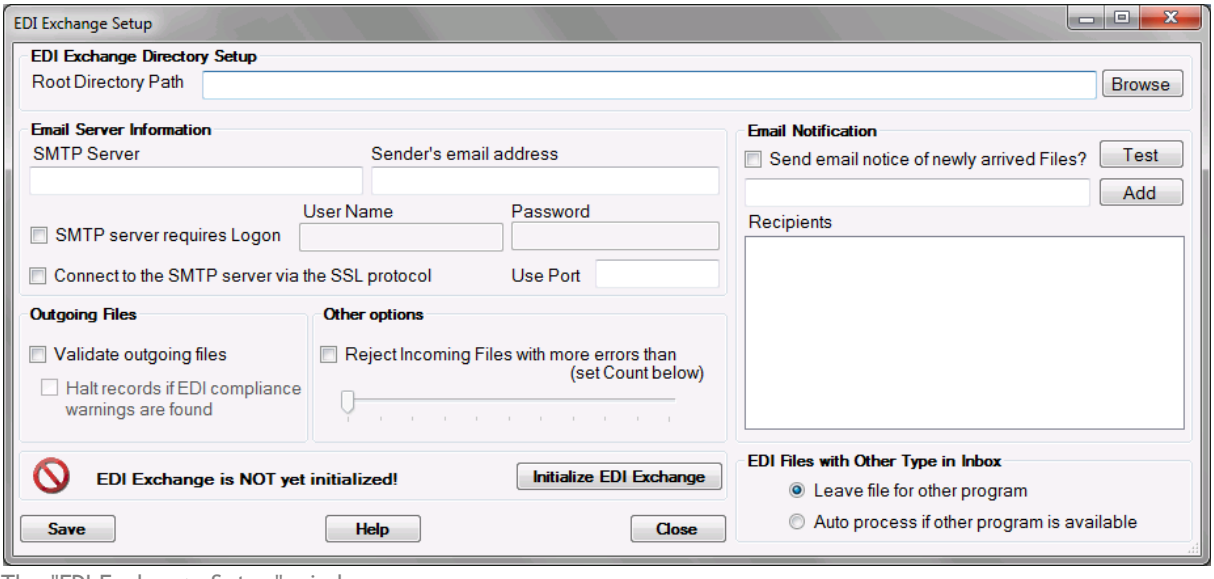
EDI Exchange can send emails to operators and trading partners to notify them about files and processing results. This functionality of EDI Exchange lies beyond the most basic setup that the initialization checks for. For this feature to work properly, you need to set up an email server which EDI Exchange 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.

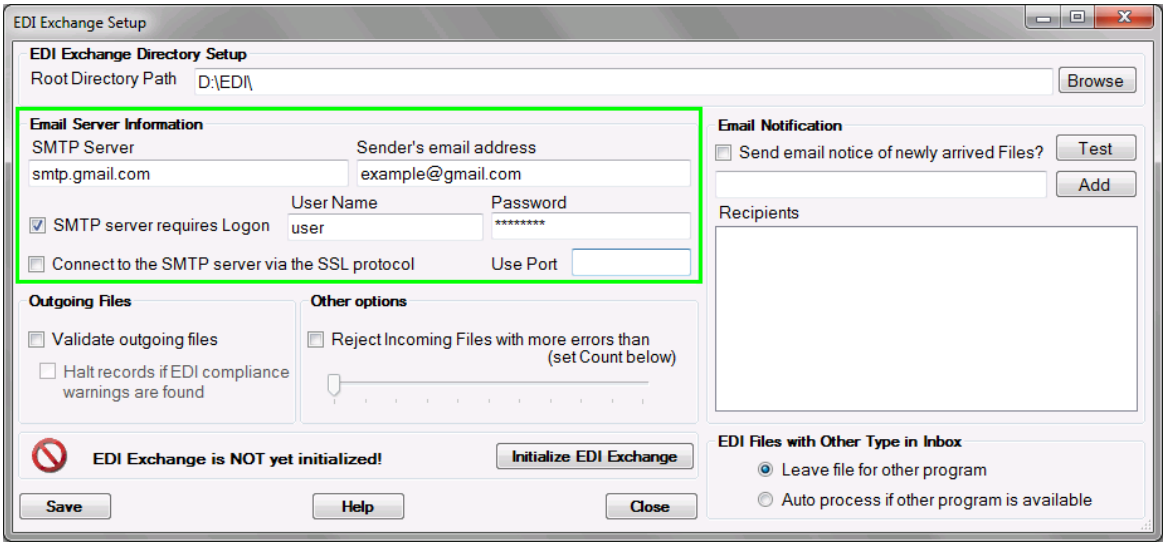


The "EDI Exchange Setup" window

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

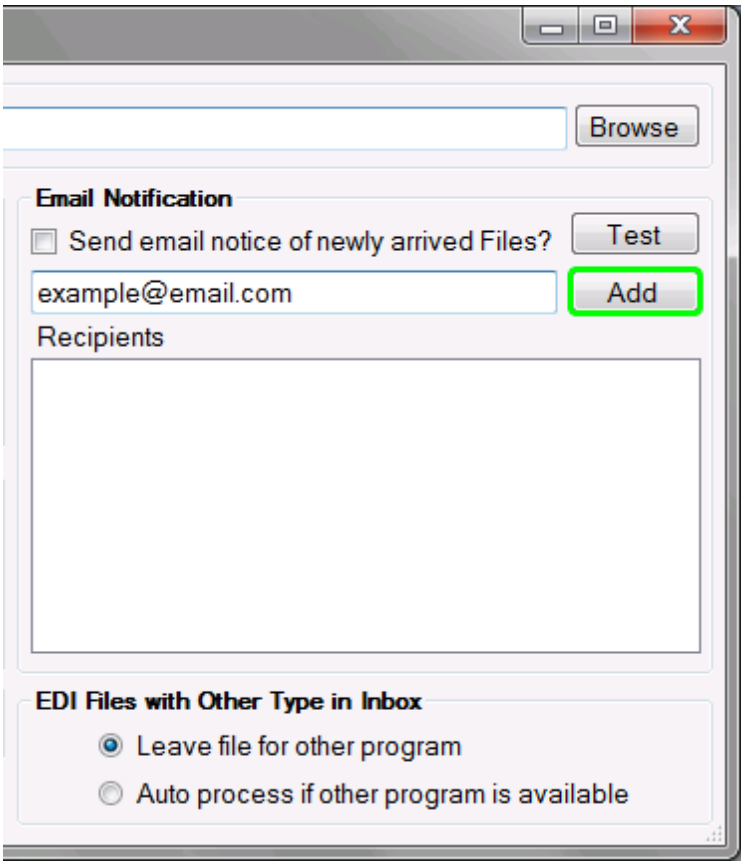
> Note: If you do not have this information, please ask your administrator to set this portion up for you.

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

Email Notification

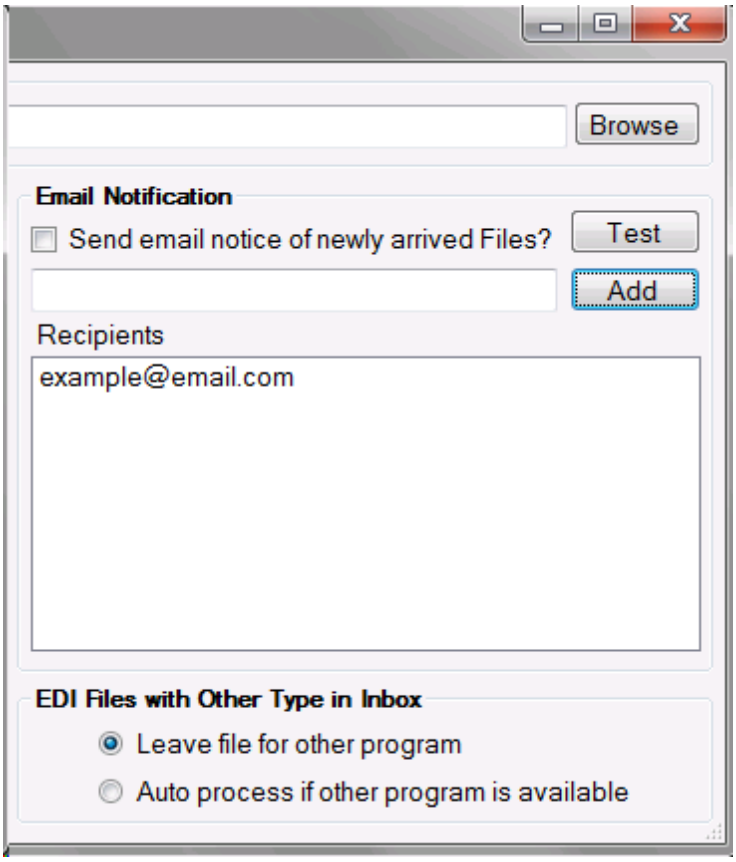
- **Send email notice of newly arrived files?** — Use this checkbox to define if you want to send email notice once new files have arrived.
- **Recipients** — You can add your staff's email(s) and the processing messages will be sent to these emails.

Enter an email address and click "Add."



Setting up the email recipients

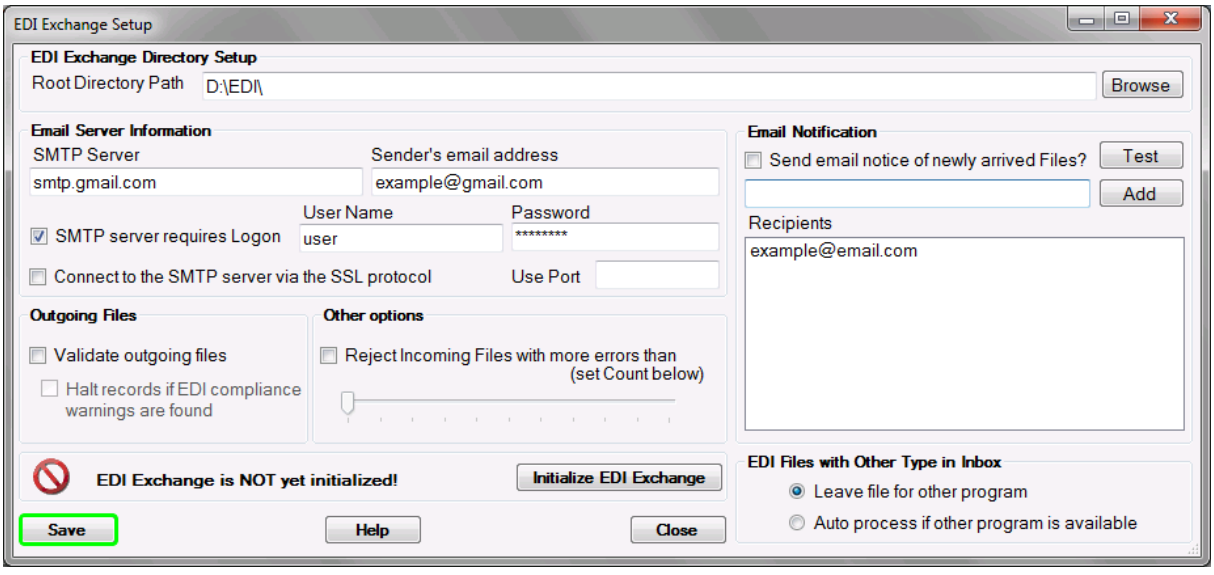
The email address will appear in the list.



Added email recipient

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

6. Click on the "Save" button.



The "Save" button

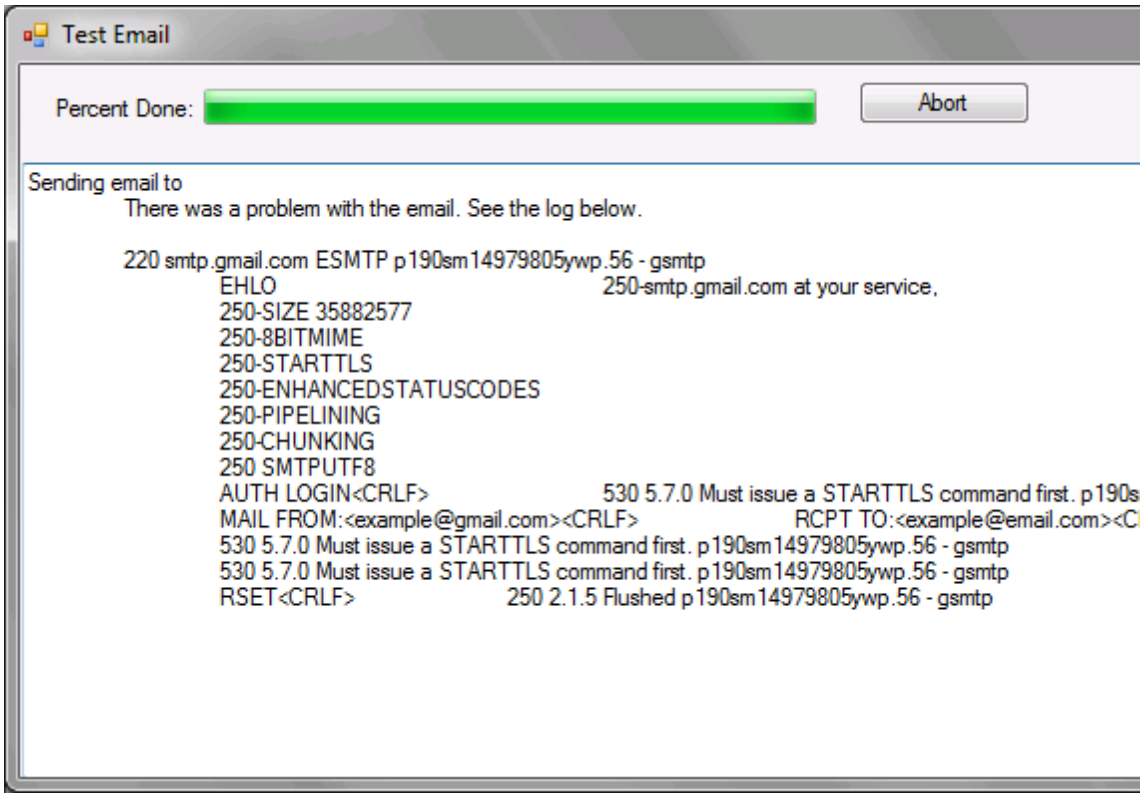
Troubleshooting Email Settings

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.



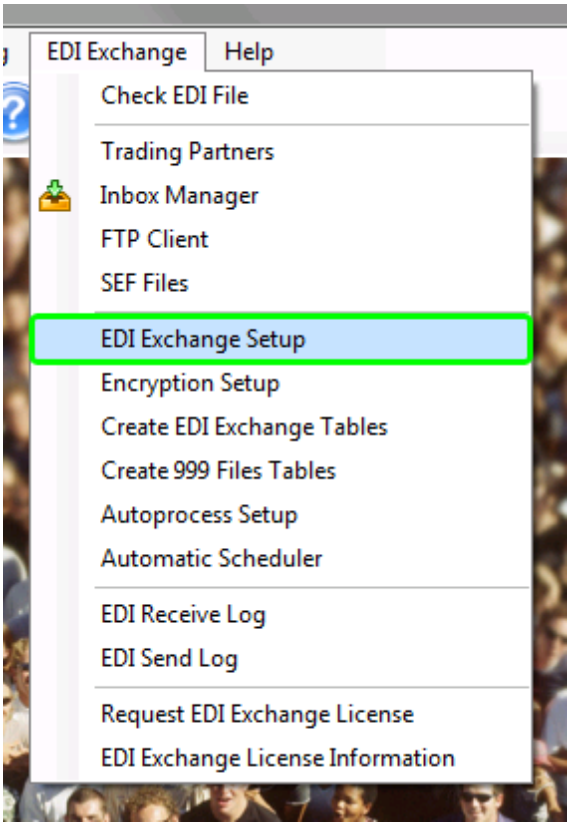
The process result screen with a detailed error message

7.3.2 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.

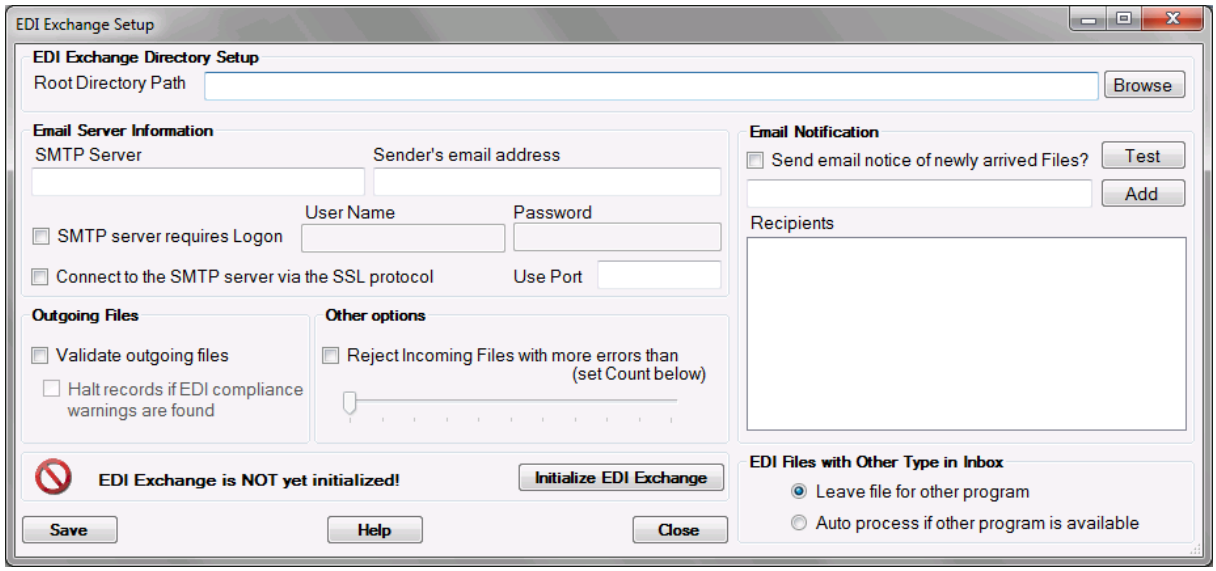
Follow the instructions below.

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



The "EDI Exchange Setup" menu item

2. The following window will appear.

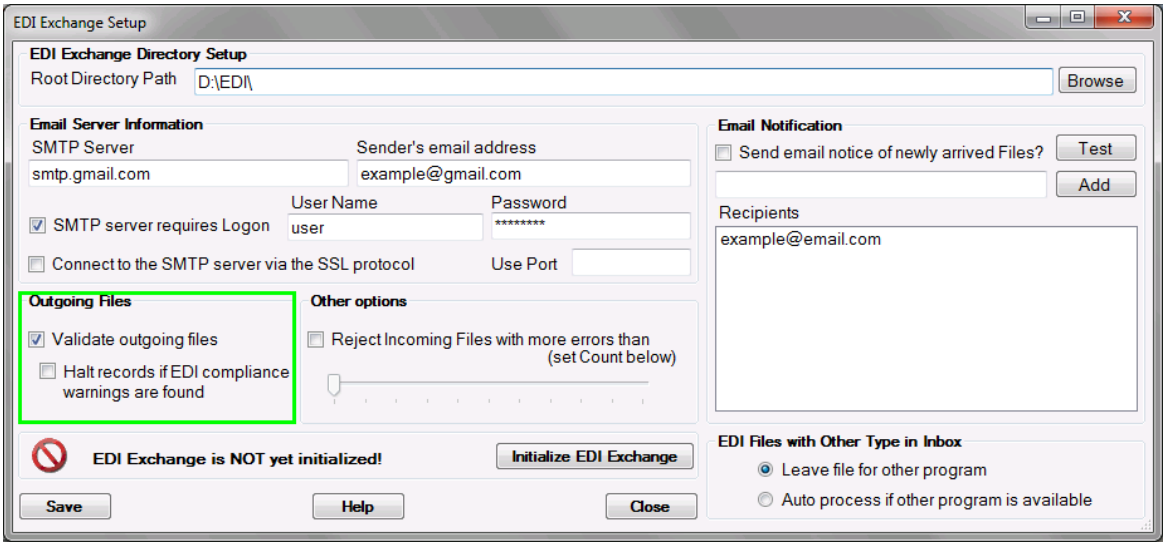


The "EDI Exchange Setup" window

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.

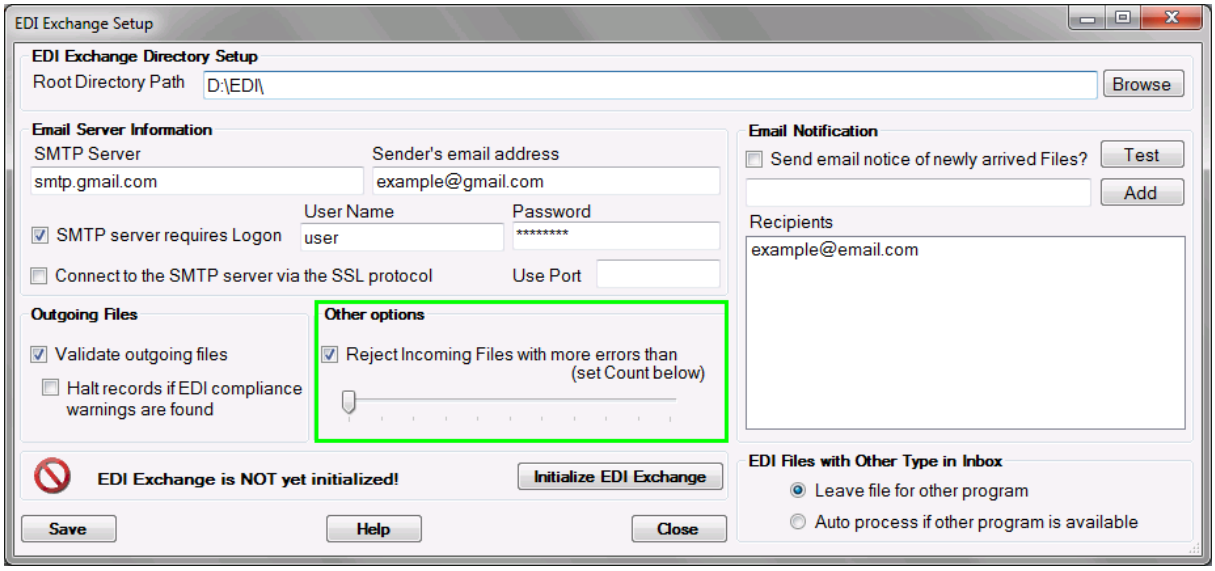


Validating outgoing files

4. Specify the following incoming files options:

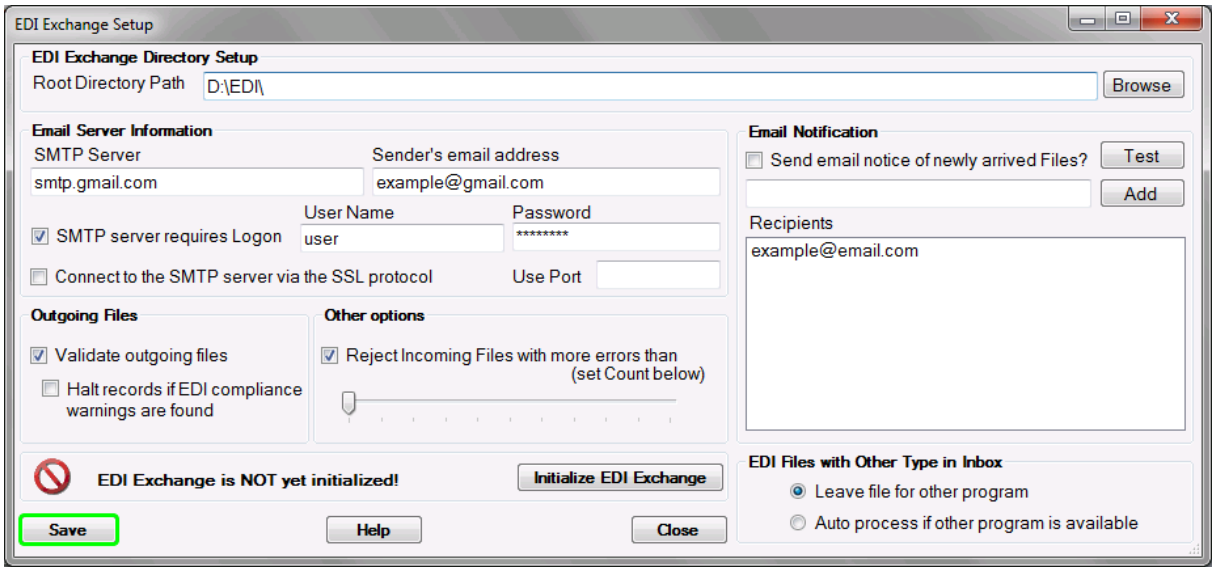
Other Options

- **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."



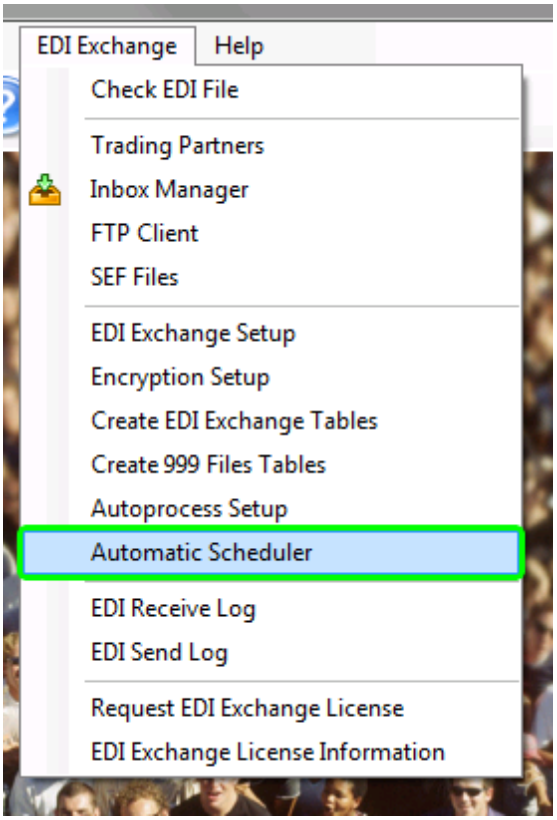
7.3.3 Running the Application via Scheduler

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.

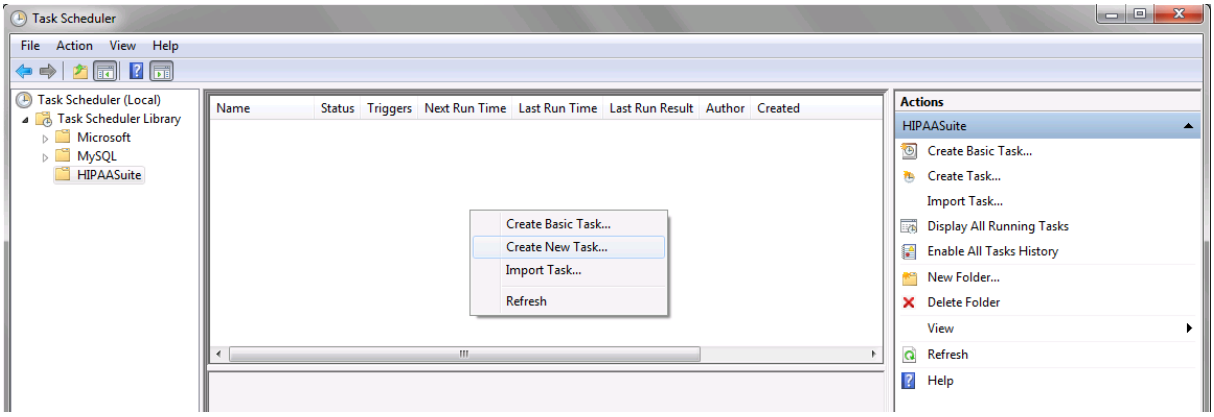
Follow the instructions below to schedule the EDI files exchange process.

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



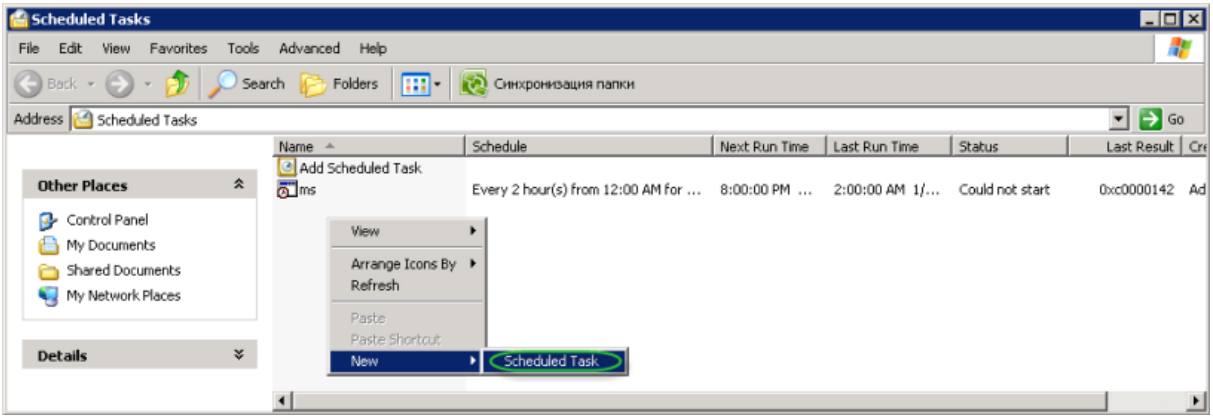
The "Automatic Scheduler" menu item

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



Task Scheduler in Windows Vista onwards.

In Windows XP, the Scheduled tasks directory looks like this:



The "Scheduled Task" menu item in Windows XP.

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

7.3.4 Using the Command Line Arguments (CLI)

The only EDI Exchange specific command line argument is "Auto"

The Auto processing options are defined in another screen and, with the command line argument "Auto," they will be exercised. Make sure that you have configured them according to your needs.

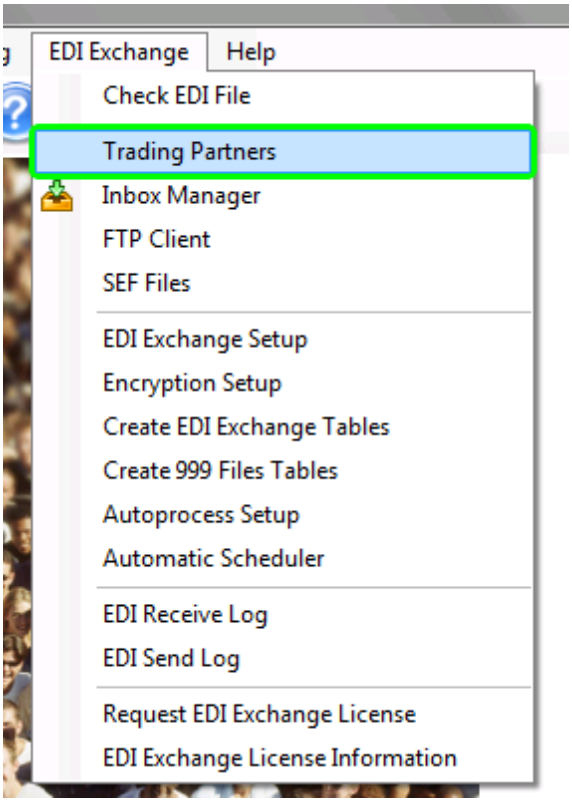
7.4 Working with Trading Partners

7.4.1 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.

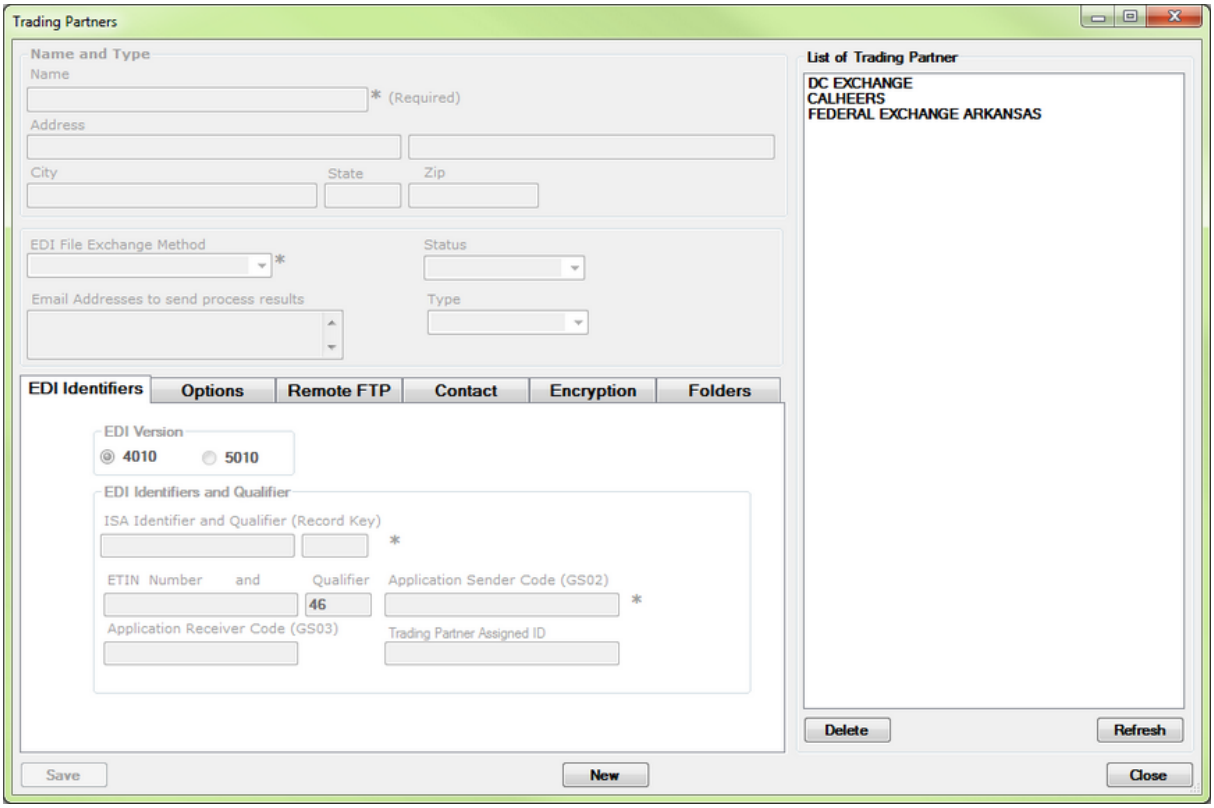
Once you have created the trading partner table (see Creating Database Tables) and initialized EDI Exchange (see Initializing EDI Exchange), you can set up the relationships with your trading partner. Follow the instructions below.

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



The "Trading Partners" menu item

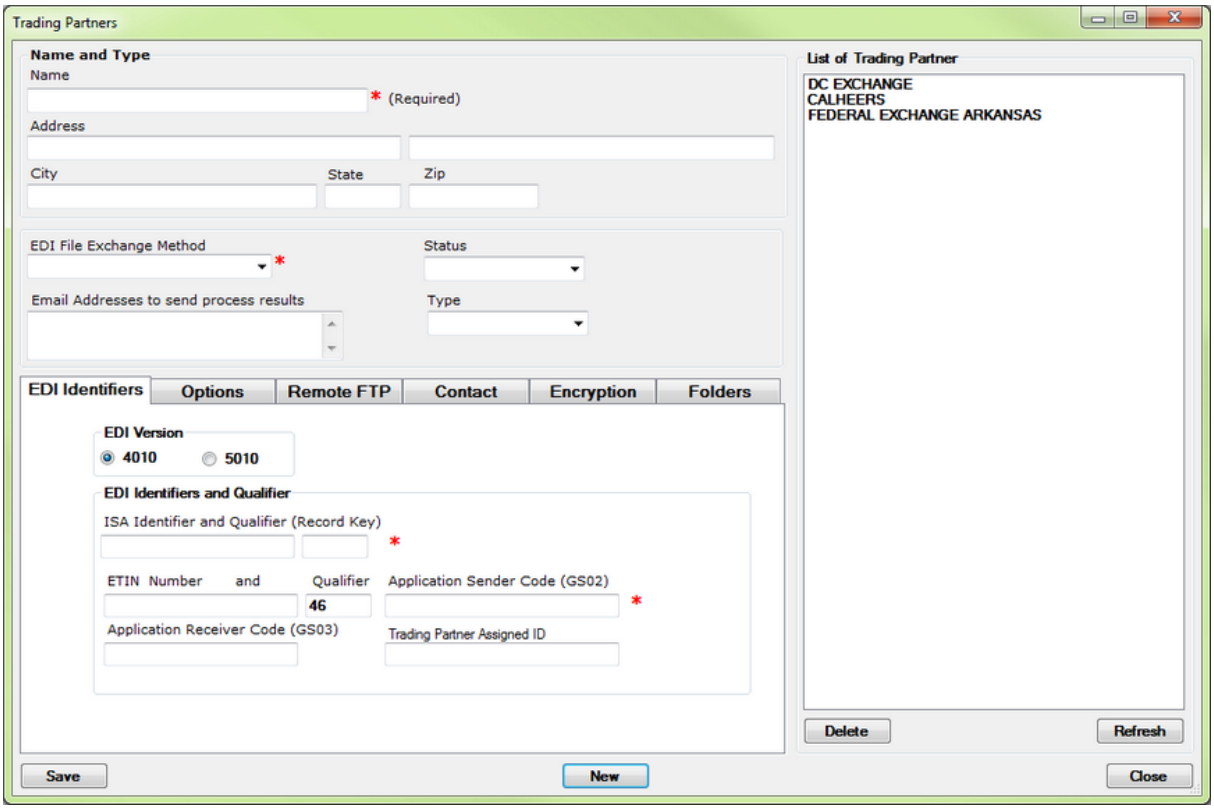
2. The following screen will appear.



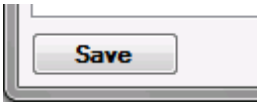
The "Trading Partners" window

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."

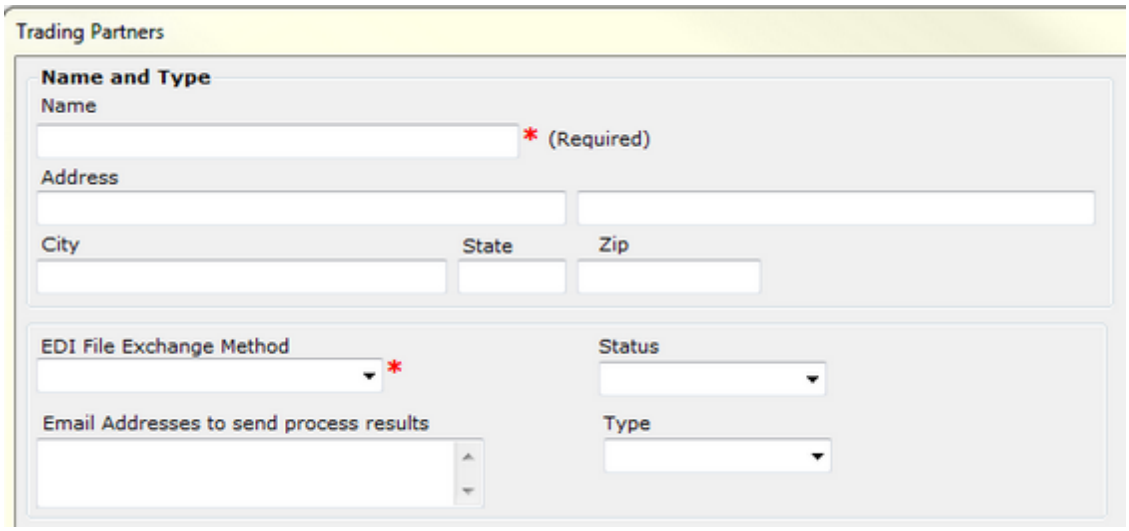


The "Save" button

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 Live 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.

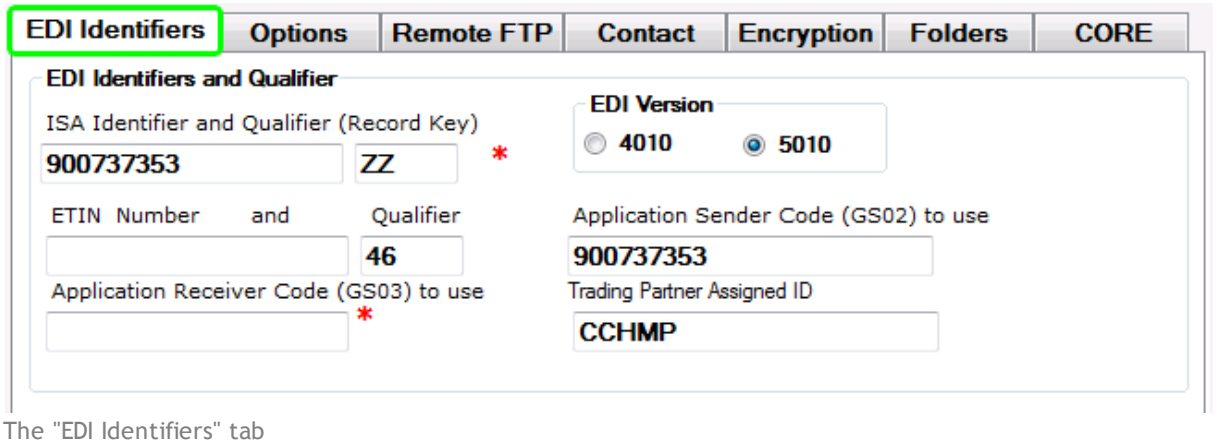
- **Payers** — Entities that pay for health care benefits such as health insurers.

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.
  - **SOAP** - Allows you to transmit files to the Trading Partner or his Clearinghouse using SOAP 1.2 (CORE) by default.
    - o **SOAP Version** - Defaults to CAQH CORE "SOAP 1.2". "SOAP 1.1" is also provided as a compatibility option for Trading Partners that are not yet CORE-Certified but use SOAP services.
  - **MIME** - Allows you to transmit files to the Trading Partner or his Clearinghouse using MIME (CORE). This is one of two CORE options.
- **Email Addresses** — Enter the email address(es) into the text field.

EDI Identifiers Tab

This tab relates to the EDI identifiers and EDI Version.



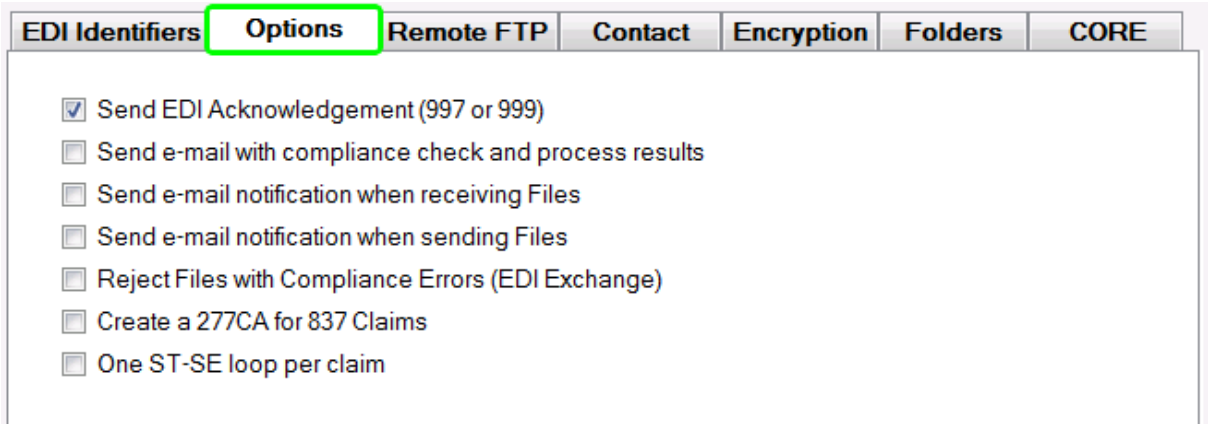
The "EDI Identifiers" tab

- **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.
  - **Assigned ID** - Some trading partners, like health insurance exchanges will give a plan an ID that is different from the ISA identifier defined in the Company Setup screen of the application. Especially in the creation of filenames is this Assigned ID important.

Options Tab



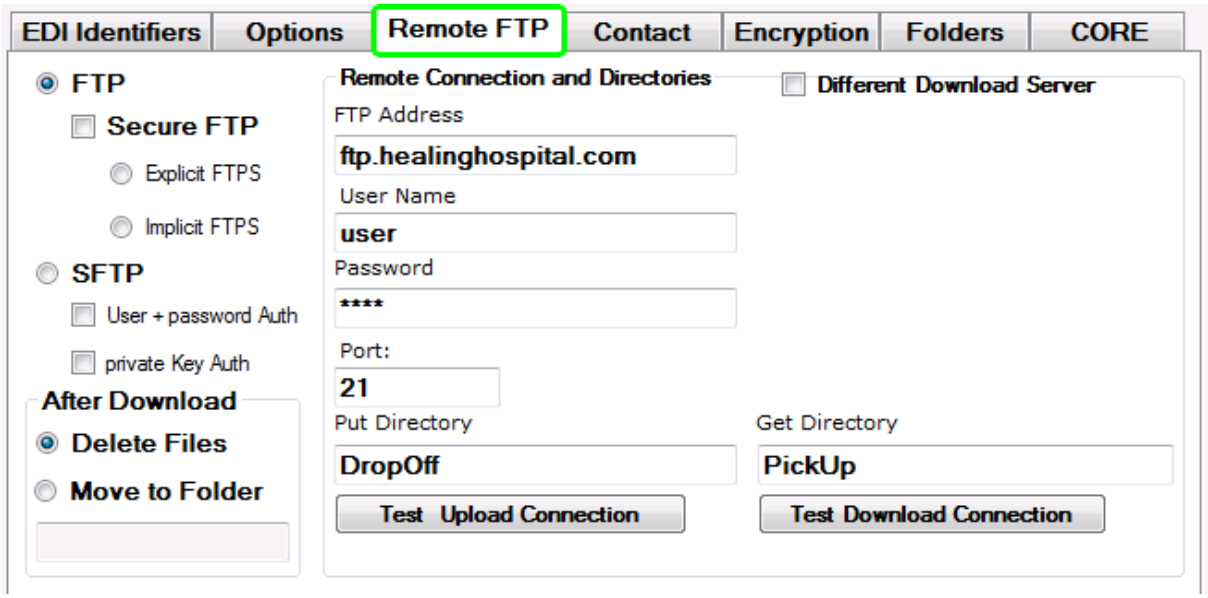
The "Options" Tab

You can choose one of the following options:

- **Send EDI Acknowledgment (997 or 999)** — This check-box allows sending Functional Acknowledgment transactions to the Trading Partner.
- **Send e-mail with compliance check and 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."
- **Send e-mail notification 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.
- **Send e-mail notification when sending files** — This option allows sending a file to the Trading Partner notifying them that a file has been created for them.
- **Reject Files with Compliance Errors -** This option will reject files that have compliance warnings and move them into the suspended files directory. It also determines whether the TA1 and 999 indicate acceptance or the 999 lists all the errors and warning.
- **Create a 277CA for 837 claims** — This option only applies to 837 Claims. Checking this option will produce a 277CA Claims Acknowledgment report for received 837 Claim files.
- **One ST-SE loop per claim** - This option separates all claims into individual transactions enclosed by their own ST and SE segments.

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

The file transfer protocol (FTP) is one of the first internet protocols and goes back to the 1960's. Transporting electronic files was one of the great achievements of the internet. During the last 50 years a lot of improvements to this protocol have been made, mainly to increase the security of the transfer.

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

- **SFTP** — also known as FTP over SSH is deemed the most secure form of FTP and uses encryption certificates. There are 3 different ways to authenticate a SFTP connection,
  - With user name and password, just like a regular FTP connection,
  - User name and a certificate
  - User name, certificate and password

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:

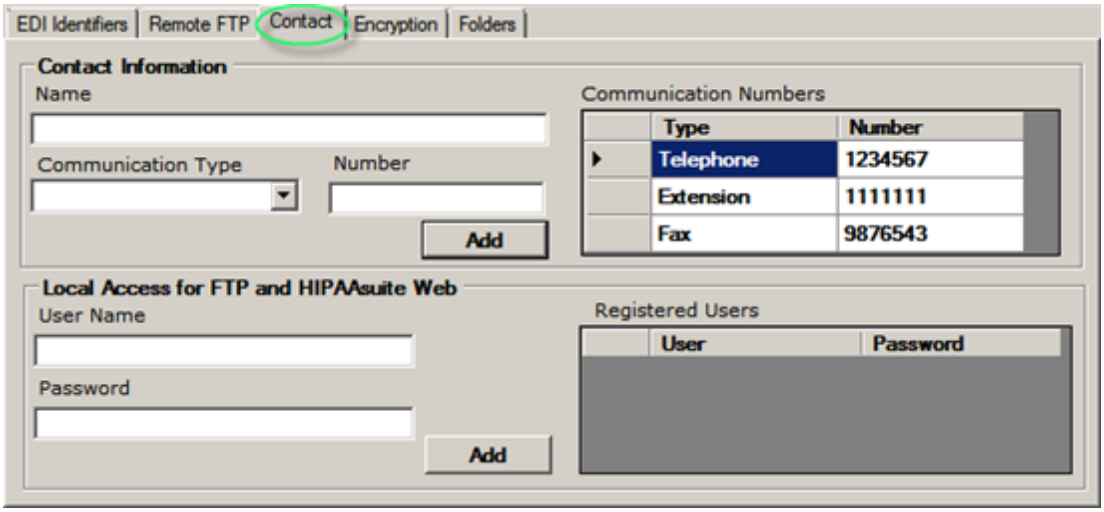
- **FTP Address -** This is usually the IP address of the server
- **User Name**
- **Password**
- **Put Directory -** This is the directory where you drop off files
- **Get Directory -** This is the directory where you download files from

It is possible that a trading partner has two FTP servers, one for 'put' and another one for 'get'. If so, check "Different Download Server" and additional fields will become visible so you can specify the those connection parameters.

After Download: You have two choices. Files on the server will be either deleted or moved to another folder of your choice .

Contact Tab

The Contact Tab stores contact information for your selected Trading Partner.



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.

- **Contact Name**
- **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

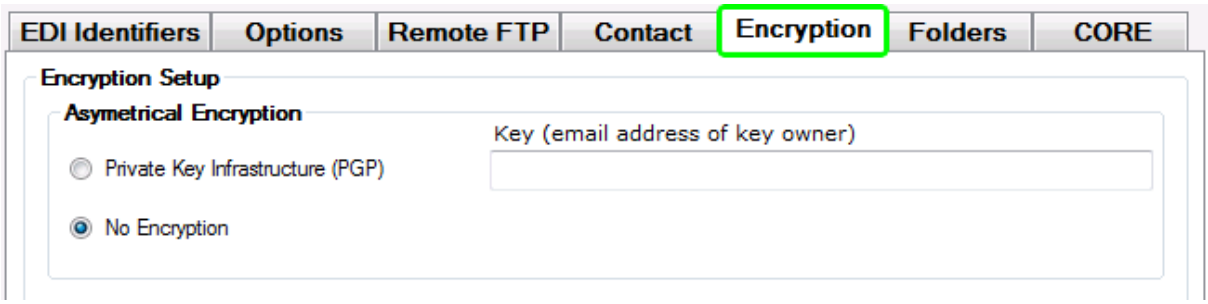
To register a user, enter the user name and the password into the corresponding fields and click the "Add" button. The user will appear in the "Registered Users" table.

- **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

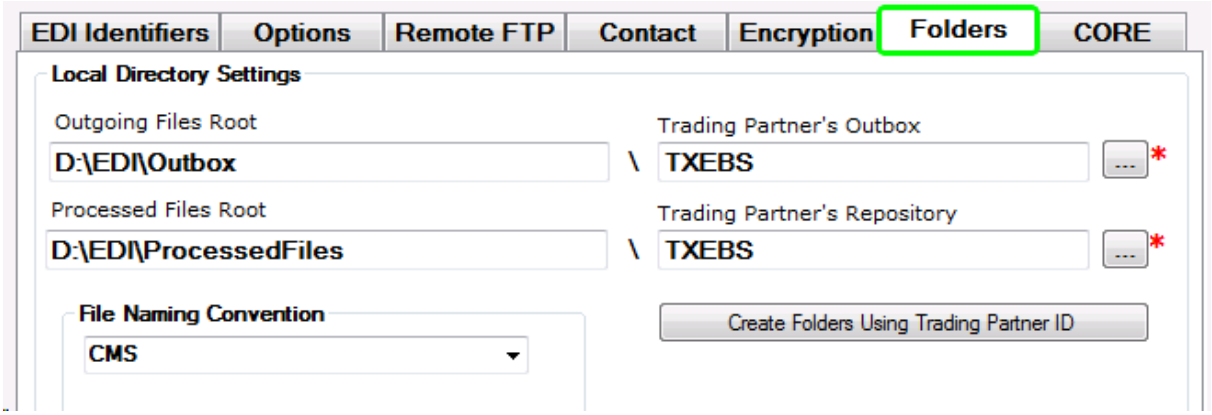
Encryption Setup

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

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

Folders Tab

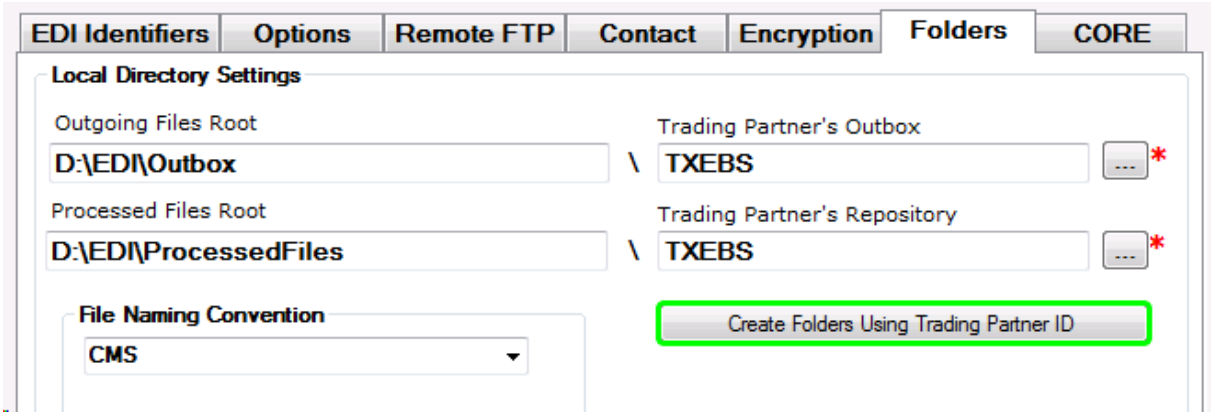
Within the HIPAAsuite Communications Directory, each Trading Partner has his own folder. This keeps files finely separated and in order. Here is where you can set this up. Read more in Defining Communications Directory.



The "Folders" tab

- **Outgoing Files Root** — This field has a pre-generated path. You can change this path by changing the EDI Root Directory.
- **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 by changing the EDI Root Directory.
- **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.

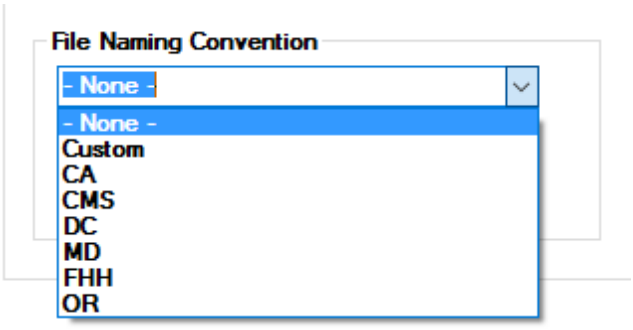
Once you have specified the directory settings, click on the "Create Folders Using Trading Partner ID."



The "Create Folders Using Trading Partner ID" button

- **File Naming Convention** - Health Insurance Exchanges (HIX) demand that a carrier adheres to more or less complex File naming conventions. Since these conventions are often really complicated we decided to hard code several schemes. California,

Maryland, DC and the CMS scheme are among those currently configured and we will add other schemes if needed.

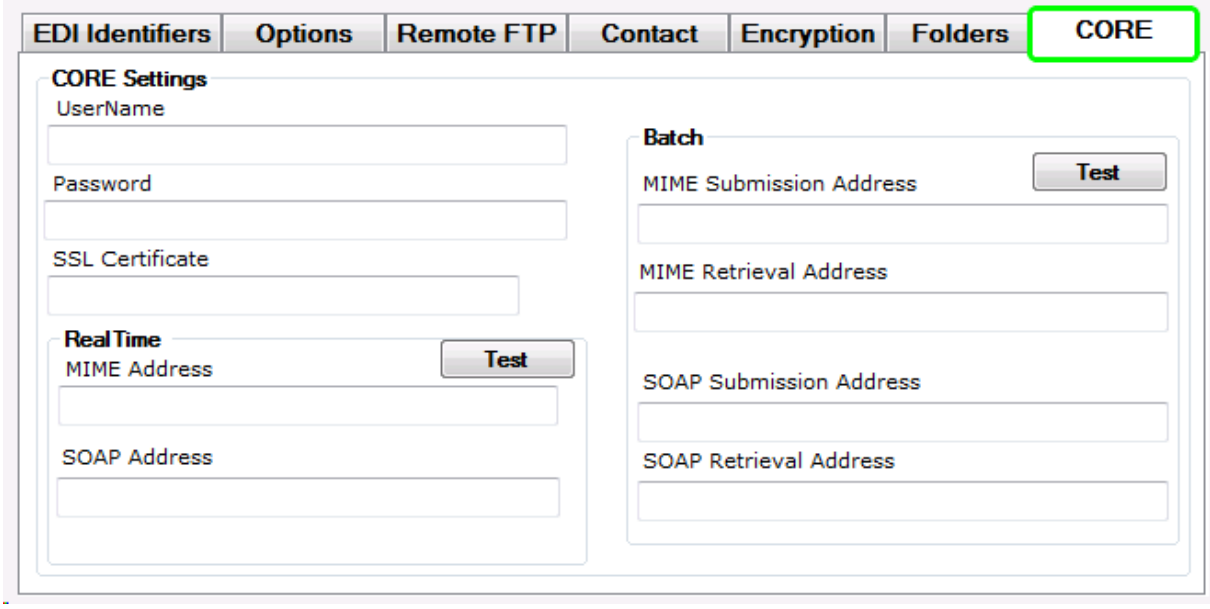


Filenaming dropdown menu options

The *Custom* File Naming Convention option requires some additional setup. This is covered in Custom File Naming Conventions.

CORE Tab

This tab stores settings for the use of CORE-Compliant SOAP- and MIME-enveloped transactions. When using a Requester or similar application, these settings apply to the information source. When using a Responder or similar application, these settings apply to the information requester/receiver. Soap 1.2 or 1.1 will use the same options.

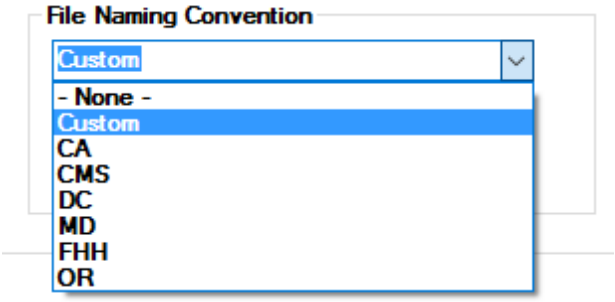


CORE settings tab

- **UserName** - UserName portion of the username authentication token. Used to verify a Trading Partner's Username token's Username or in your own Username token authenticate yourself to a Trading Partner's CORE-compliant servi e.
- **Password** - Password portion of the username authentication token. Used to verify a Trading Partner's Username token's Password or in your own Username token to authenticate yourself to a Trading Partner's CORE-compliant service.
- **SSL Certificate** - Instead of Username tokens, use an SSL certificate to verify a Trading Partner's identity or access a Trading Partner's CORE-compliant service. Not currently implemented.
- **RealTime**
  - **MIME Address** - Trading Partner's web address for MIME Real-Time transactions.
  - **SOAP Address** - Trading Pertner's web address for SOAP Real-Time transactions.
- **Batch**
  - **MIME Submission Address** - Trading Partner's web address for MIME Batch transactions.
  - **MIME Retrieval Address** - Some Trading Partners may use a different address to submit or retrieve batch transactions. Use this field for a retrieval-specific address.
  - **SOAP Submission Address** - Trading Partner's web address for SOAP Batch transactions.
  - **SOAP Retrieval Address** - Some Trading Partners may use a different address to submit or retrieve batch transactions. Use this field for a retrieval-specific address.

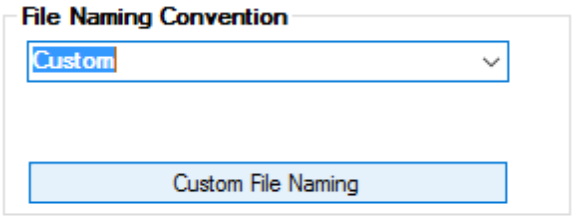
7.4.2 Custom File Naming Conventions

Health Insurance Exchanges (HIX) demand that a carrier adheres to File naming conventions. These file naming conventions enable a reader to quickly determine the date, time, sender, recipient, etc. of a particular file among other files without the need to open them individually. The custom File Naming Convention option enables you to create a file naming convention scheme tailored to your (or your trading partner's) requirements.



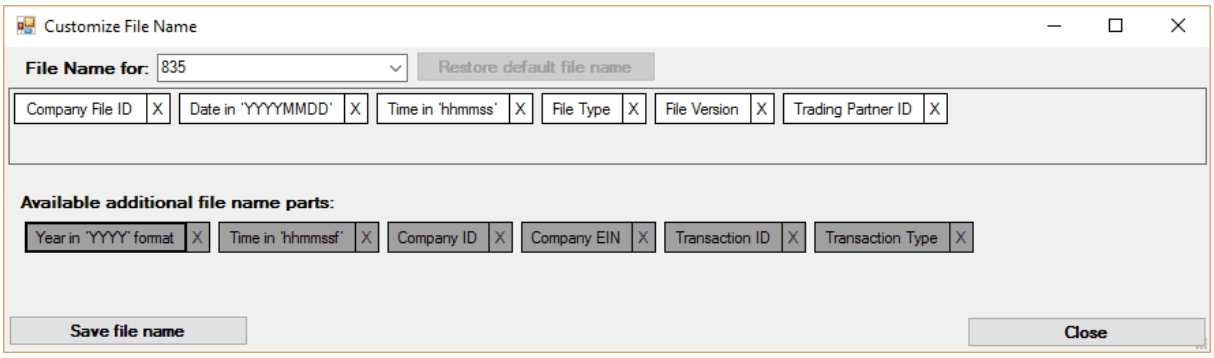
Custom File Naming Convention option highlighted

Selecting the Custom option in the File Naming Convention dropdown menu option and clicking the *Custom File Naming* button below it:



Custom File Naming button enabled

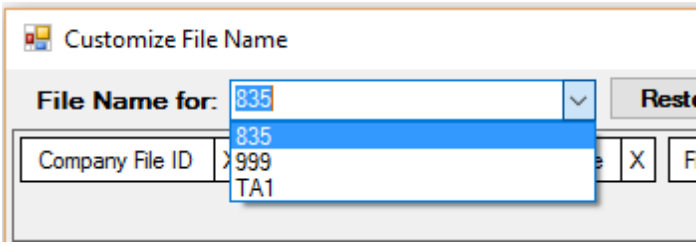
will bring up the screen pictured below. This screen is used to create file naming conventions for a particular trading partner. These examples will use the 835 file type as an example, but all file types the HIPAASuite product represents (as well as TA1s and 999s) can have their own file naming convention applied to each trading partner. The following picture shows the file name customization screen with the default building blocks for an 835 EDI file.



File Naming Customization screen with default custom file naming convention

Filetype

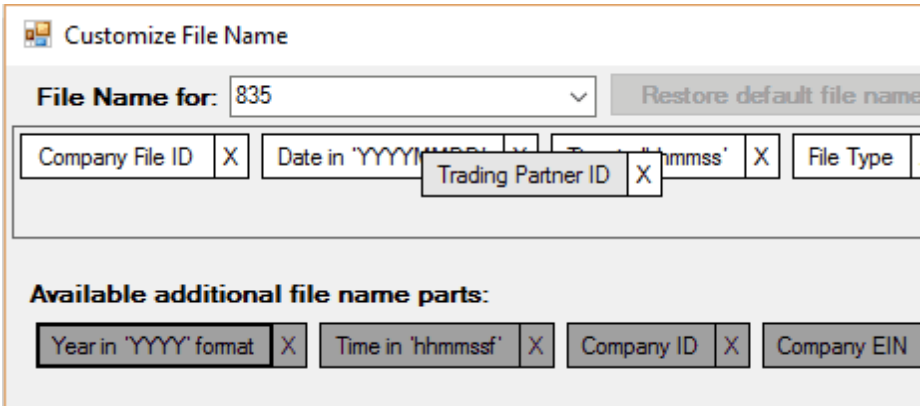
Here we can create a custom file naming convention for a specific file type. The file types available will depend on the HIPAASuite product used to create the file naming convention. To change the file type, select it from the file type dropdown menu:



Changing the filetype

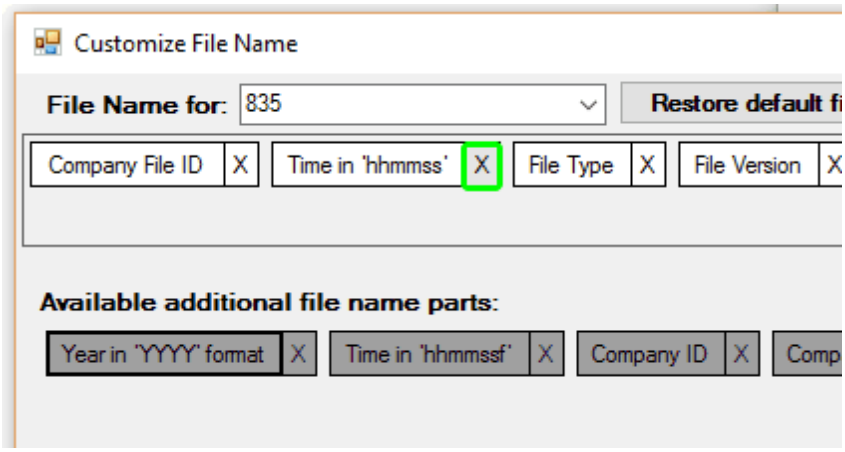
Creating the file naming convention

A coherent file naming convention can be created by clicking and dragging elements into order. Present elements can be reordered by clicking and dragging them into position:



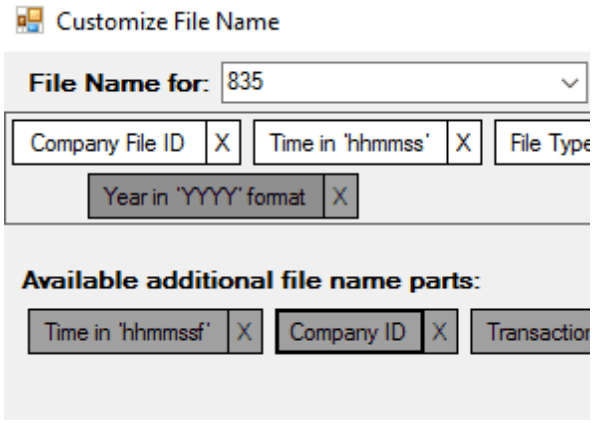
Click-dragging an element into position

Existing elements can be removed by clicking the *X* to the right of the element:



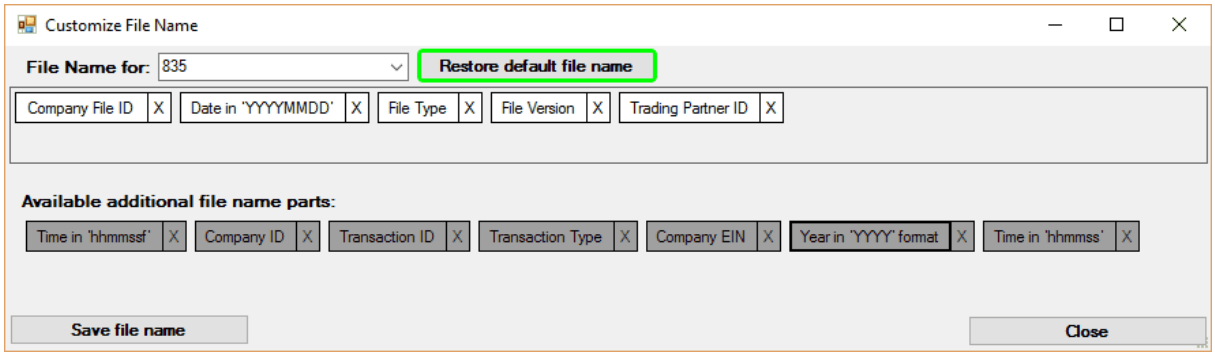
Deleting an element

The greyed-out elements towards the bottom of the screen can be added to the custom file naming convention by clicking and dragging them into place:



Adding a file name element

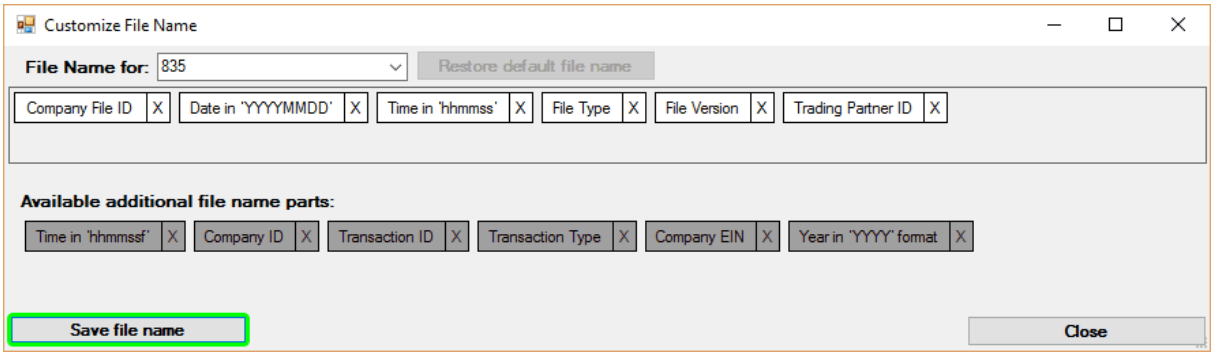
To discard the current changes and start over with the default file naming convention, click the *Restore default file name* button.



Restore default file name button

Saving or discarding

Finally, the custom file naming convention can be saved by clicking *Save file name* or discarded by clicking *Close*.



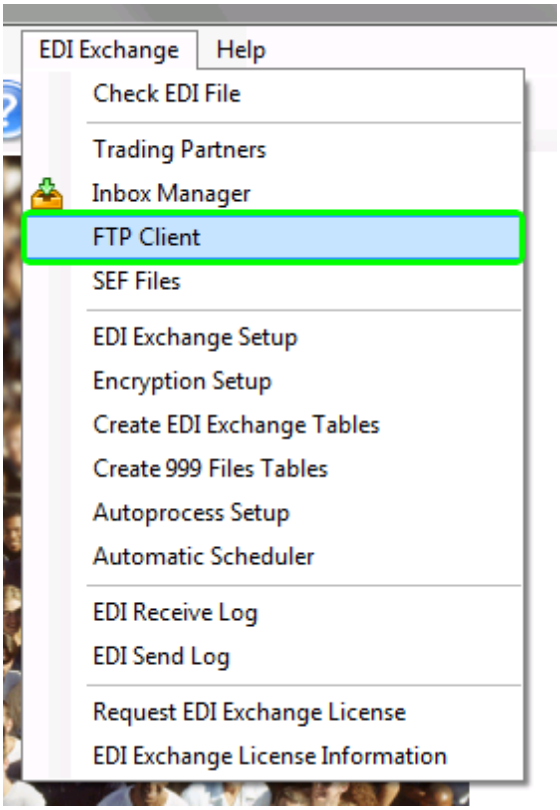
Save button on file name customization screen

7.4.3 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.)

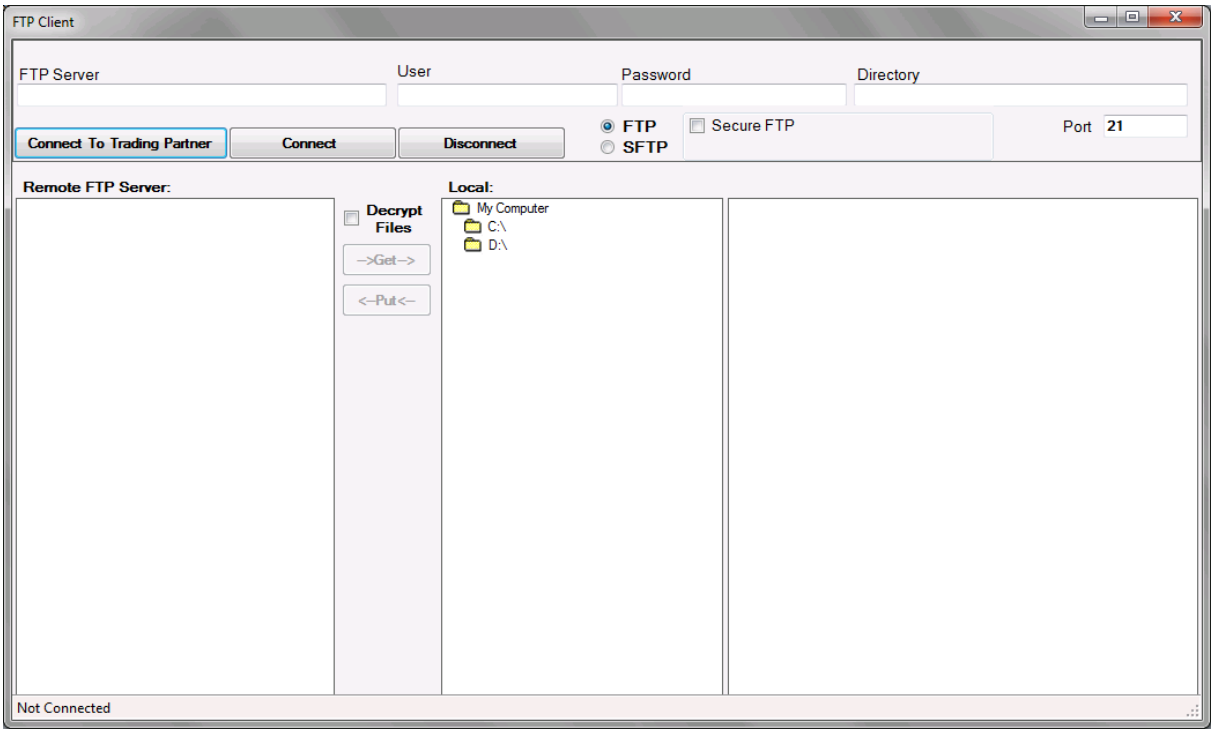
Follow the instructions below to exchange EDI files with your Trading Partner.

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



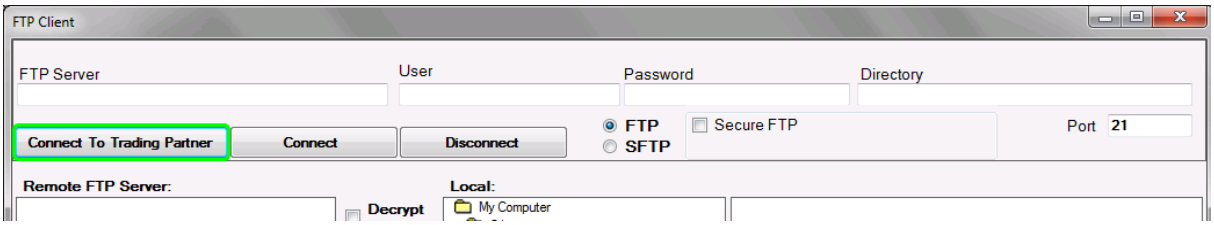
The "FTP Client" menu item

2. The following window will appear.



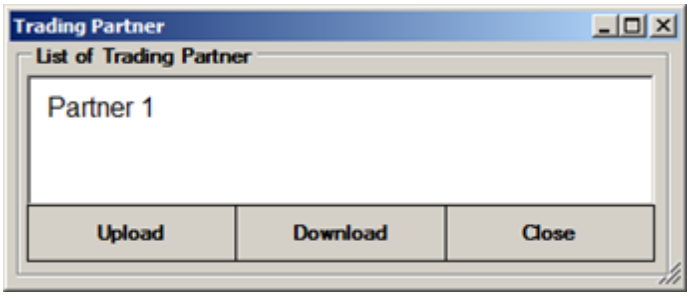
The built-in FTP client

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



The "Connect to Trading Partner" button

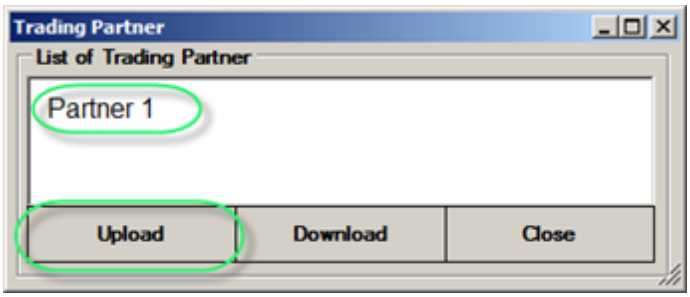
4. The following screen opens.



Selecting a Trading Partner for FTP transfer

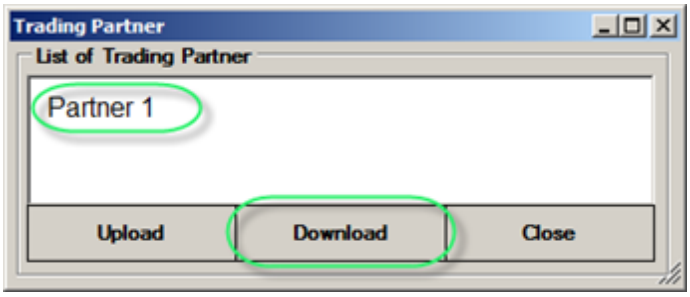
5. Highlight the trading partner that you want to connect to.

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.



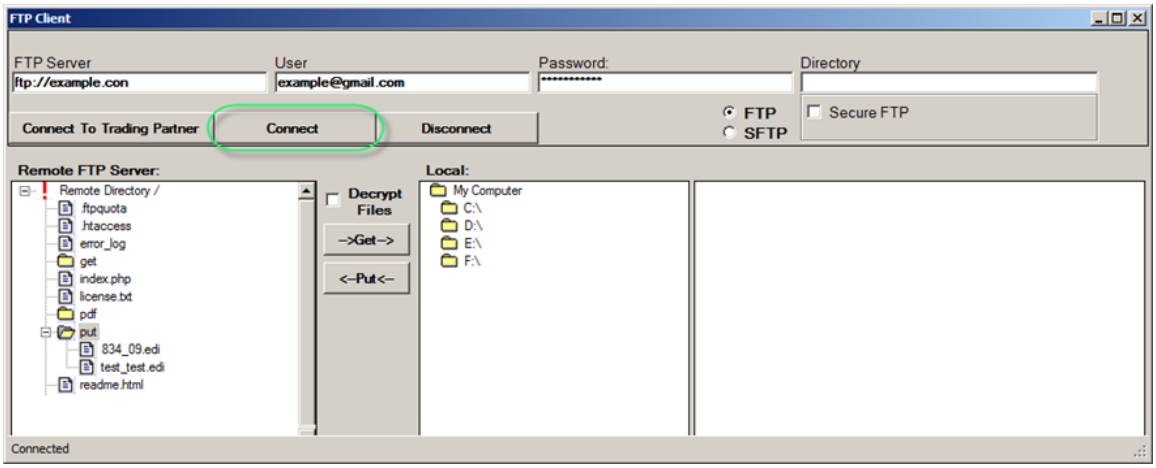
The "Download" button

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**

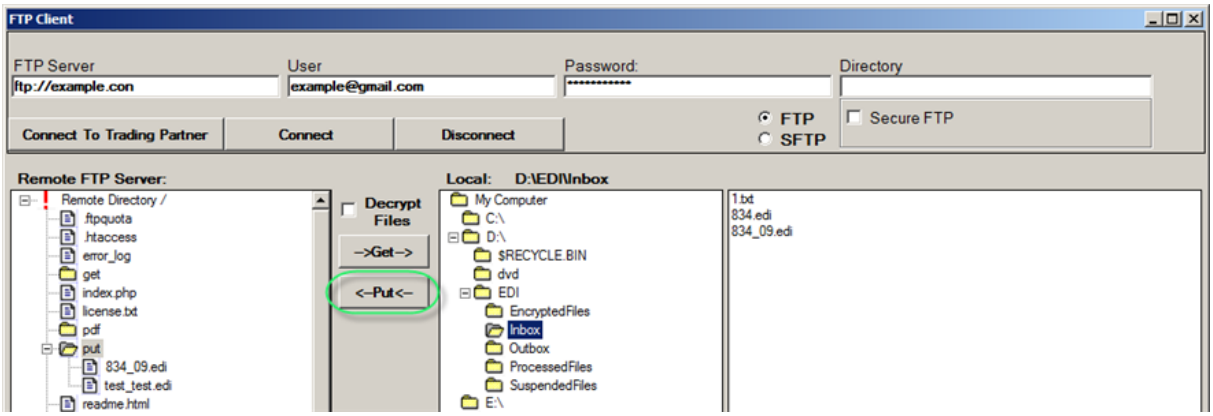
Note: You can also fill in the connection information manually. In this case, the entered credentials will not be saved once you close the FTP client window. Click on the "Connect" button to establish

connection to the FTP server.

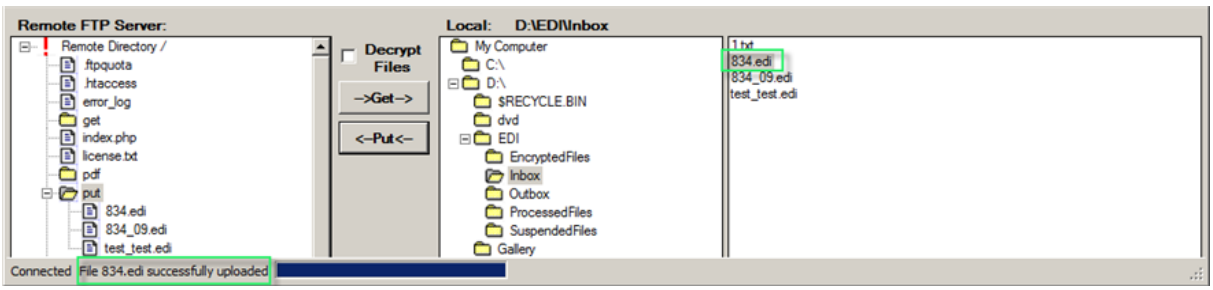


4. Once connected, the content of the folder on the server is displayed. On the right side, you can browse your local PC.

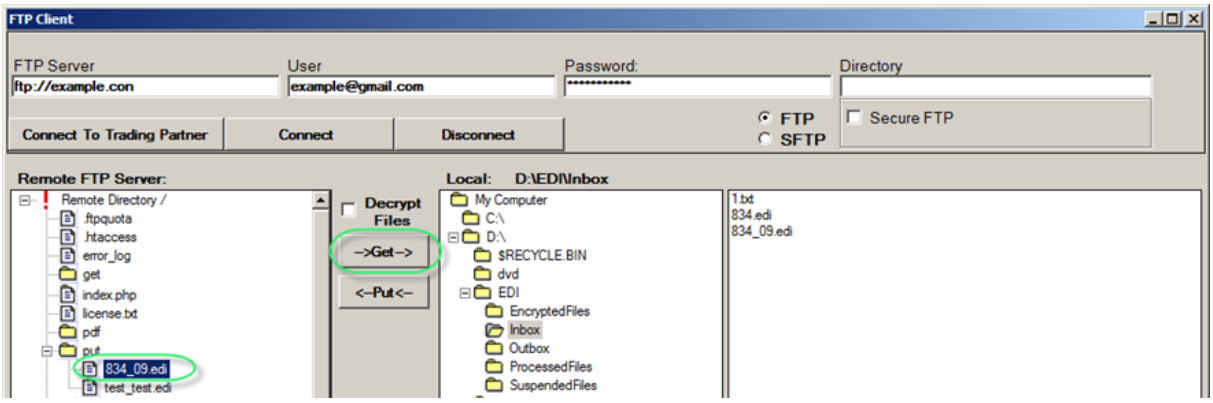
5. To upload a file to the server, select the file on your local PC and click on the "Put" button.



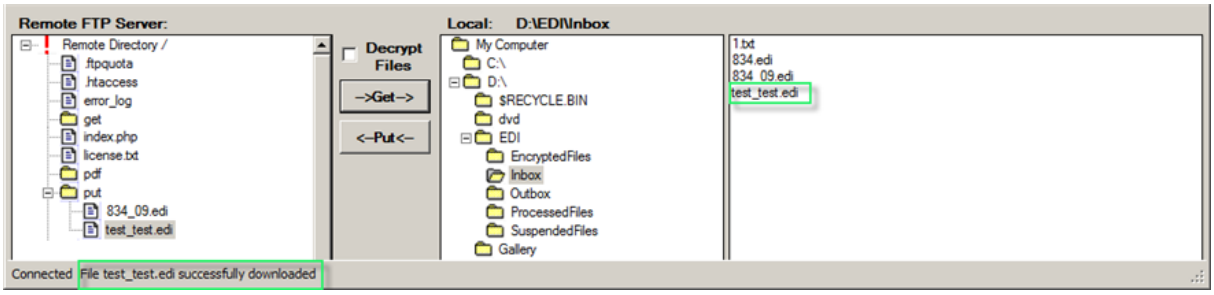
The file will appear in the remote folder. You will receive the "File <filename> successfully uploaded" message on the bottom status bar of the FTP client.



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

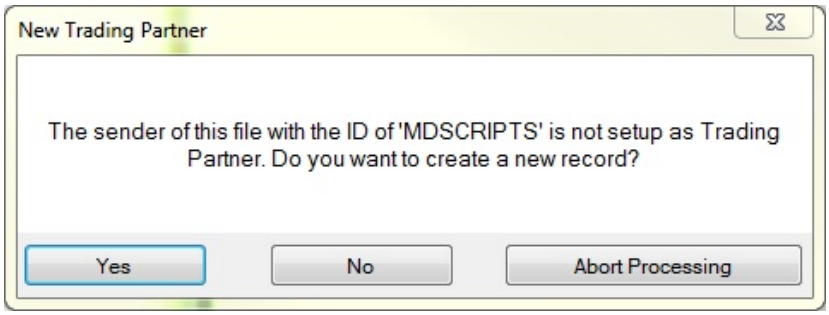


The file will appear in the local folder. You will receive the "File <filename> successfully downloaded" message on the bottom status bar of the FTP client.



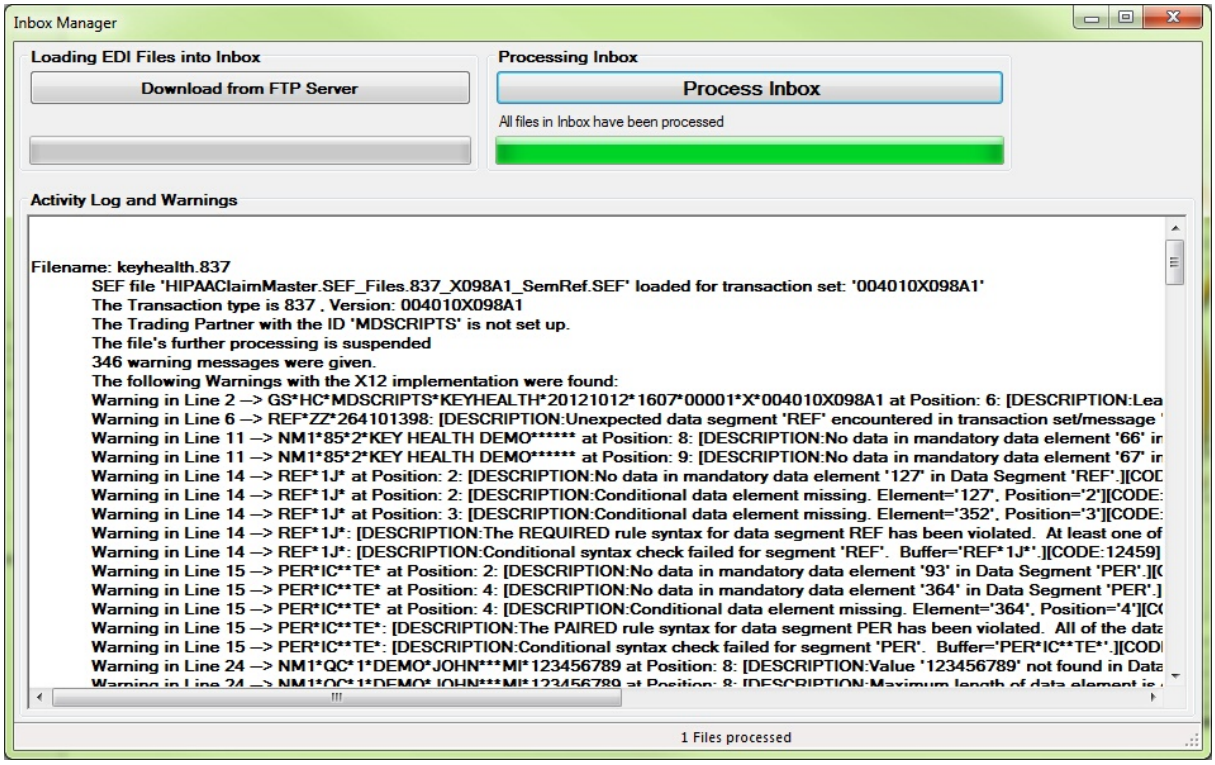
7.4.4 Creating a Trading Partner Automatically

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.



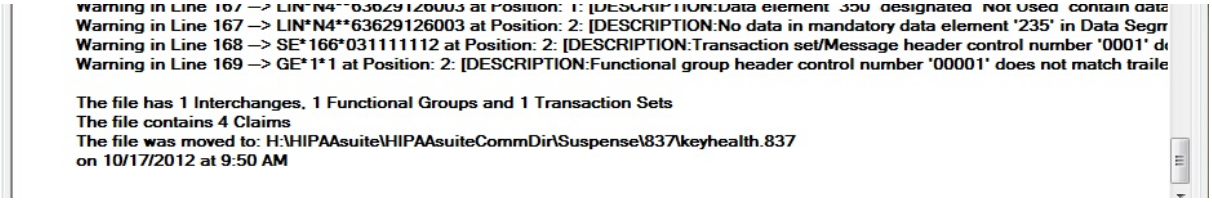
The "New Trading Partner" dialog box

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 the "suspended files" directory. The final action taken after the analysis is recorded at the end of the results.



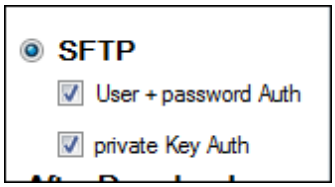
This file's processing was aborted. The file was moved to the suspended files folder

7.4.5 Certificate based authentication in SFTP

SFTP or FTP over secure shell as it is also known is deemed to be the most secure method of file transport. There are 3 methods of authentication in Sftp.

1. with a user name and password
2. with a user name and a private key cryptographic certificate and
3. with a user name, a certificate and a password

When you select SFTP as the FTP protocol, you will see two check boxes appear.



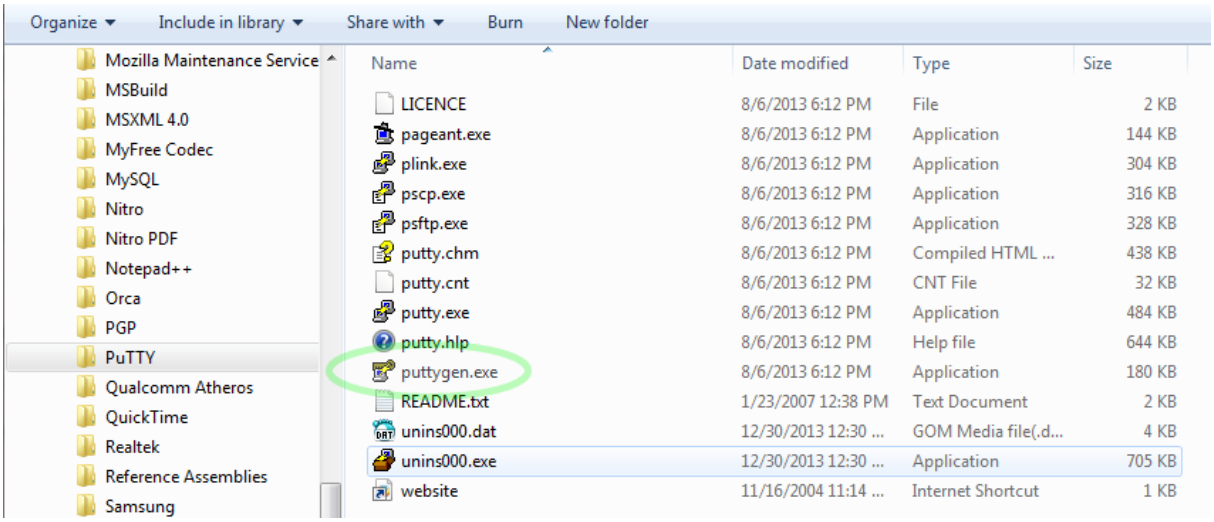
The sub choices when you select SFTP

Leaving both check boxes unchecked will result in the first option: Authentication with user name and password. You can also check just the user name and password with the same result.

In order to use the certificate based authentication you need to create and link to your own certificate. The certification module that HIPAAsuite employs uses a so called private key SSH2 certificate in pem format.

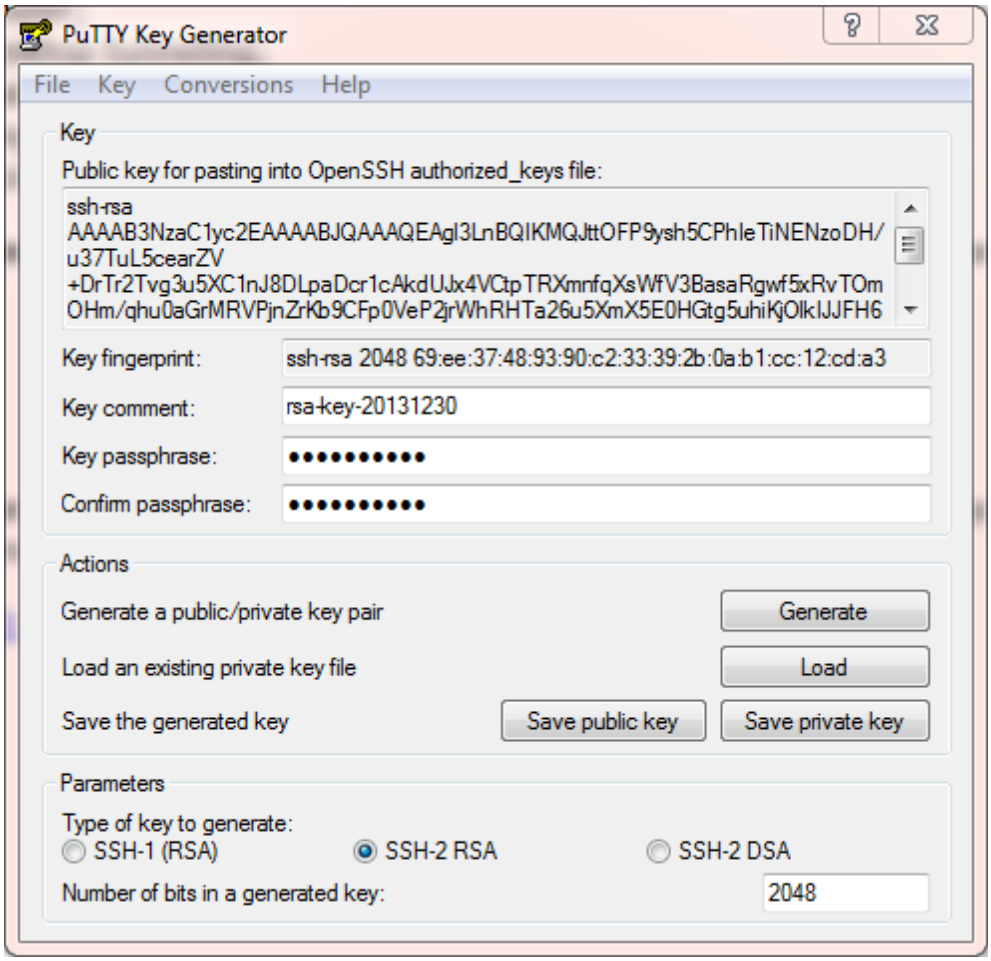
How do you create such a certificate? Here is one way:

The free secure shell program putty has the necessary tools. Download putty from www.putty.org When you install the program you will see several program installed on your computer.



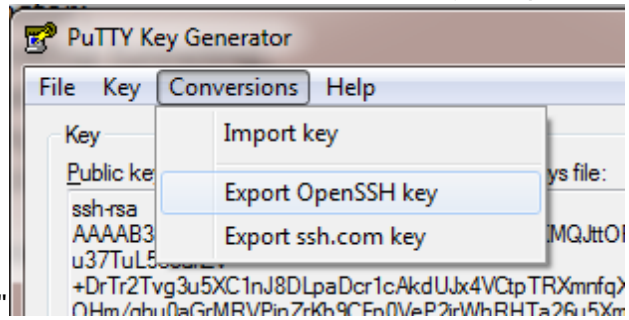
The programs and files that come with putty

One of the programs is puttygen.exe. This program creates the necessary keys. When you start it up, you can generate a key pair.



Creating a public/private key pair with puttygen

You can save the public and private keys separately as .ppk files but that is not what we need. But puttygen has also tool to convert the keys to pem files. The top menu has a tab "Conversions"



Converting the SSH key into a pem certificate

When we click on "Export OptnSSH key" we can then save the key with an .pem ending and that is it.

7.5 Using Encryption

7.5.1 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:

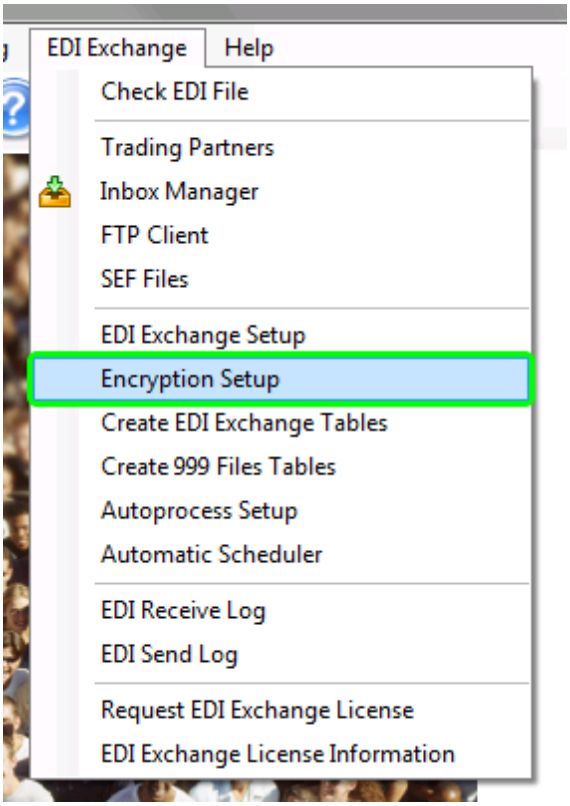
- A certificate authority (CA) that both issues and verifies the digital certificates.
- A registration authority which verifies the identity of users requesting information from the CA.
- A central directory is a secure location to store and index keys.
- A certificate management system.

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 separately install 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.

7.5.2 Setting up Encryption

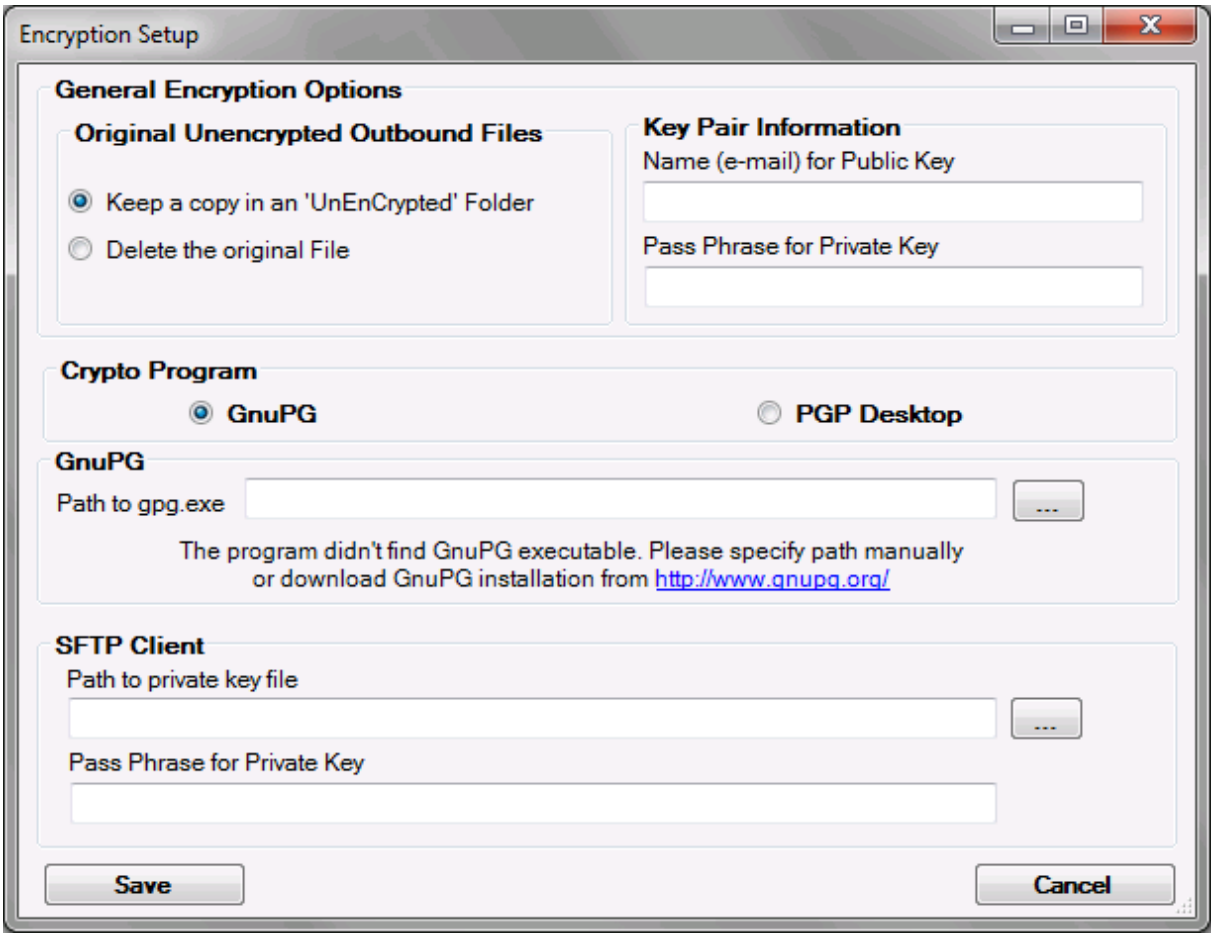
EDI Exchange allows you to set up the encryption for your EDI files. Follow the steps below.

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.

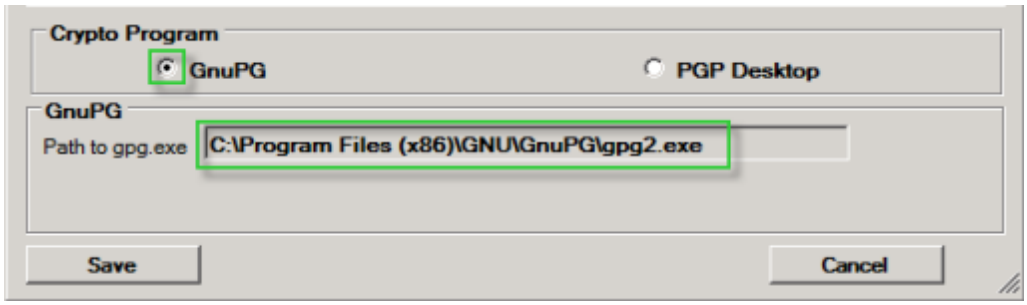
> Note: Once you encrypt a file with the public key of your trading partner, you will not be able to open it again. Only the owner of the private key can decrypt it and read it.

  - **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.

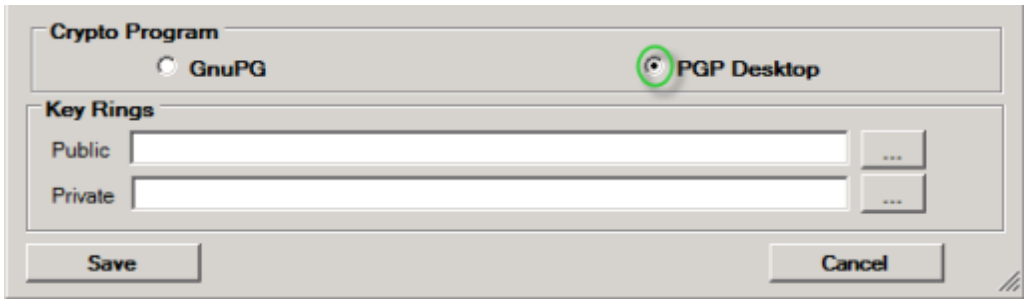
- **Crypto Program**
  - **GnuPG** — Select this option if you have already installed the GnuPG software and want to use it.



The configuration using GnuPG

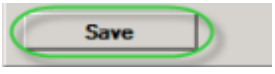
Note: When you select GnuPG, the program checks if the executable **`gpg.exe/gpg2.exe`** is present on your computer. If it is not found, you will have to specify the path manually or install the program first.

  - **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.



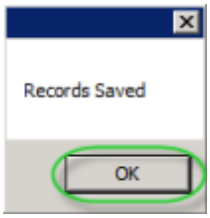
The configuration using PGP Desktop

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

7.5.3 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:

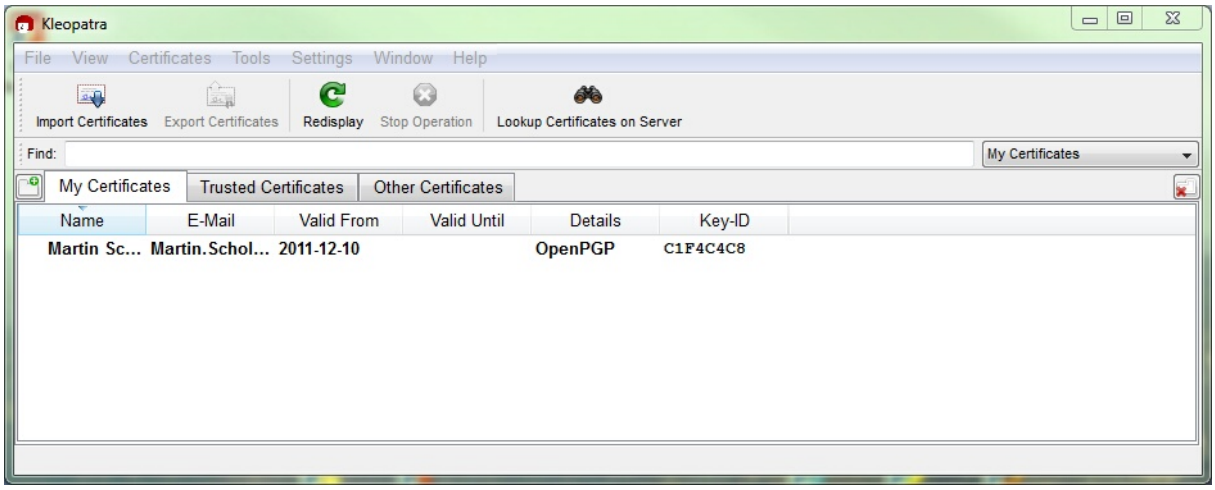
1. Drive Encryption. See System Requirements.
2. Desktop Email Encryption. See System Requirements.
3. Encryption Management Server. See System Requirements.

7.5.4 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.

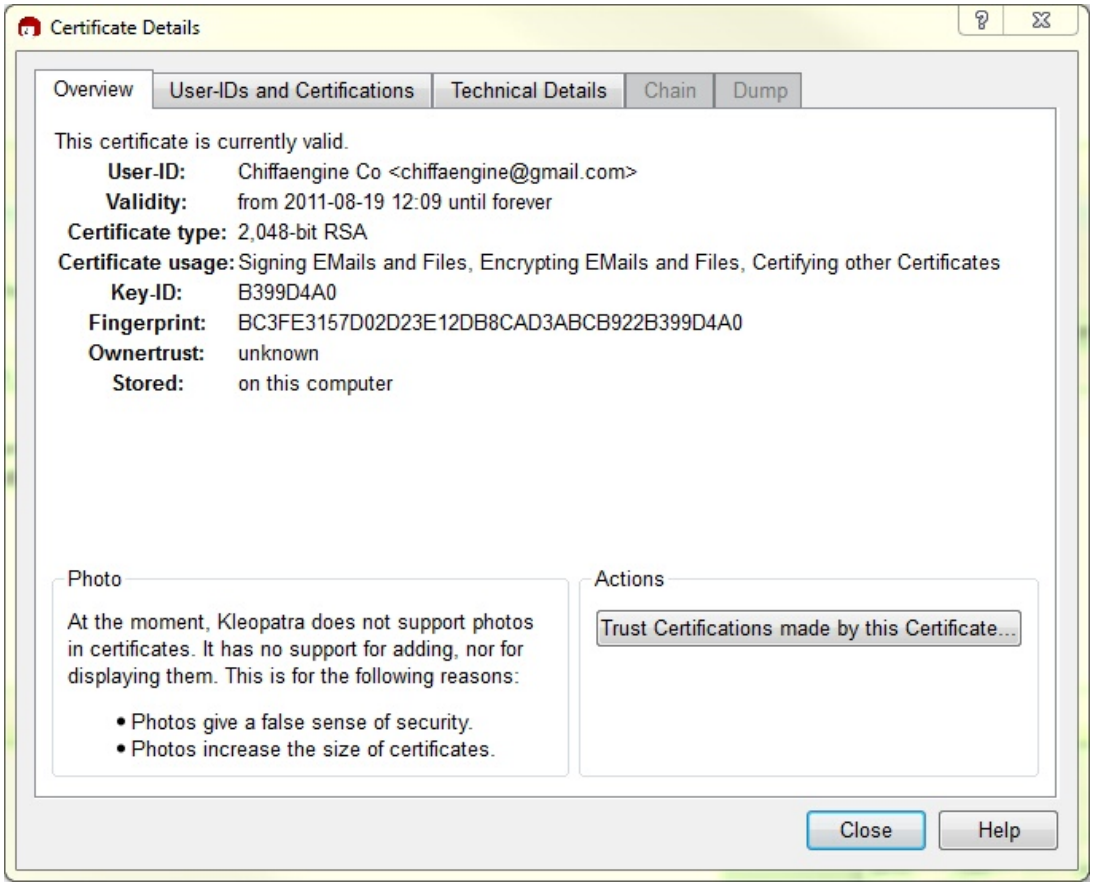
GnuPG is a free software, so it can be freely used, modified and distributed under the terms of the GNU General Public License.

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.



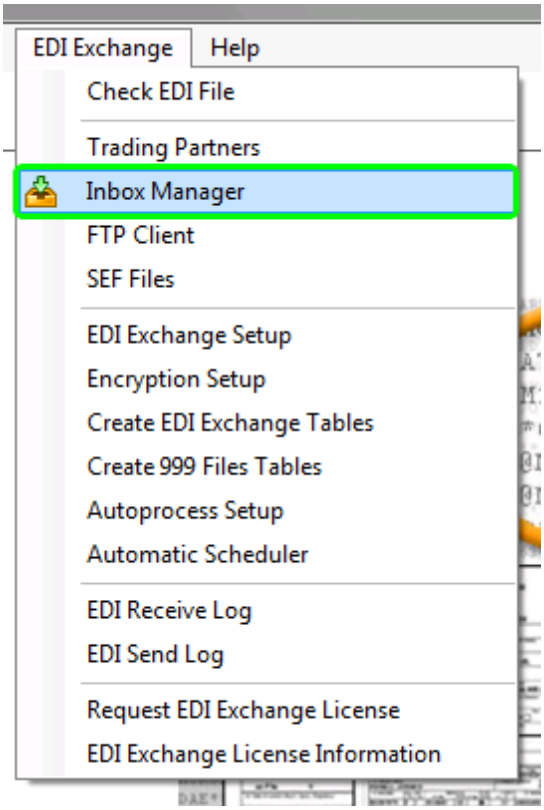
Certificate details with Kleopatra

7.6 Using EDI Exchange Features

7.6.1 Accessing Inbox Manager

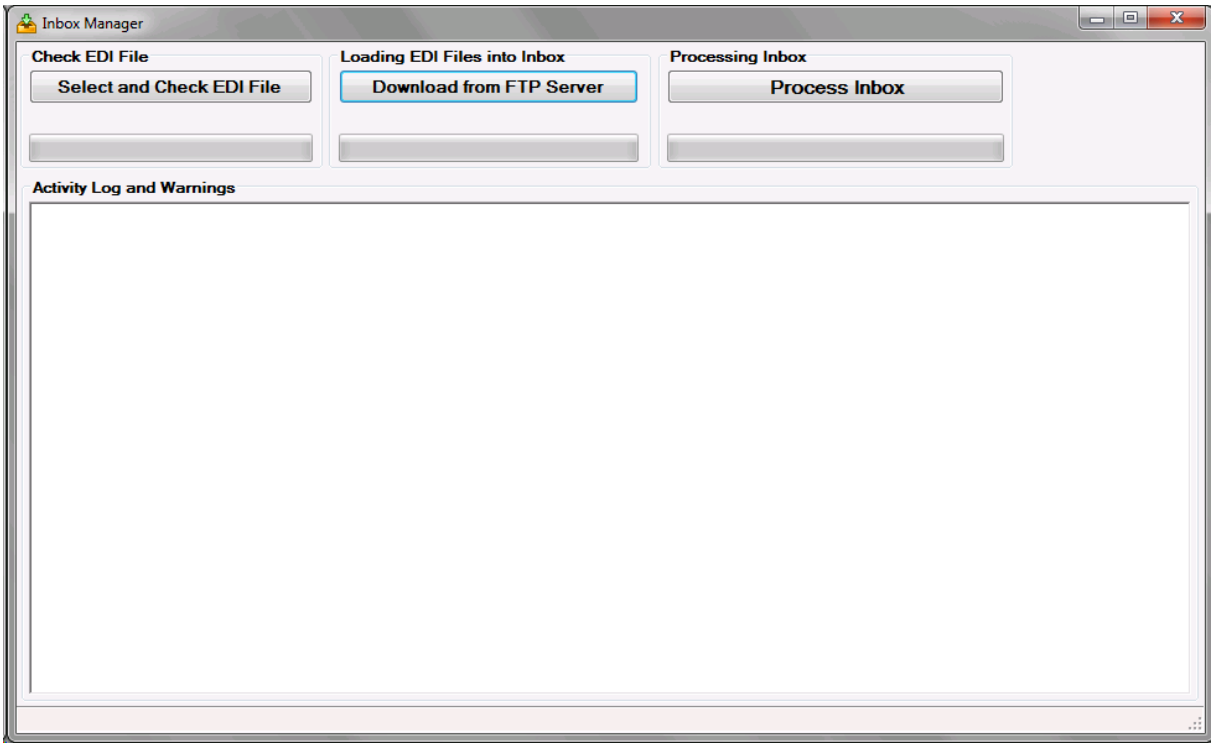
Using the Inbox Manager you can access the most important functions of EDI Exchange. Inbox Manager allows you to download EDI files into the "Inbox" folder and process these files. This screen handles the post-processing of the EDI files, their compliance check and auto-processing options.

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

7.6.2 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.

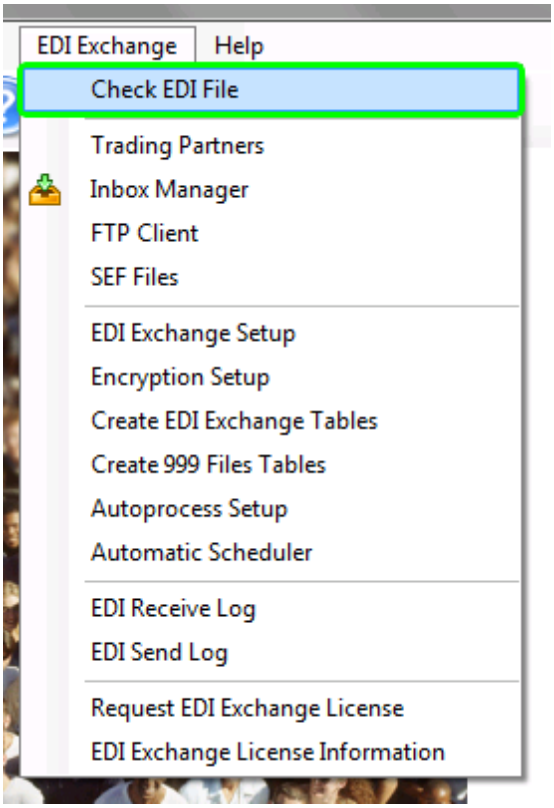
EDI Exchange has a built-in compliance engine that analyzes each incoming and outgoing EDI transaction. Line by line, element by element, error reporting provides a powerful tool to determine the quality of the incoming and outgoing EDI files. All HIPAA file versions are supported. The compliance check 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.

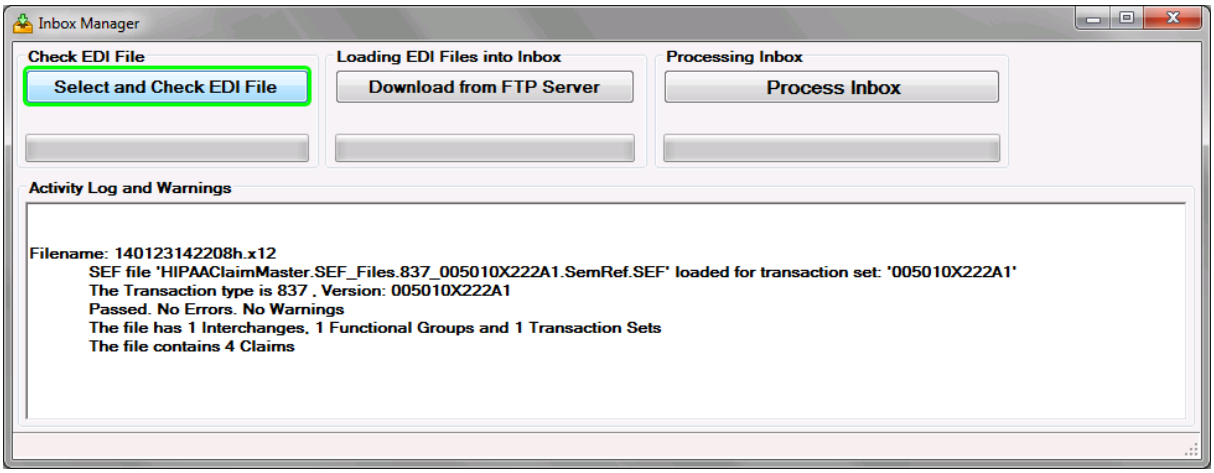
Follow the instructions below to check EDI files for compliance.

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



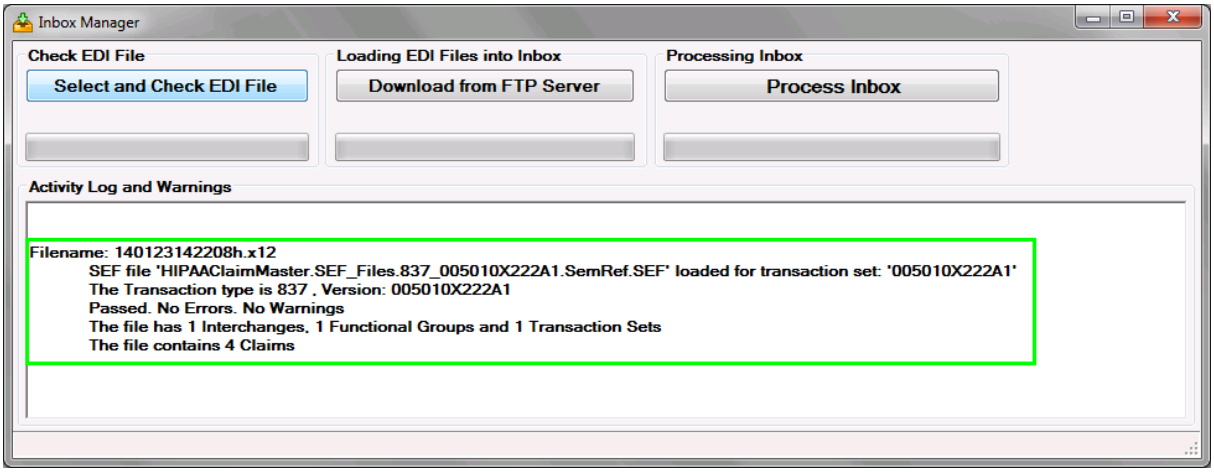
The "Check EDI File" menu item

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.



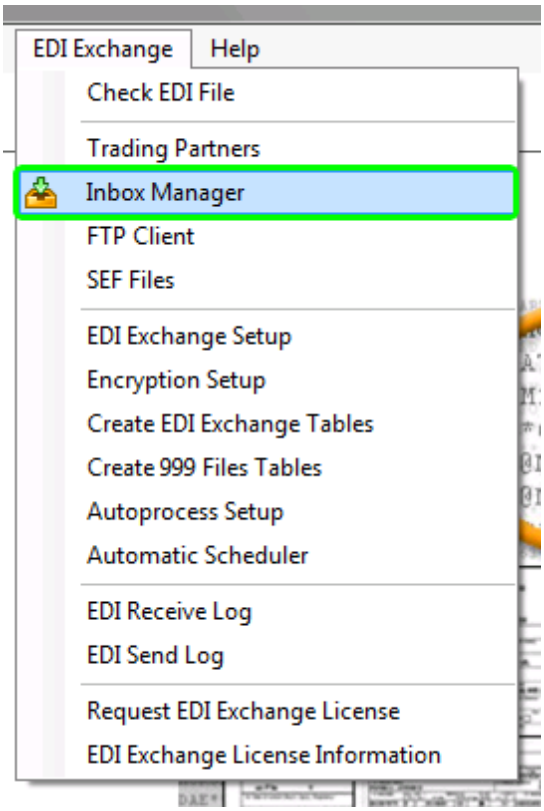
The "Activity Log and Warnings" area displaying log messages

7.6.3 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).

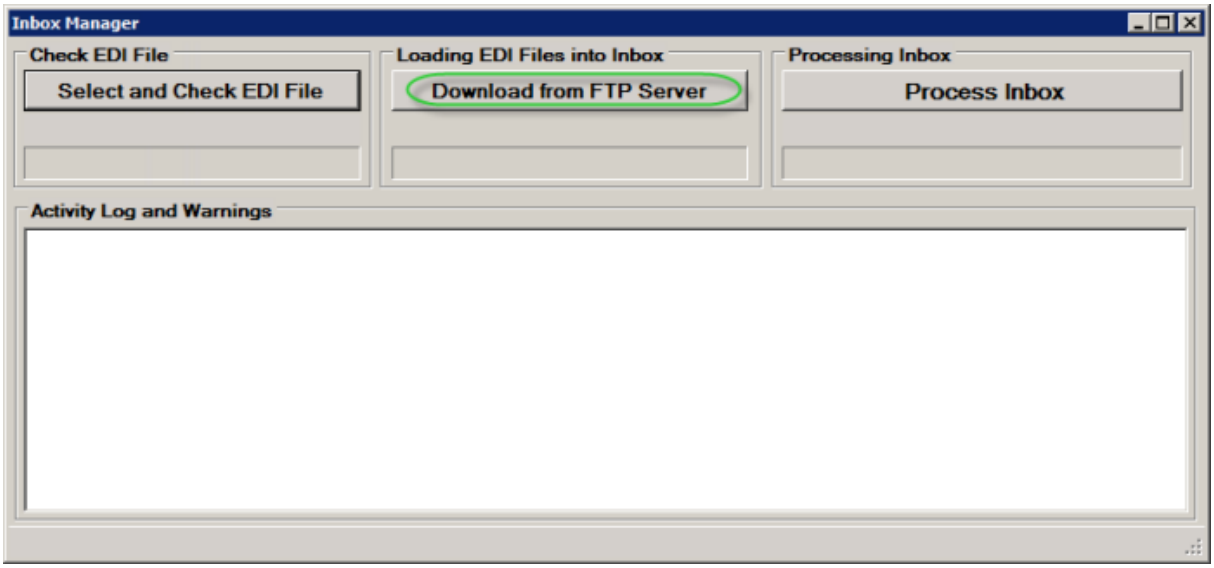
Follow the instructions below to upload EDI files into the "Inbox" folder.

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



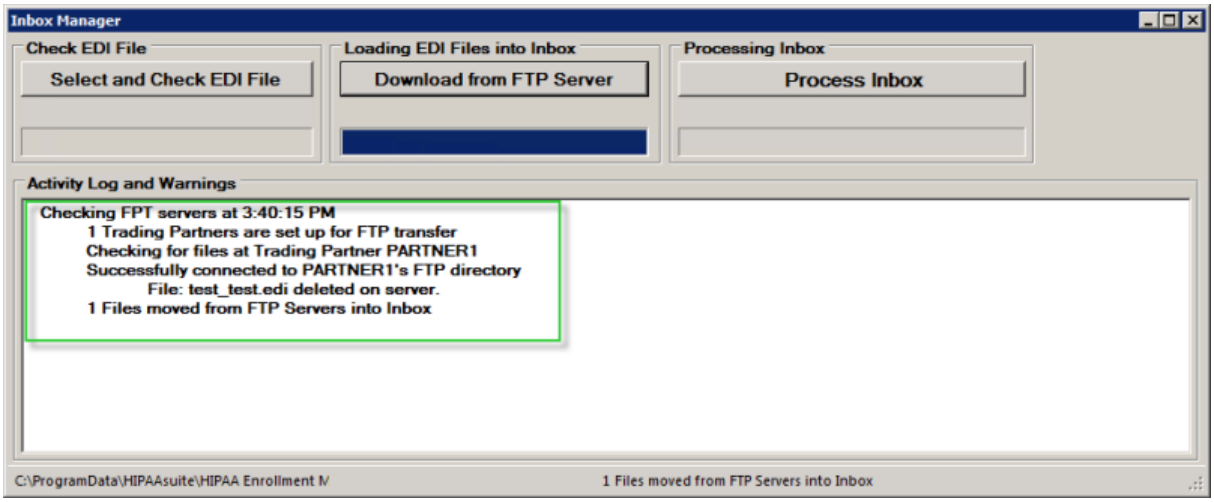
The "Inbox Manager" menu item

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.



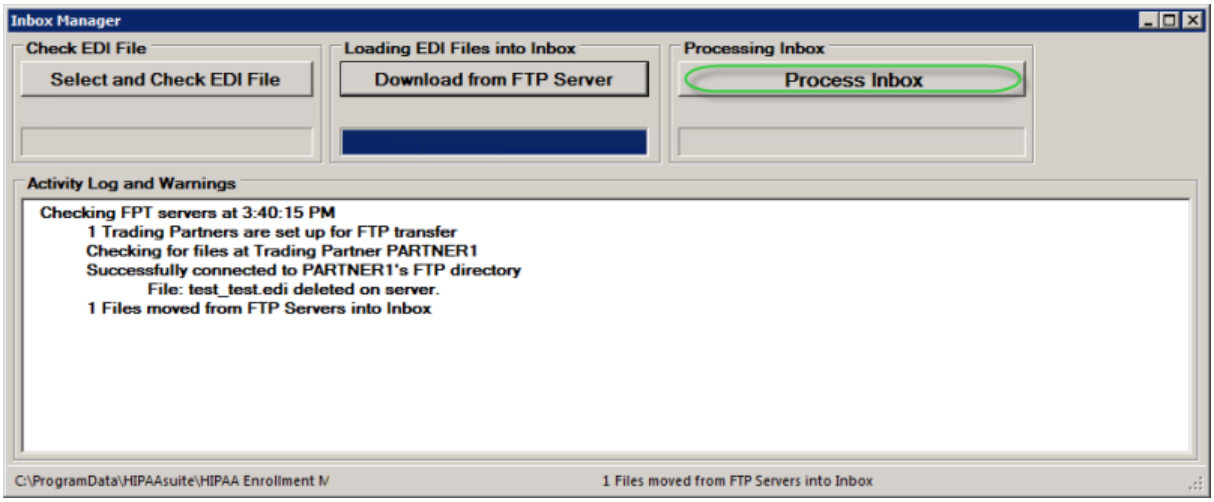
Activity Log and Warnings information

7.6.4 Processing EDI Files

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

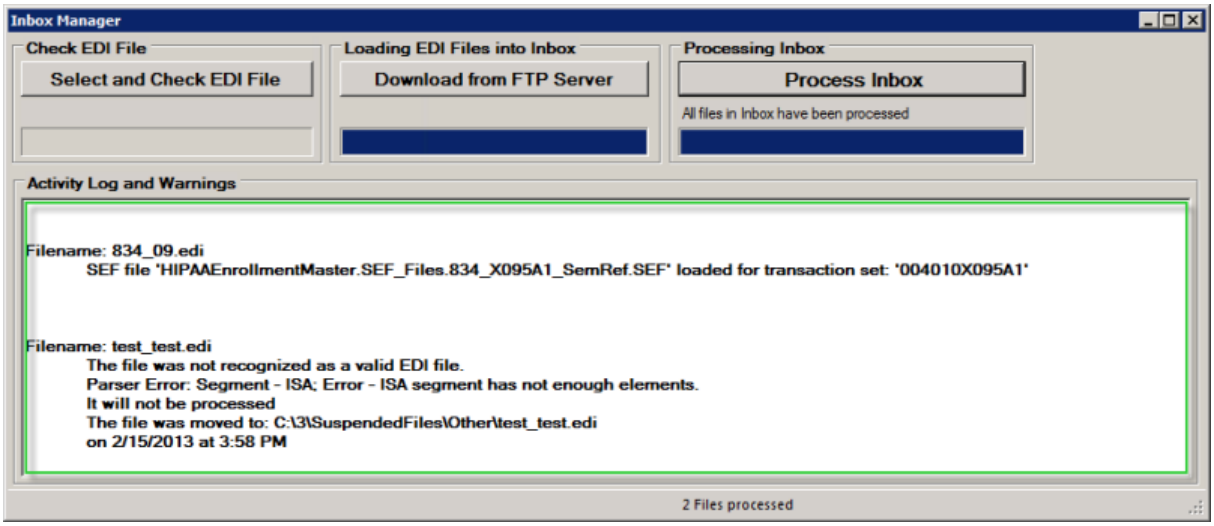
> Note: Once you have saved the auto-processing options (see Defining Auto-Processing Options), the files will not only be analyzed but also processed according to the defined settings. The auto processing enables you to combine and run multiple fulfillment steps together (for example, export, saving,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

1. Once Downloading EDI Files From FTP Server is completed, and no errors are displayed, click on the "Process Inbox" button. This will autoprocess all files present in the EDI inbox directory.



The "Process Inbox" button

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

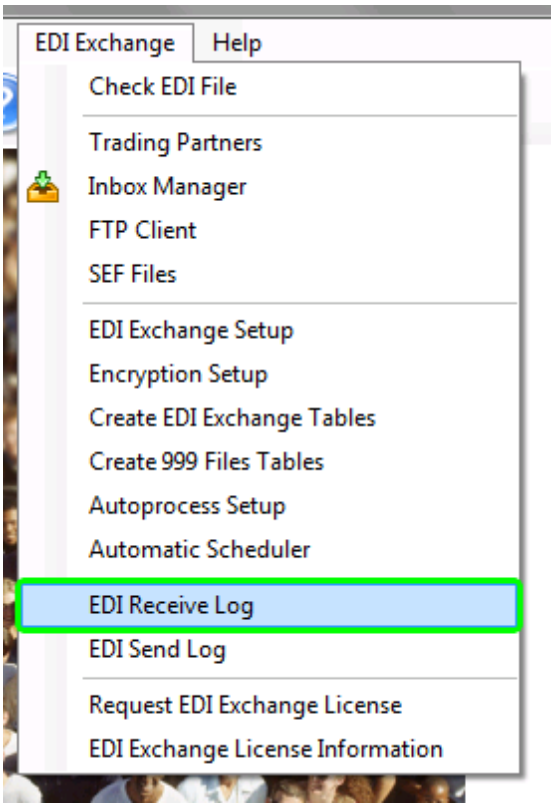


Activity Log and Warnings information

7.6.5 Accessing EDI Receive Log

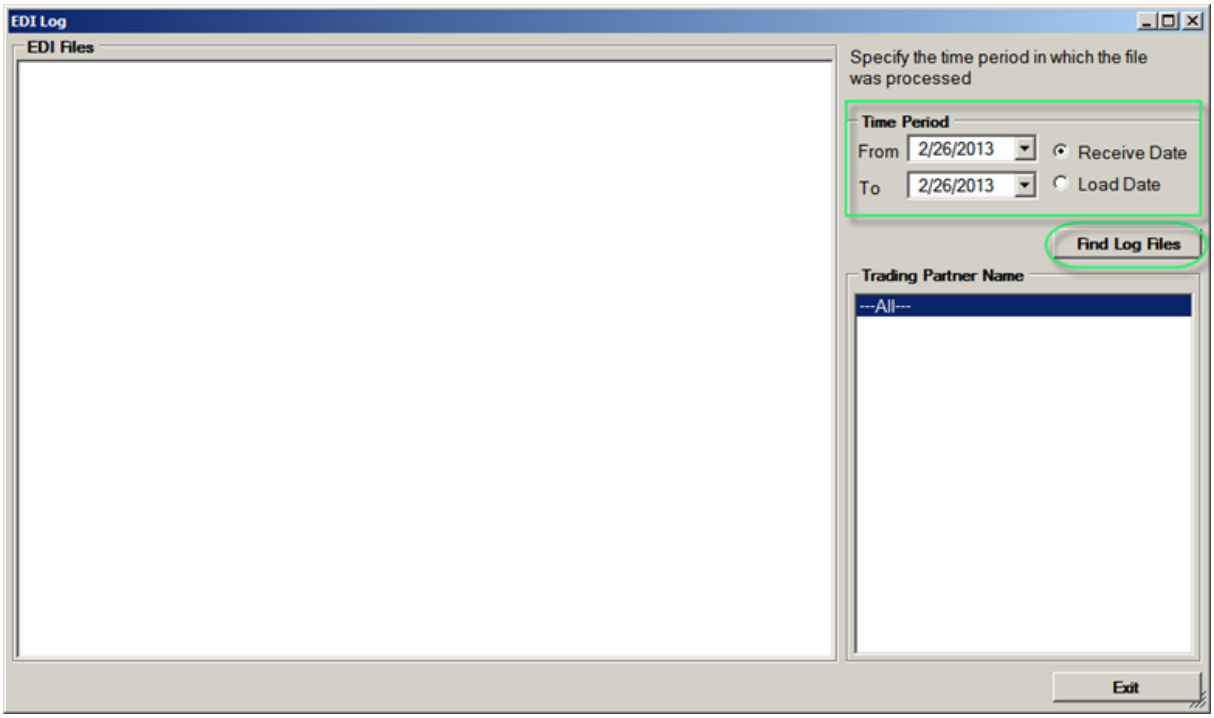
EDI Exchange has a file log. Each processed file creates an entry in the **`Trans_Log`** table. You can access the "EDI Log" window to query this table and see what files came in and how they were processed. You can access the EDI Receive Log once the application has been initialized. Follow the instructions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

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



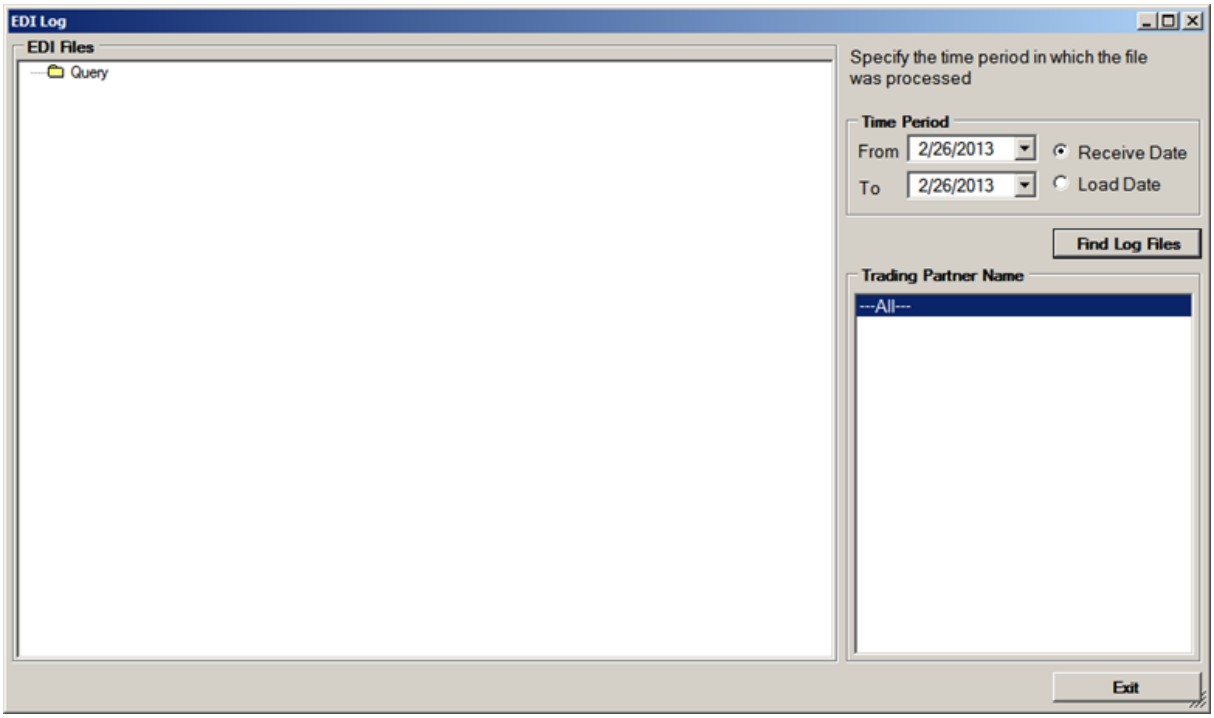
The menu for the EDI Receive Log

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.



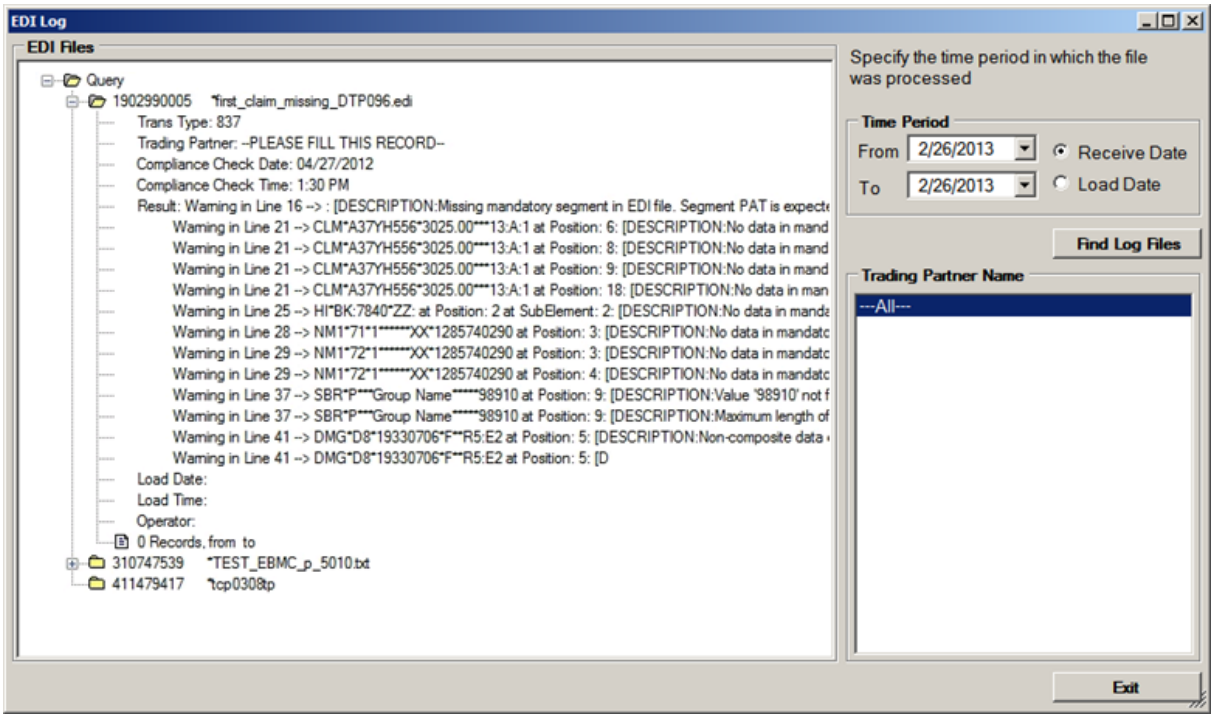
Specifying the time period

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.



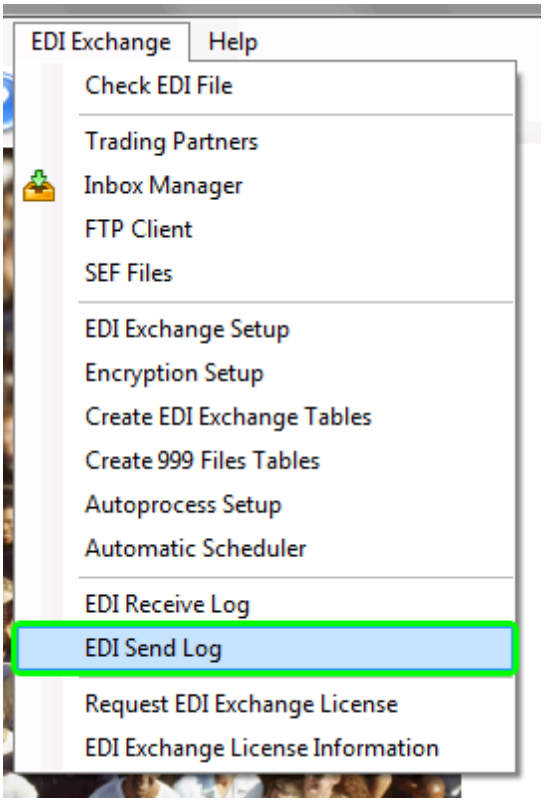
Details of the EDI Receive Log

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

7.6.6 Accessing EDI Send Log

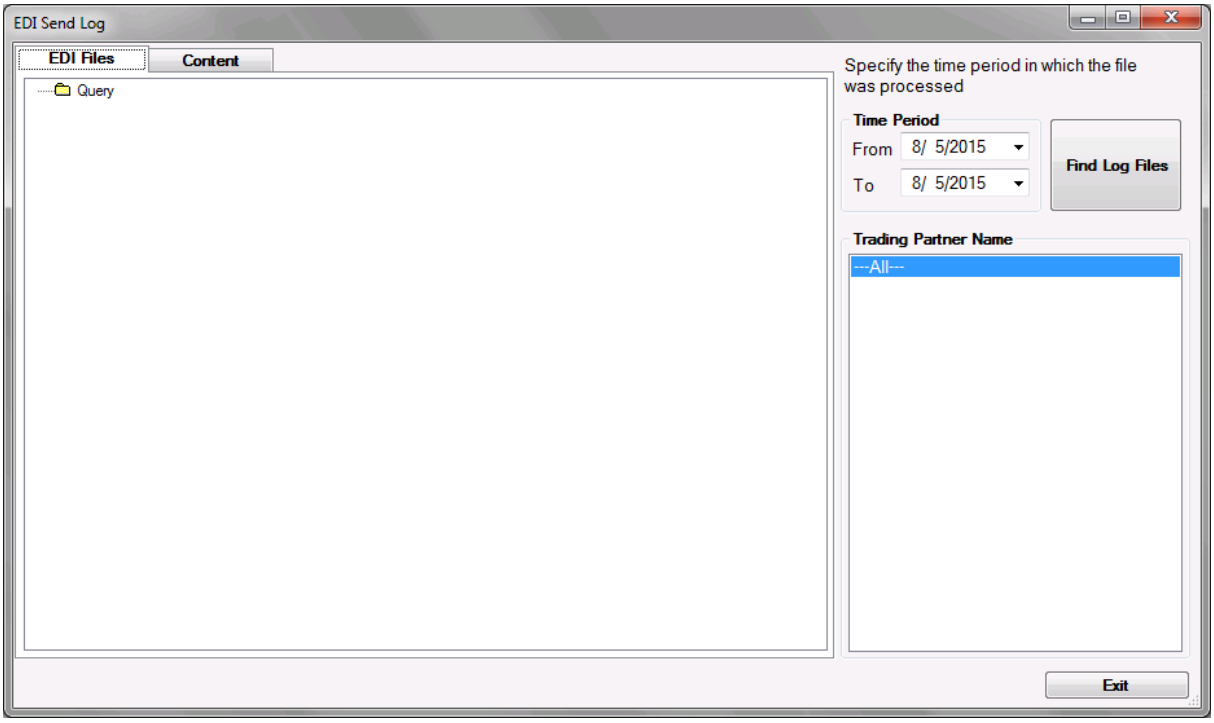
This page contains instructions on how to access the "EDI Send Log" window. It becomes available once EDI Exchange has been initialized.

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.

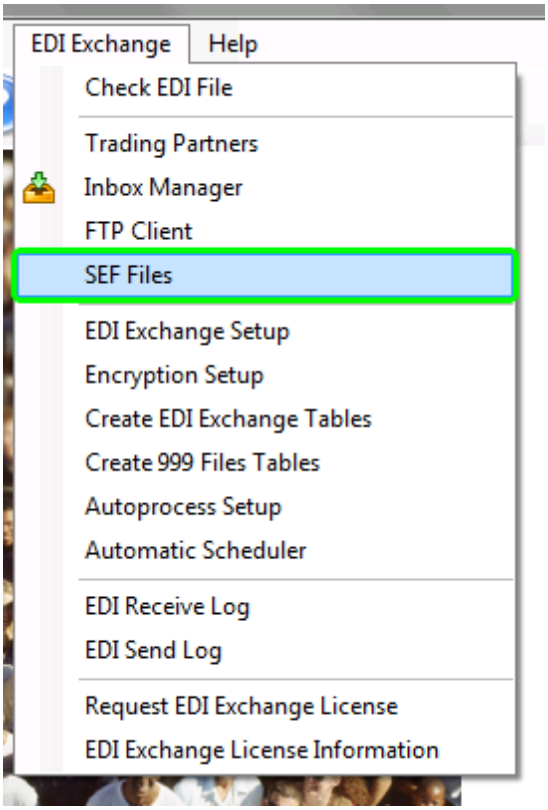
    - **Time Period** — Period of time when the file was processed. Choose one of the available options:
        - **Receive Date**
        - **Load Date**
    - **Trading Partner Name** — Select a trading partner in the list. If you select "---All---", all trading partners will be included.

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

7.6.7 Listing SEF Files

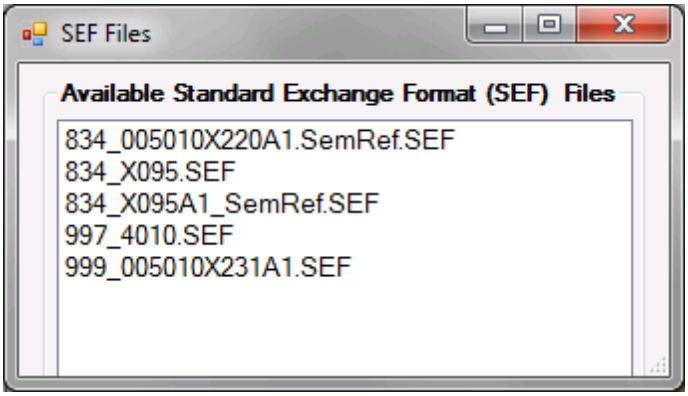
SEF (Standards Exchange Format) files are repositories of standards information that define the format of EDI documents. SEF files are the basis for the compliance check engine that EDI Exchange uses. These files contain all rules of the implementation guide of a transaction. There is a SEF file for 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

8 Automating File Processing

8.1 Using Command Line Arguments

The HIPAA Claim Status Responder can accept command line arguments. The following is

the list of the command line arguments; they must be separated by commas.

1. The first command line argument is the **filename** or the **directory path**.

2. The second argument contains the processing options. The following argument may be used:

> X - Export to database.
>
> Example: To export a Claim Status Request to the database:

```
C:\Program Files\HIPAAsuite\HIPAA Claim Status Responder>HIPAAClaimStatusRespond
er.exe D:\EDI\276_2.edi
```

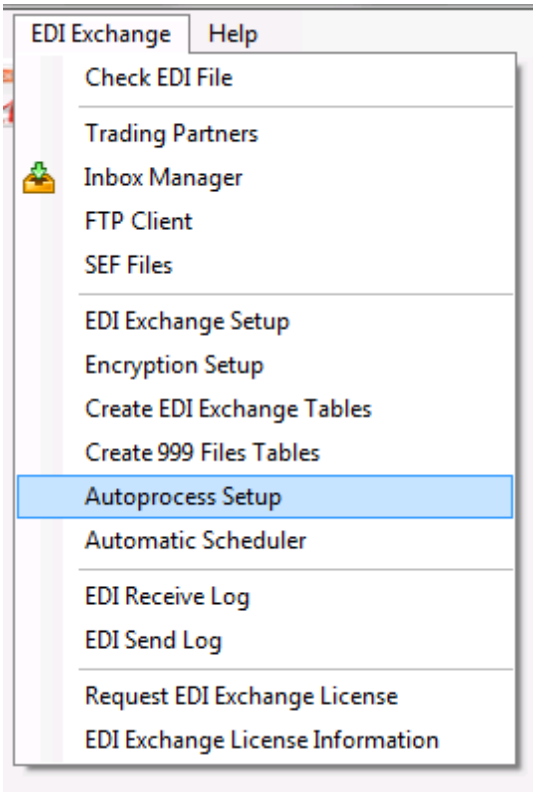
8.2 Autoprocessing with the EDI Exchange Module

Autoprocessing the Inbox

When processing from the command line with the EDI Exchange module enabled, the argument you need is "Auto". The directory used to look for new files and the processing options are defined in the setup screens for EDI Exchange. No further arguments are needed.

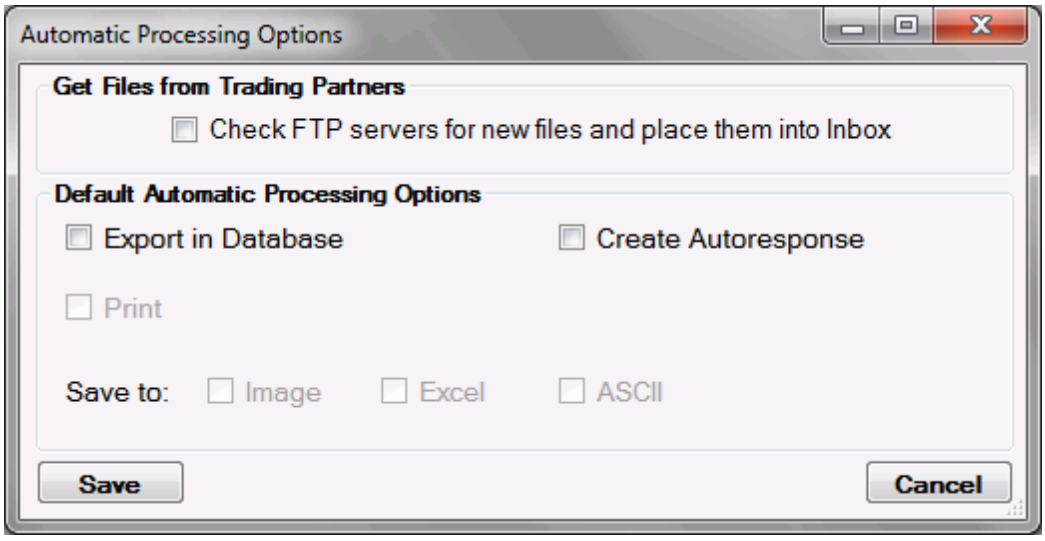
```
C:\Program Files\HIPAAsuite\HIPAA Claim Status Responder>HIPAAClaimStatusRespond
er.exe auto
```

To setup autoprocess options, go to EDI Exchange ▸ Autoprocess Setup:



Autoprocess Setup option in EDI Exchange menu

Any options selected for autoprocessing will carry over to the command line.



EDI Exchange Automatic Processing options

Autoprocessing a Single File

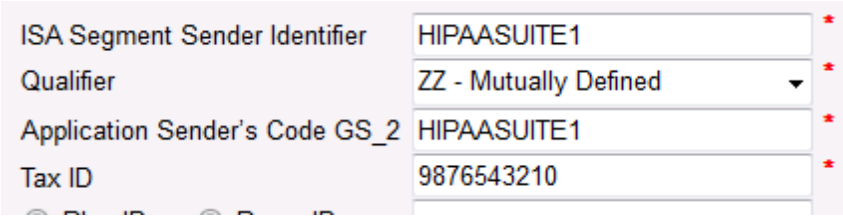
To run a single file through the autoprocessor, add the full filename as second argument to your command.

```
C:\Program Files\HIPAAsuite\HIPAA Claim Status Responder>HIPAAClaimStatusRespond
er.exe auto,D:\EDI\276_2.edi
```

Command to autoprocess a single file.

8.3 Changing the Default Company

The default company can be changed using command line arguments, affecting the ISA and GS sender ID segments.

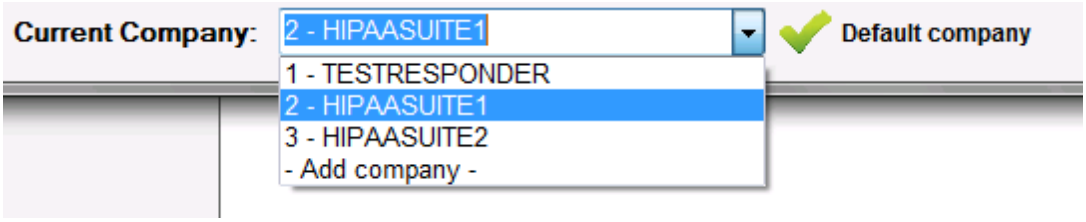


Sender ID segments in Company Setup

To change the default company, a single argument is needed. "**Setcompany**" followed by the company ID of the company you wish to set.

"setcompany <ID>"

The Company's ID in this case is not its EDI identifier, but the value of the ID row in the COMPANY_SETUP table. It can also be found in the Company Setup window:



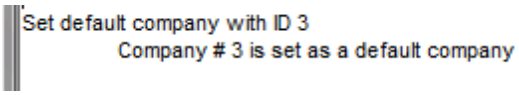
Company selection in Company Setup

Example

The command argument **setcompany 3**

```
C:\Program Files\HIPAAsuite\HIPAA Claim Status Responder>HIPAAClaimStatusRespond
er.exe setcompany 3
```

will set the default company to ID = 3, which is HIPAASUITE2 in the example picture above. The log entry for this command will be



Excerpt from log. Default company changed.

9 Automatic Responses

9.1 Introduction

The HIPAA Claim Status Responder can autoprocess Claim Status Requests and Functional Acknowledgments without the need to launch the program User Interface. To do this, the HIPAA Claim Status Responder can accept command line arguments. The following is a list of the command line arguments; they must be separated by commas.

1. First Argument - mode
    a. "auto" will process a 276 file. If no other arguments are included, all 276 files in the EDI Exchange Inbox directory will be processed. Any other files in the Inbox directory will be ignored. If the filepath is included as a second argument, that file will be processed individually.
    b. "soap" will process a specific 276 or 999 file. A second and third argument containing the file directory (including filename) and PayloadID are necessary.

2. Second Argument – full filepath (auto, optional / soap)
    a. Not necessary for "auto" process mode. If included will only autoprocess that file.
    b. Necessary for "soap" mode.

3. Third Argument – PayloadID (soap only)
    a. SOAP/MIME PayloadID tied to request/response transaction. Necessary to identify request, response, and acknowledgements associated with a single transaction.

4. Fourth Argument – FileType (soap only, optional)
    a. Used to differentiate between a request file and an acknowledgment file. If omitted, file will be processed as a 276 request.

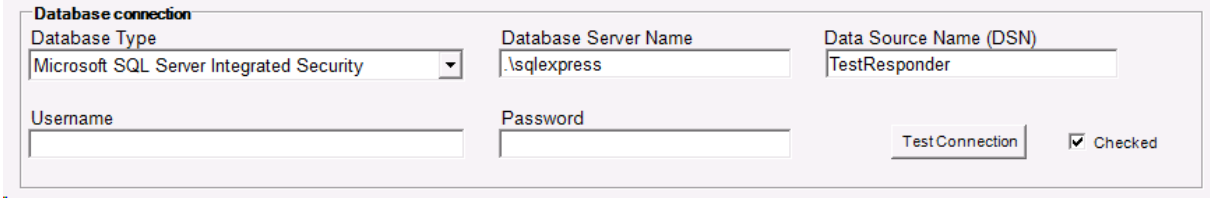
The HIPAA RealTime Server can also be used to run the Claim Status Responder without the need for user interaction. With the addition of HIPAA Claim Master, it can accept 276 EDI Claim Status Request

transactions, draw data from claims stored in the Claim Master, store the relevant Claim Status request/response(s) in the HIPAA Claim Status Responder, and send a 277 Claim Status Response in under 10 seconds.

9.2 RealTime Server

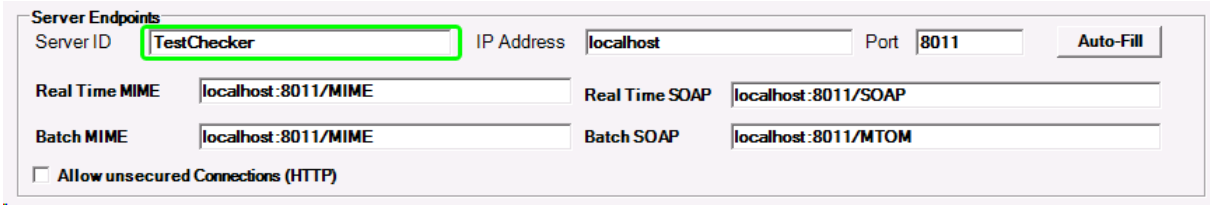
The HIPAA RealTime Server can be used in conjunction with any HIPAAsuite Responder application to provide MIME/SOAP functionality as described in CAQH CORE Phase II. This means the Claim Status Responder will be CAQH CORE compliant, being able to answer 276 Real-Time and Batch mode messages in both SOAP and MIME formats. The source data for a claim's status can be the HIPAA Claim Master's tables or a separate set of claim tables.

To respond to SOAP or MIME 276 Claim Status requests, the HIPAA RealTime Server must be configured to use the same database as the HIPAA ClaimStatus Responder. This serves to provide the RealTime Server with information such as the Trading Partner's ID and credentials. If the incoming SOAP/MIME request's SenderID is not the Trading Partner ID associated with a username/password, the message will be rejected. The following is a part of the RealTime Server's configuration window:



The Database used by the RealTime Server must be the same used in the ClaimStatus Responder.

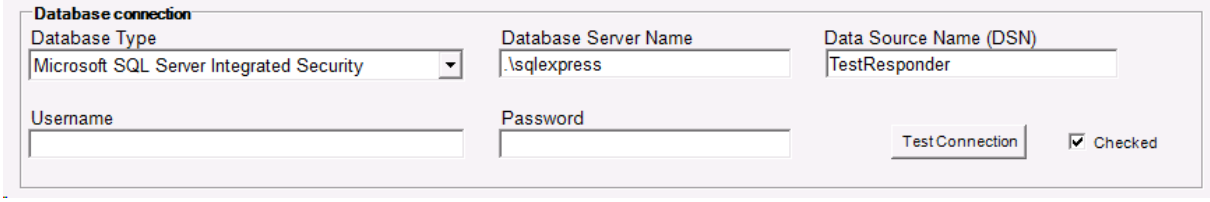
The name specified in the HIPAA RealTime Server's Server ID field is the name that will be used to identify you or your organization in the SOAP and MIME Sender/Receiver ID fields.



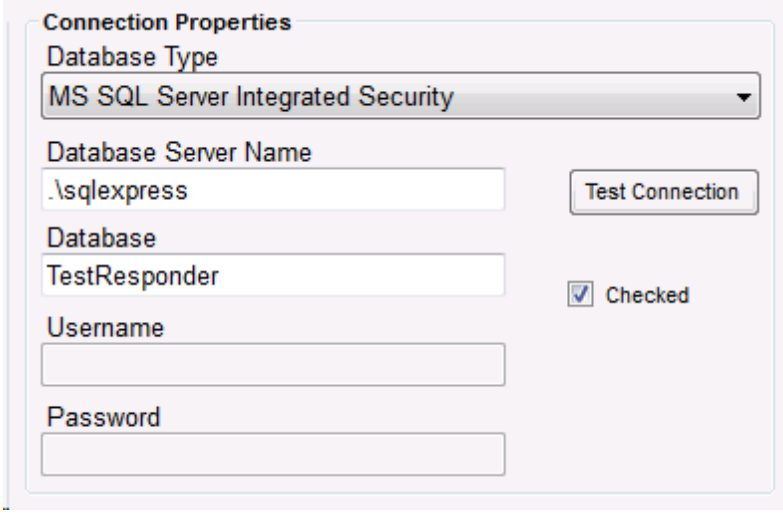
This will be your identifier when sending/receiving SOAP or MIME messages.

9.3 Server Setup

In order for the HIPAA RealTime Server to know what to do with a particular incoming 276 request, an outgoing 277 response, or a 999 acknowledgment, it is necessary to use the same database as the HIPAA Claim Status Responder.

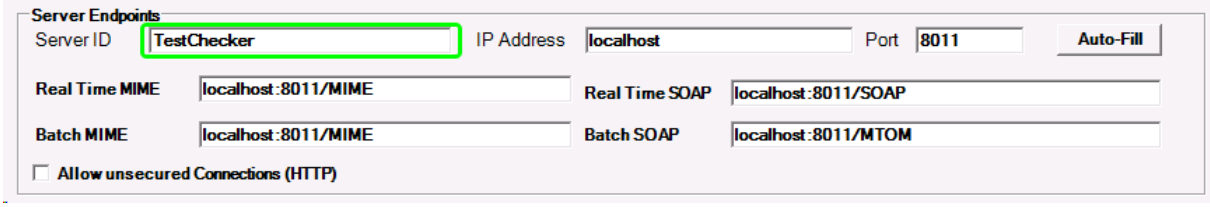


RealTime Server Database configuration.



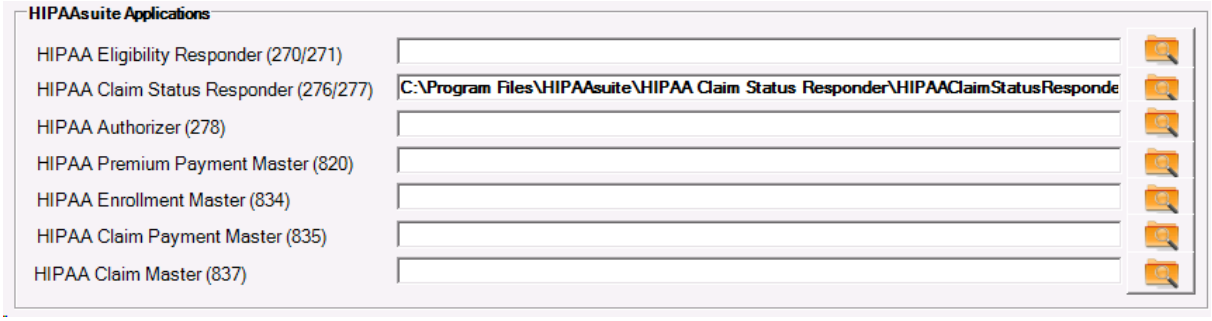
ClaimStatus Responder Database Configuration.

The server should also be using the desired Trading Partner ID to identify you or your organization as the recipient when processing incoming messages and as a sender when responding to messages.



Part of RealTime Server configuration. Emphasis on ServerID.

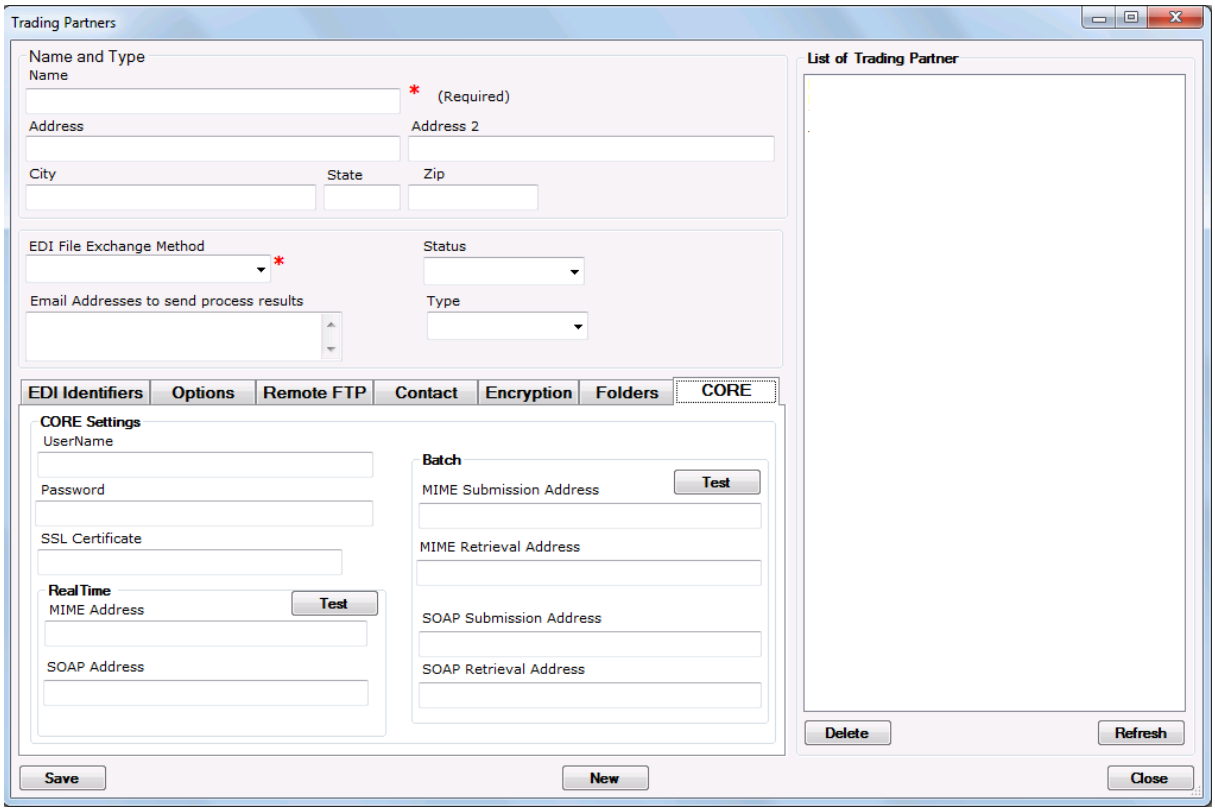
Finally, the full HIPAA ClaimStatus Responder path must be included in the *HIPAAsuite Applications* section of the RealTime Server setup screen. If the default install location was used, the HIPAA Claim Status Responder's path will be *C:\Program Files\HIPAAsuite\HIPAA Claim Status Responder\HIPAAClaimStatusResponder.exe* if the x64 bit version was installed. For the x32 bit version *C:\Program Files (x86)\HIPAASuite\HIPAA Claim Status Responder\HIPAAClaimStatusResponder.exe* will be the default directory.



HIPAA ClaimStatus Responder install directory.

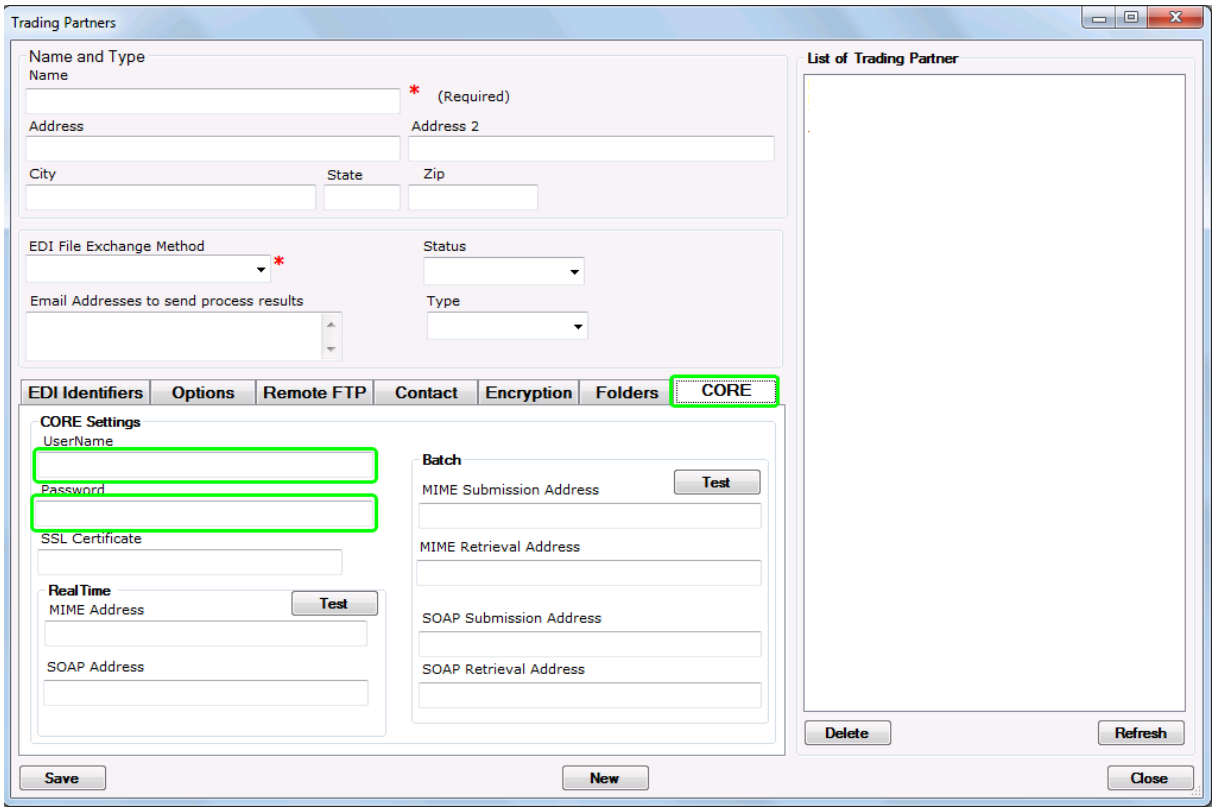
Trading Partners

To set up a Trading Partner to use your HIPAA RealTime Server, both the HIPAA Claim Status Responder and HIPAA RealTime Server must be using the same database. In the Claim Status Responder's Trading Partner setup screen, select the desired Trading Partner or make a new one.



New Trading Partner.

Having a Trading Partner selected, the CORE tab can be populated with the correct values. Necessary fields to respond to a Trading Partner are a Username and Password. These are set in the ClaimStatus Responder and read by the RealTime Server and serve as the Trading Partner's MIME/SOAP username key authentication credentials.



Username/Password fields are used by the RealTime Server to authenticate Trading Partners.

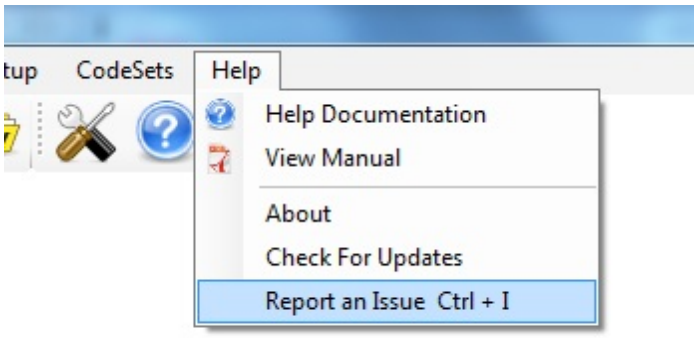
This is all the setup necessary on our end. Inform the Trading Partner of their username key credentials and your RealTime Server's addressing and your Trading Partner will be able to request and receive Claim Status information from your server.

10 Issue Tracking

10.1 Reporting an Issue

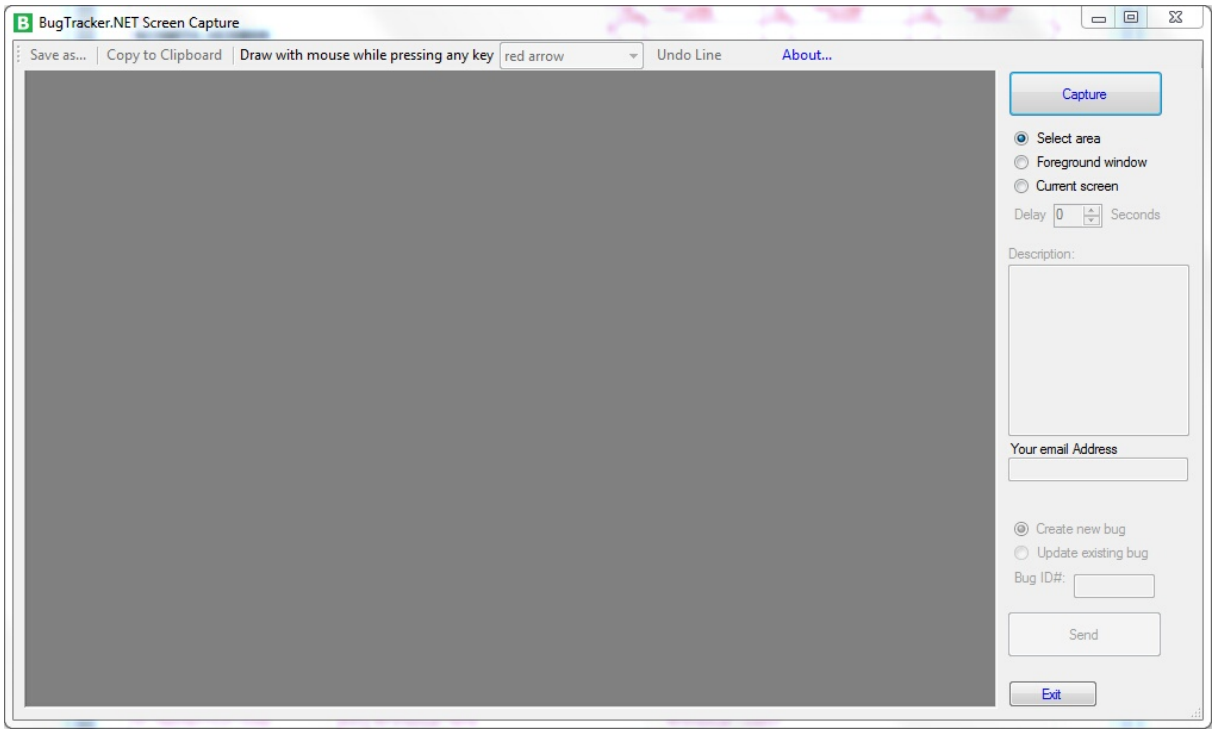
HIPAAsuite likes to make bug fixes fast and transparent. For this purpose we include a Bug tracker with the HIPAA Claim Status Responder. btnet, Bugtracker in ASP.Net is an open source project. HIPAAsuite implemented Bugtracker.Net in all its products to track bugs and enhancements. One of the reasons we liked btnet was the screen capture capabilities. We adapted and included this facility

You can reach the Issue Tracker under the Help menu



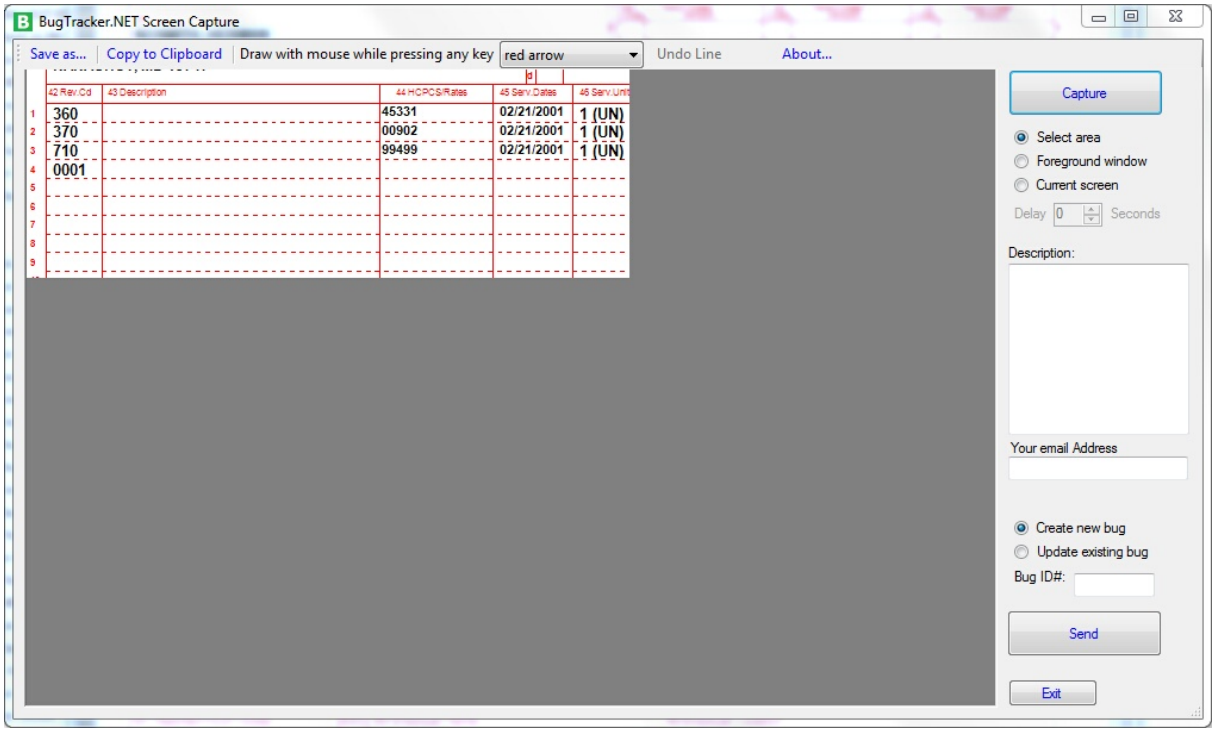
The menu for the issue tracker

Please remember the shortcut Ctrl + I to call the Issue tracker. Some screens do not give you access to the menu while they are open, but the key combination **Crtl + I** will call up the issue tracker report screen.



The BugTracker.Net screen capture facility

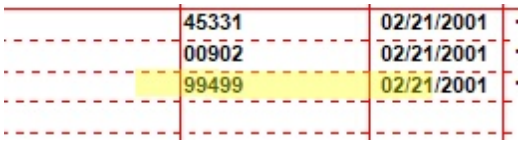
If you click on 'Capture' you can snap a picture of your screen



With a section from the underlying screen

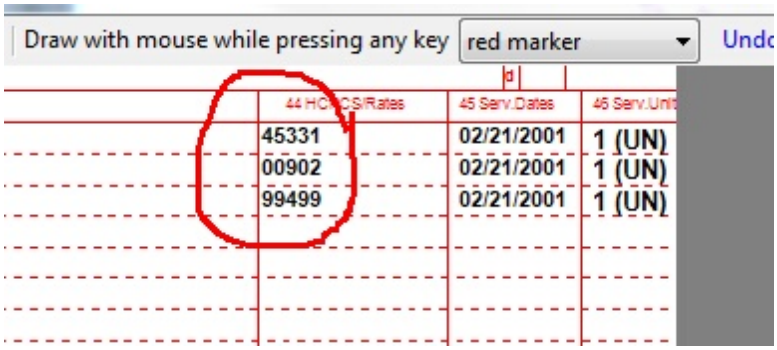
Enter as much information into the description as possible. You can enhance your screen shot with drawings. By pressing any key and holding down the mouse while over the canvas, you either highlight in yellow, free draw in red or make red arrows:

You can high light sections



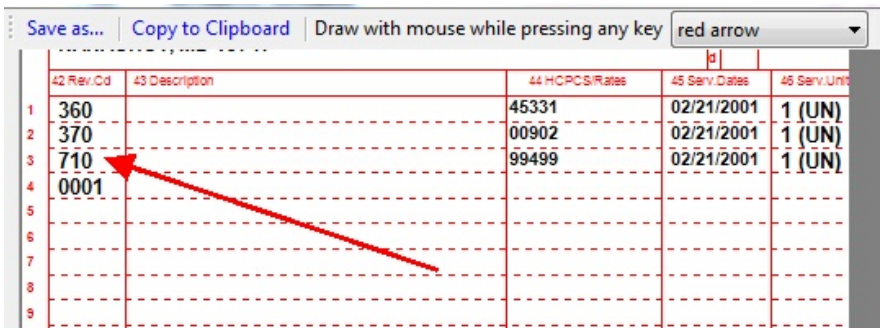
High lighting a section

You can draw circles



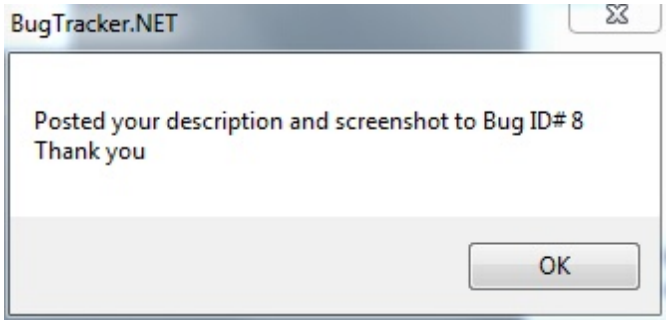
Circling a section

You can point arrows to pinpoint your concerns



Drawing an arrow

Now please enter your email address so that we can get in contact with you and indicate whether this is a new bug or a follow up on an existing issue. Then click on 'Send'



Acknowledgement of Issue submission

Now this bug has been submitted, we will be notified by email and you will get updates on the issue.

Back Cover