The HIPAA Claim Status Checker

Table of Contents

1 Introduction

1.1 About the HIPAA Claim Status Checker

The HIPAA Claim Status Checker is a program to electronically inquire about the status of health insurance claims and designed to be used by providers of health care services.

Providers usually send either directly or through clearing houses the bills for services that they rendered to the carrier of the insurance policy since the vast majority of their patients are insured. Most states have prompt payment laws urging the carriers of payers as they are called, to pay outstanding claims within 30 days. But often the payment is delayed through incomplete or missing information or other circumstances that pend the payment. Providers up to now had to use personnel who spend most of the day being on-hold trying to talk to a customer service representative of the payer trying to find out why a certain claim has not been paid. This time consuming and often frustrating task leads often to unpaid bills and write-offs, severely cutting into the profit of providers apart from paying the billing specialists on staff. A whole industry arose around unpaid claims in that there are companies buying unpaid and outstanding claims at a discount to pursue the payment and relieve the provider of the tedious task to collect the money.

The HIPAA act of 1996 was the first attempt to create nationwide rules to enact administrative simplification and make the process of information exchange between providers and payers more efficient by employing electronic data exchange (EDI). This technology was already used in the banking and long distance phone call industry to tremendous advantage. Whenever you go to an ATM machine to withdraw money there will be electronic transactions from the machine to the owner of the machine and then to the issuer of the card. Within a few seconds nowadays one get cash in practically any place on earth. The government through its National Bureau of Standards is the guardian of the rules and details of the different EDI transactions for each involved industry.

The original HIPAA act described the 276 as the transaction set for the claim status request and the 277 for the claim status response. But it did not specify the necessary infra structure such as transport protocols and even now, nearly 20 years after the HIPAA act there is only spotty usage of these protocols. Things changed with the Affordable Care Act (ACA or Obamacare) which adopted the rules developed by the Coalition for Affordable Quality Healthcare (CAQH) which is a consortium of healthcare industry providers and insurers. They devised and prescribed mechanisms to transfer claim status information in real-time between two computers.These new CORE standards will greatly enhance the efficiency of billing and getting paid once they are widely adopted.

The HIPAA Claim Status Checker allows to create electronic claim status requests, to send them to the payer and to receive and interpret the response.

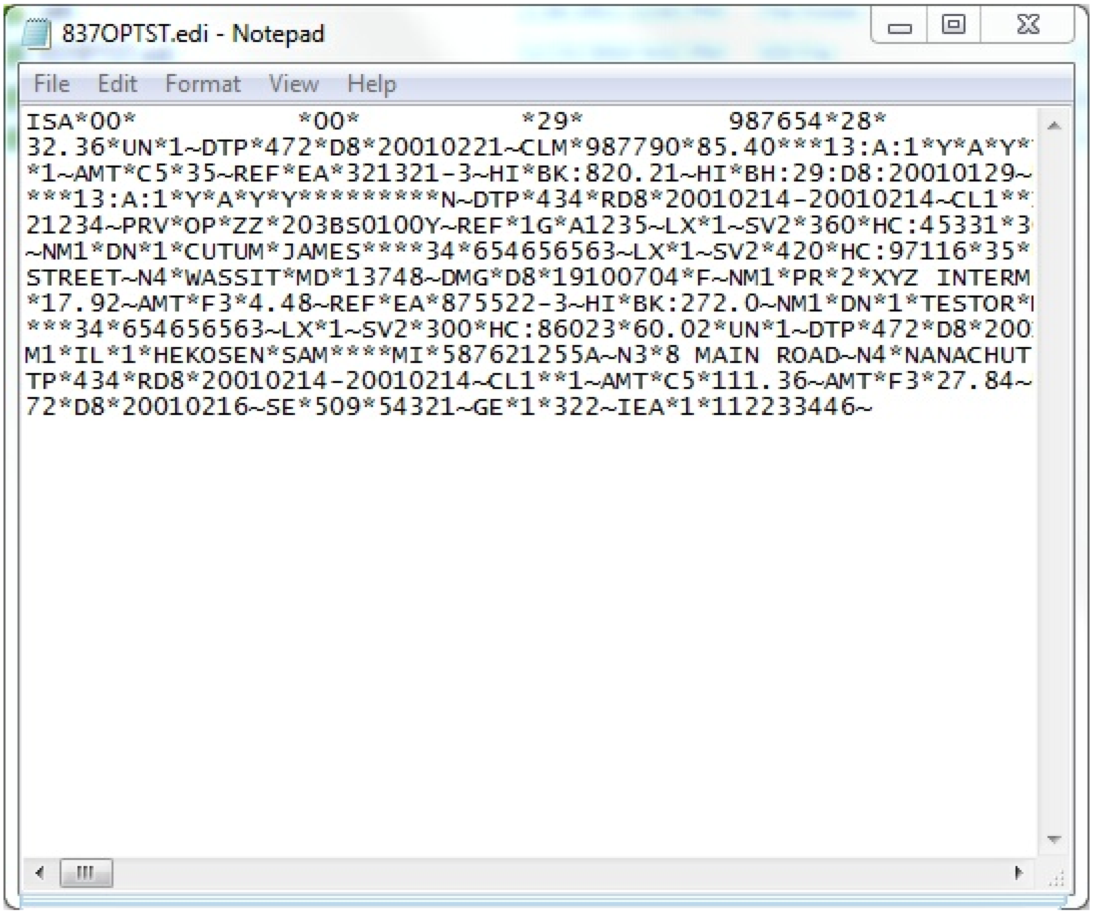
1.2 What is EDI

Electronic Data Interchange (EDI) is standardized in the USA and behind much of the economic success of this country. From ATM transactions over phone bills between carriers to Wal-Mart's supply chain, commerce relies on standardized electronic data interchange. Its rules and standards are administered and maintained by the National Bureau of Standards within the X12 working group.

The HIPAA act mandates eligibility transactions need to be transmitted in a standardized way. The 270 and 271 transaction sets deal with the eligibility to medical insurance benefits. Typically a provider would send out a 270 request for eligibility benefits and a payer either directly or through a clearing house reads this request messages and sends back a 271 eligibility response message listing all the available benefits or the specific subset that what questioned. The Affordable Care Act (Obama Care) mandates that payers provide real time responses to such requests.

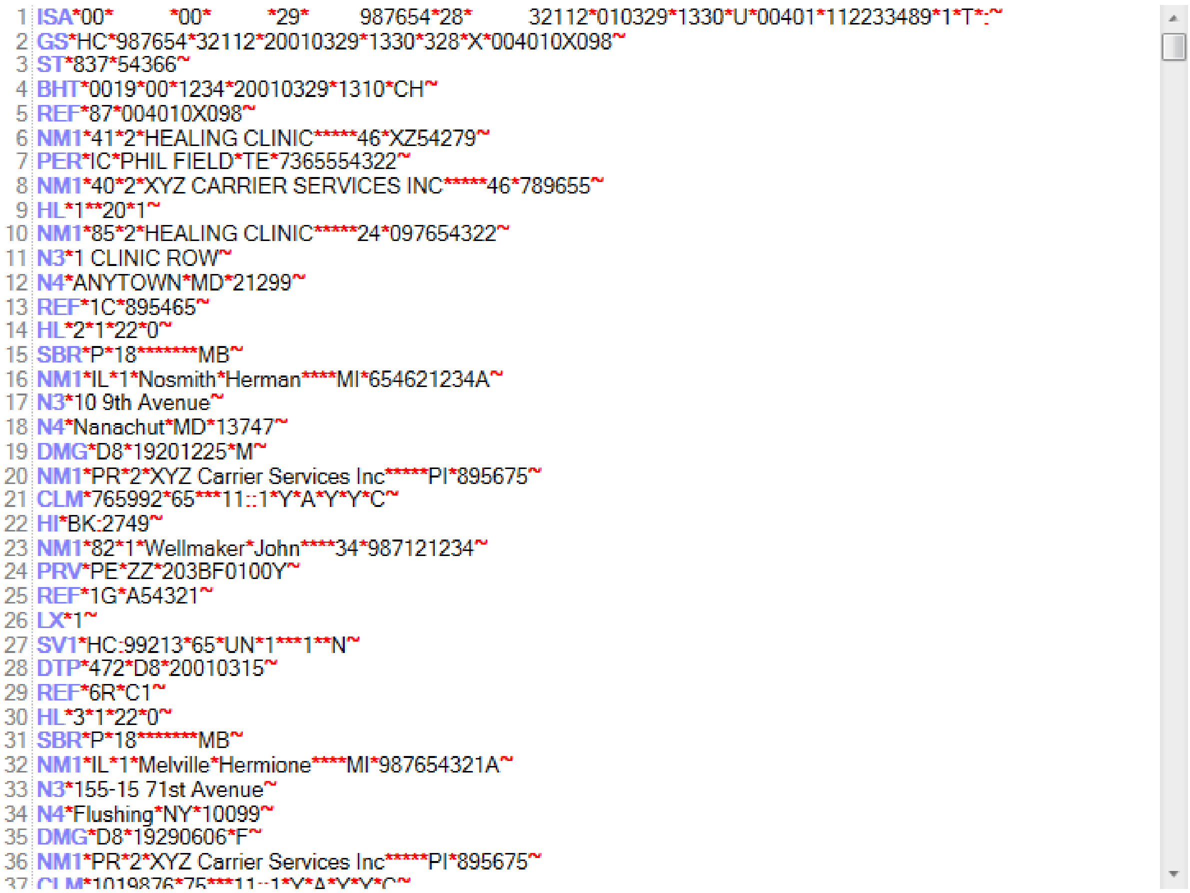
What is an EDI file?

X12 is an ASCII standard. This means that all the content of a transmission consists of ASCII characters. ASCII or text files can be viewed and edited with a regular text editor. Below you see an EDI file opened with Notepad. It opens alright but since EDI does not use line feeds and carriage returns to mark the end of a line, an EDI document is usually very hard to view.



A view of raw EDI data

Making sense of this data stream is quite difficult. Even if we display the data in a special EDI Editor the untrained cannot make out what it means.



```
ISA*00*          *00*          *29*       987654*28*        32112*010329*1330*U*00401*112233489*1*T*:~
GS*HC*987654*32112*20010329*1330*328*X*004010X098~
ST*837*54366~
BHT*0019*00*1234*20010329*1310*CH~
REF*87*004010X098~
NM1*41*2*HEALING CLINIC*****46*XZ54279~
PER*IC*PHIL FIELD*TE*7365554322~
NM1*40*2*XYZ CARRIER SERVICES INC*****46*789655~
HL*1**20*1~
NM1*85*2*HEALING CLINIC*****24*097654322~
N3*1 CLINIC ROW~
N4*ANYTOWN*MD*21299~
REF*1C*895465~
HL*2*1*22*0~
SBR*P*18*******MB~
NM1*IL*1*Nosmith*Herman****MI*654621234A~
N3*10 9th Avenue~
N4*Nanachut*MD*13747~
DMG*D8*19201225*M~
NM1*PR*2*XYZ Carrier Services Inc*****PI*895675~
CLM*765992*65***11::1*Y*A*Y*Y*C~
HI*BK:2749~
NM1*82*1*Wellmaker*John****34*987121234~
PRV*PE*ZZ*203BF0100Y~
REF*1G*A54321~
LX*1~
SV1*HC:99213*65*UN*1***1**N~
DTP*472*D8*20010315~
REF*6R*C1~
HL*3*1*22*0~
SBR*P*18*******MB~
NM1*IL*1*Melville*Hermione****MI*987654321A~
N3*155-15 71st Avenue~
N4*Flushing*NY*10099~
DMG*D8*19290606*F~
NM1*PR*2*XYZ Carrier Services Inc*****PI*895675~
CLM*1019876*75***11::1*Y*A*Y*Y*C~
```

EDI data displayed in the built-in EDI Editor

To fully explain the structure of EDI is not part of this introduction but we can point out some of the features. Each line in this editor screen is called 'Segment'. Every EDI file starts with the ISA segment. Each segment has multiple elements which are separated by the element separator which in this case is the '*'. Sometimes elements themselves are subdivided into sub-elements, here it is the colon ':'. Each segment is terminated by the segment delimiter, in this case the tilde '~'. The rules of a particular transaction set are determined in the so called implementation guide.

1.3 Payer Obligations

All providers of commercial health insurance benefits must comply with the CORE operating rules. The Committee on Operating Rules for Information Exchange (CORE) was proposed by CAQH(the Council for Affordable Quality Healthcare) as an initiative to develop a solution that enables consistent provider access to healthcare administrative information before or at the time of service using their choice of electronic system. At has become law with the introduction of the Affordable Care Act (Obama Care)

CORE Operating Rules

The Patient Protection and Affordable Care Act (ACA) defines operating rules as, “the necessary business rules and guidelines for the electronic exchange of information that are not defined by a standard or its implementation specifications."

ACA Section 1104 applies to HIPAA covered entities and business associates engaging in HIPAA standard transactions on behalf of covered entities. The legislation requires that the standards and associated operating rules adopted by the Secretary will:

- Enable the determination of an individual’s eligibility and financial responsibility for specific services prior to or at the point of care;
- Be comprehensive, requiring minimal augmentation by paper or other communications;
- Provide for timely acknowledgement, response, and status reporting that supports a transparent claims and denial management process (including adjudication and appeals);
- Describe all data elements (including reason and remark codes) in unambiguous terms, require that such data elements be required or conditioned upon set values in other fields, and prohibit additional conditions (except where necessary to implement State or Federal law, or to protect against fraud and abuse).

Section 1104 of the Patient Protection and Affordable Care Act (ACA) mandates a certification process for health plans only.

Per the ACA, health plans must file a statement with HHS, in such form as the Secretary may require, certifying that their data and information systems are in compliance with any applicable transaction standards and associated operating rules; financial penalties for health plans are significant.

The adoption deadline for Eligibility and Claim Status EDI transactions (included in Phase I and Phase II of the CORE Operating Rules) was 1/1/2013, so far the HHS has not enforced this deadline with penalties and affected entities are still in the implementation phase.

On December 31, 2013, HHS issued a Notice of Proposed Rulemaking (MPRM) on the ACA-mandated health plan certification. The Department of Health and Human Services

(HHS) accepted public comments on the NPRM through April 3, 2014 (previously March 3, 2014). The NPRM includes health plan certification requirements for the eligibility, claim status, electronic funds transfers (EFT), and electronic remittance advice (ERA) transactions.

1.4 Features and Licenses

The HIPAA Claim Status Checker comes with several features. The **basic version** is has no database attached. It allows for

- Manual entry of claim status requests
- Import of 276 claim status request files that were created somewhere else and editing the information
- Display and printing of claim status requests in humanly readable format with all the cryptic codes translated.
- Creation of 276 EDI files
- Reading, displaying and printing the information of 277 claim status responses as well as 277CA claim acknowledgments in humanly readable format with all the cryptic codes translated.

The transport of the EDI files to the payer and receiving the responses are left to other devices in the basic version.

Image file creation. This feature allows for the saving in TIFF or PDF format of the display images from 276 and 277 files.

Database connectivity. By tying the HIPAA Claim Status Responder to a database the product becomes vastly more powerful. Now we can save claim status request and response records in the database and link the request with the response. In addition there are tables for the company setup and requesters, subscribers and providers that are used in the manual entry forms are remembered and make the data entry much faster.

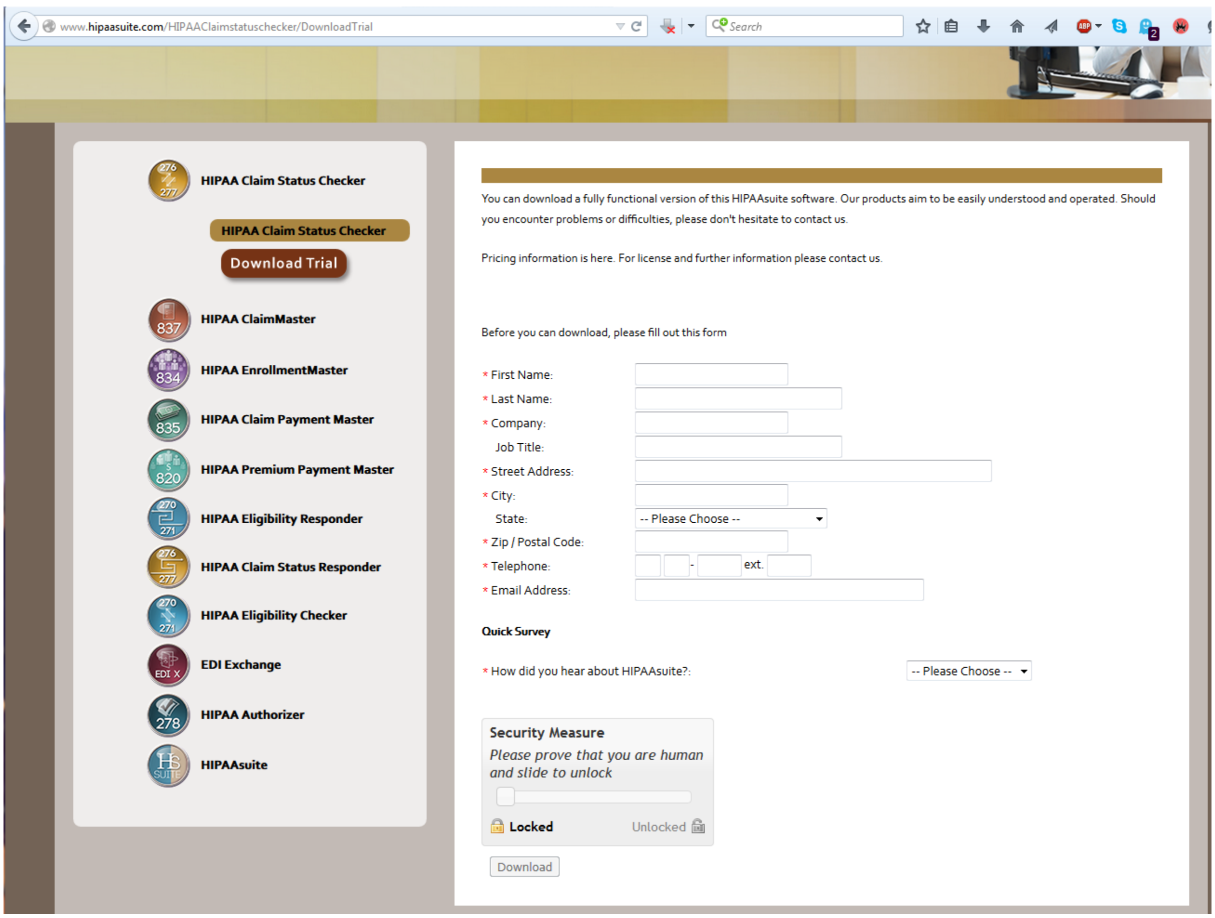
EDI Exchange. This module again expands the functionality of the software by adding all that is necessary to transport the 276 request files to the payers and receive from them the response. EDI Exchange handles the trading partners and their peculiarities, encryption, FTP, SFTP, has logs for incoming and outgoing files, Checks in and out going EDI files for HIPAA compliance and more.

RealTime Client. The HIPAAsuite RealTime client is an add-on to EDI Exchange and adds the capability to exchange requests with payers and receive responses in real-time or batch mode according to the CORE protocols MIME and SOAP.

2 Getting Started

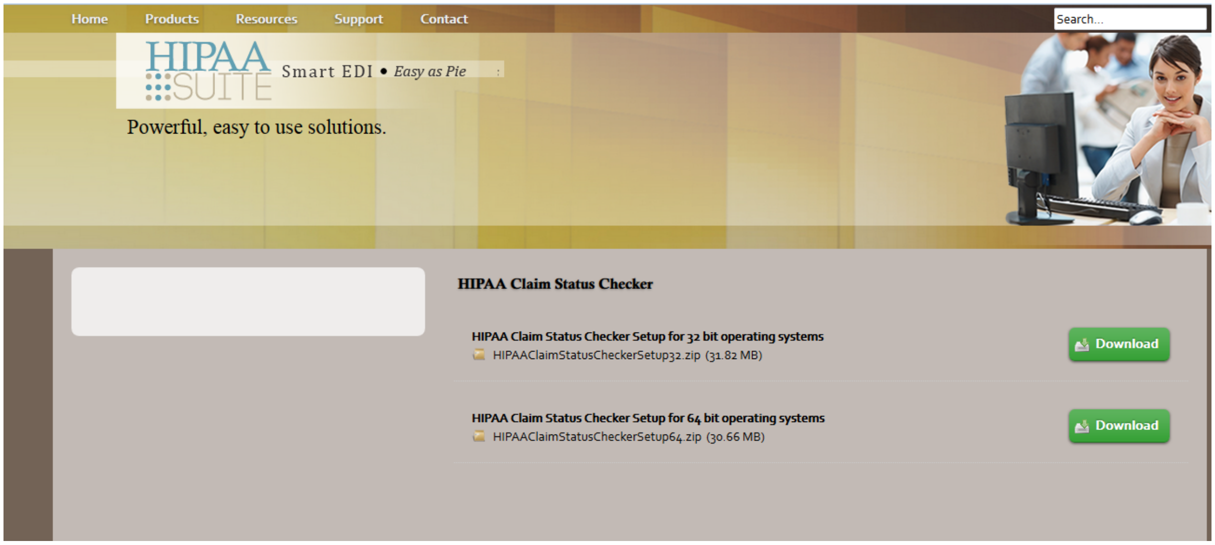
2.1 Downloading the software

The HIPAA Eligibility Checker can be downloaded from HIPAAsuite's website here



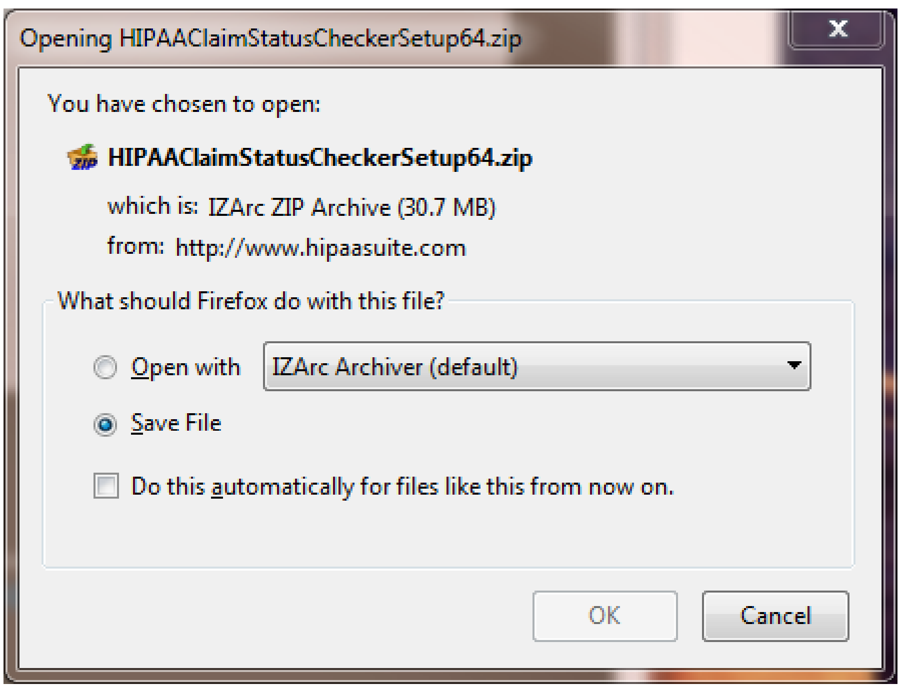
The questionnaire leading to the download

You will have to fill out a form and once you submit this, you have the choice between the 32bit or the 64 bit version of the software



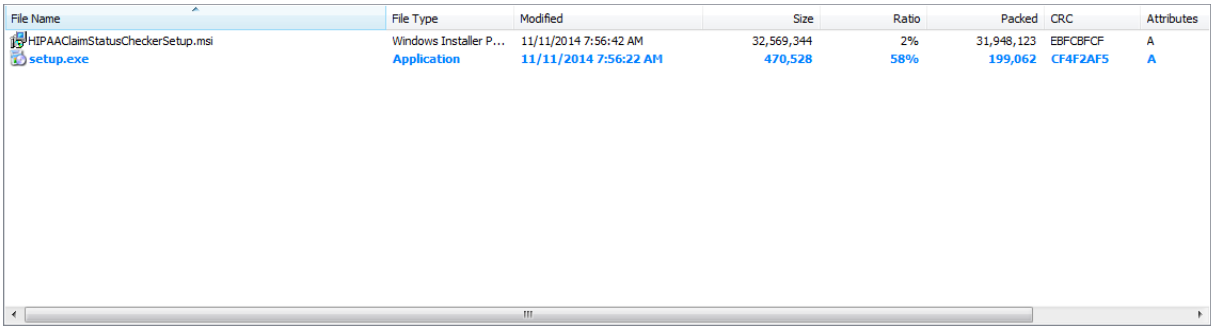
The download page showing the 2 versions of the installer

Download the 64 bit version only if you have a 64 bit version of the Windows operating system.



The downloaded zip file

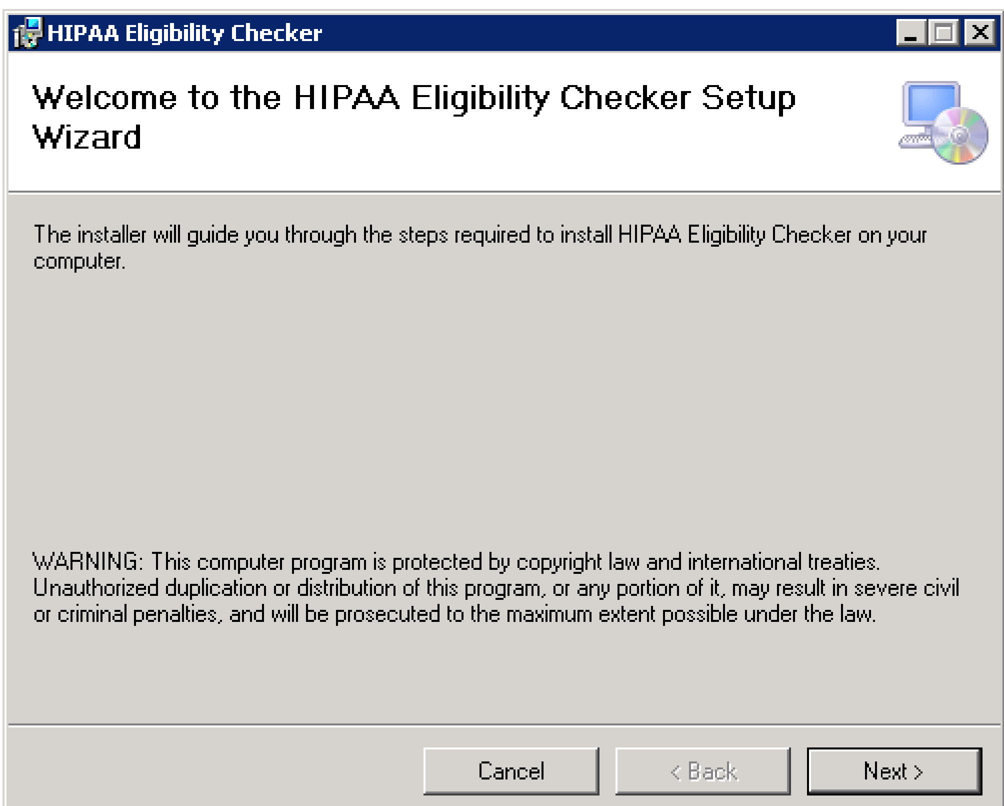
Once the download has completed you can install the software by unzipping the file and running the Setup.exe program.



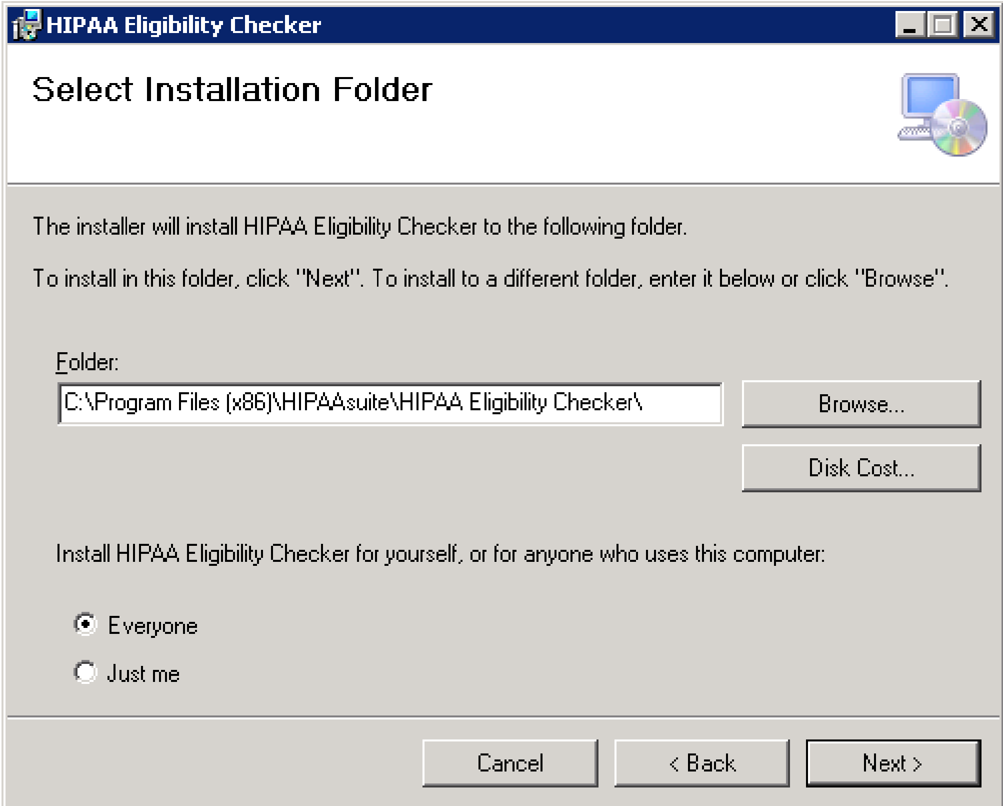
The content of the zip file

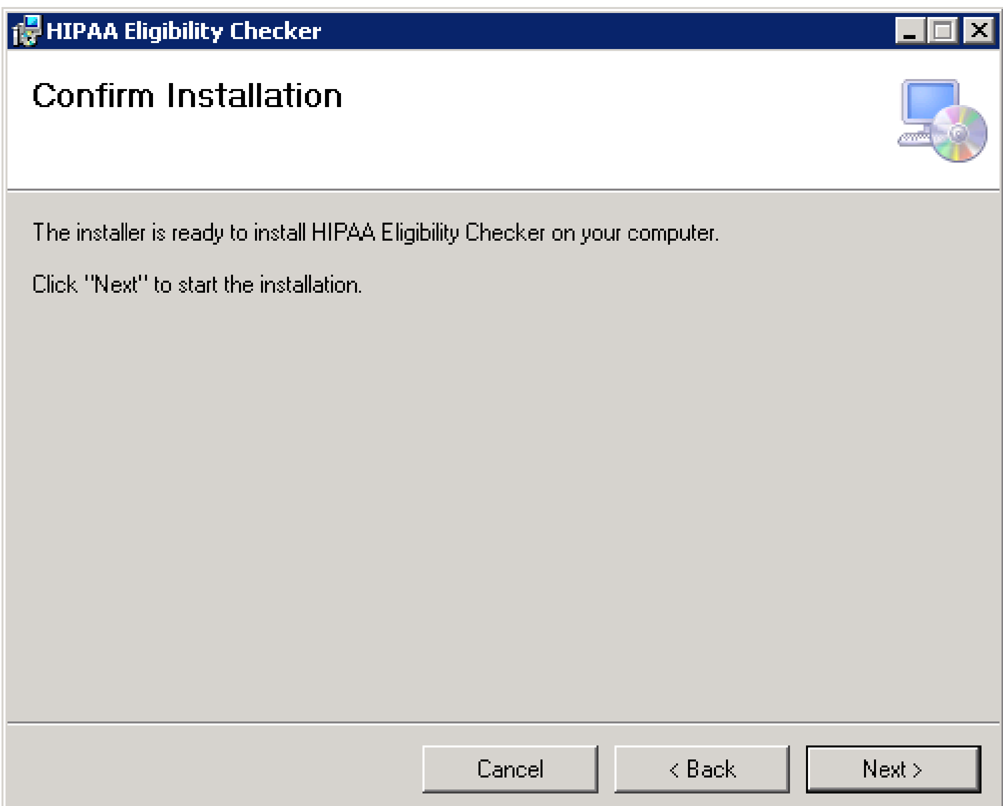
The Setup program ensures that all the Microsoft Windows components needed for the program are installed on the computer. Running just the Microsoft Installer (.msi file) might leave out critical dependencies.

2.2 Installation



Select an installation folder. The default value will be filled for you, but it can be changed.


HIPAA Eligibility Checker
Select Installation Folder
The installer will install HIPAA Eligibility Checker to the following folder.
To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".
Folder:
C:\Program Files (x86)\HIPAAsuite\HIPAA Eligibility Checker\
Browse...
Disk Cost...
Install HIPAA Eligibility Checker for yourself, or for anyone who uses this computer:
Everyone
Just me
Cancel
< Back
Next >

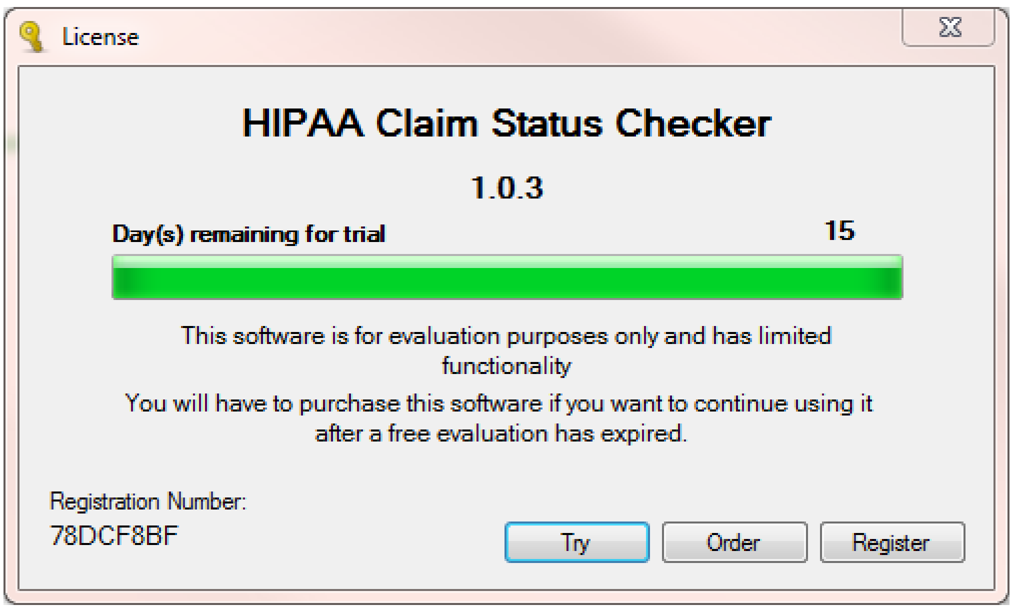

HIPAA Eligibility Checker
Confirm Installation
The installer is ready to install HIPAA Eligibility Checker on your computer.
Click "Next" to start the installation.
Cancel
< Back
Next >

2.3 Software Trial

The HIPAA Eligibility Checker comes with a free trial of 14 days.

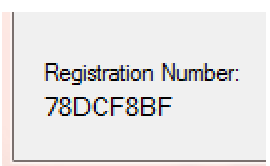
Should your trial time expire and you wish to continue your testing of the software, please send an email to info@HIPAAsuite.com with the Registration number and we will give you a trial extension.

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



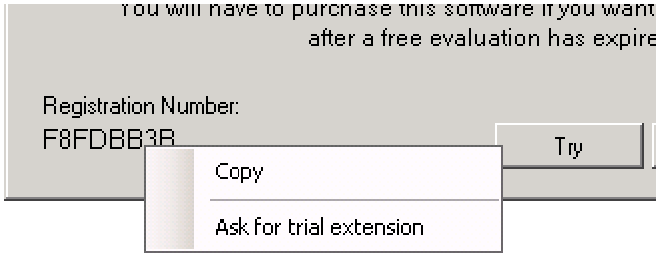
The Trial Screen

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



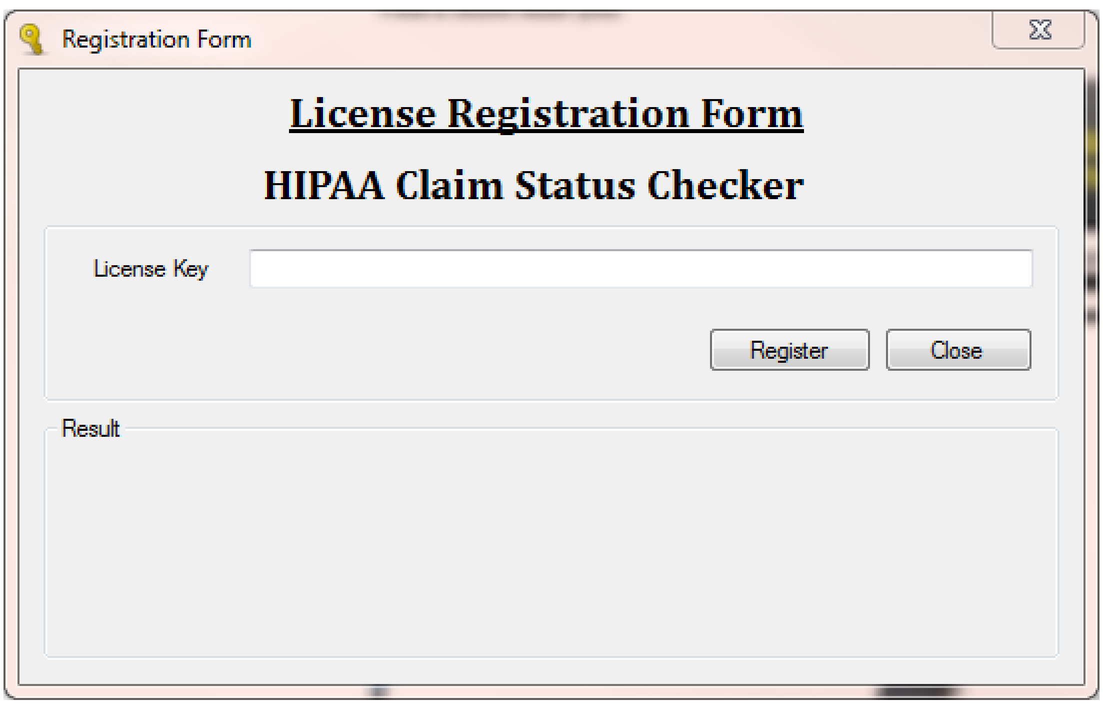
The Registration number

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!)



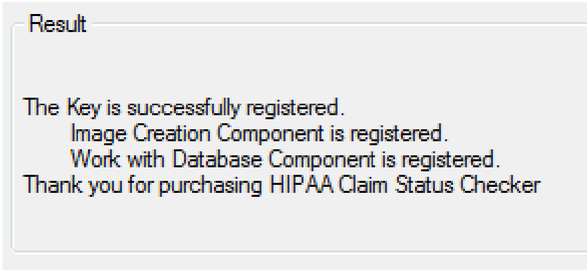
Copy the registration number to the Windows clip board by hovering over the it with the mouse

Once you have received the license key from us you click on the 'Register' button and the license registration from 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. Once you entered the license key, you will see the results



The result of entering a license key

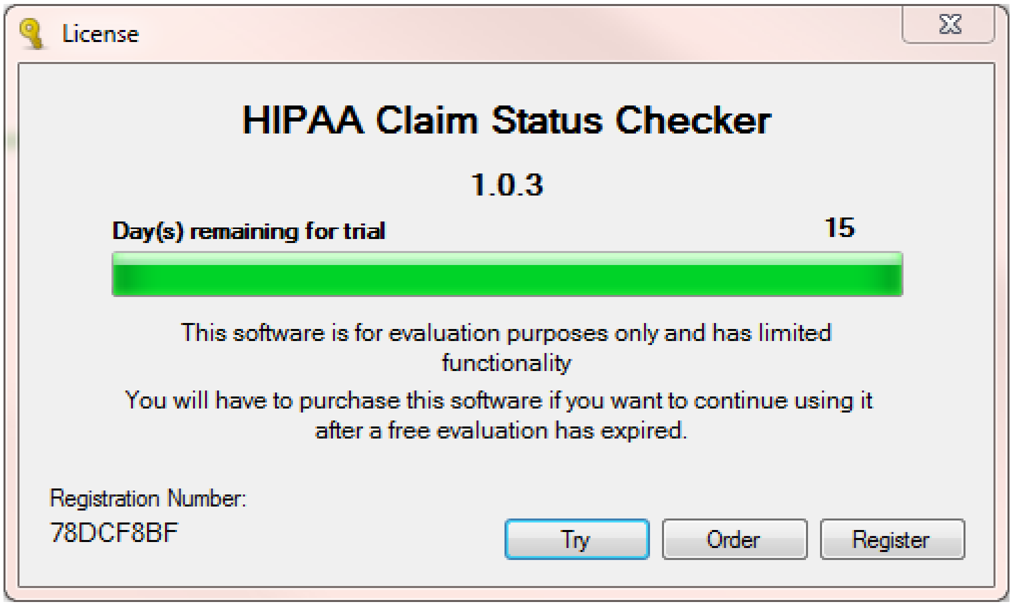
Once the product is registered with a permanent unlock code, future upgrades will find this key and install without further action necessary.

2.4 Requesting a Trial Extension

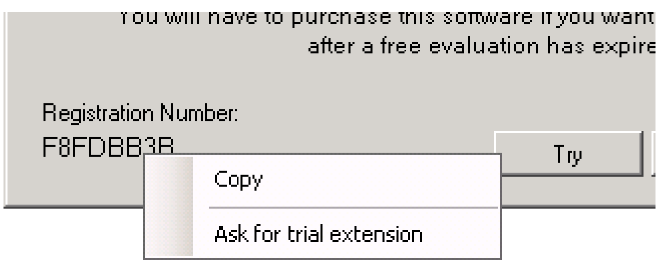
The HIPAA Claim Master comes with a free trial of 15 days. Once your trial period has expired, the application will stop working. There are limitations to the trial version, for example, you can only export the first 50 records of EDI files, and only 5 files per directory processing. We are sorry to have to limit the experience, but we had instances where organizations used the software for production purposes without purchasing it.

We do not mind extending your trial if you need extra time to evaluate the software. You will only need to send us the registration number and we will gladly give you another 15 day trial. If your trial time has expired 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 you need to continue your trial of the product, follow the instructions below.



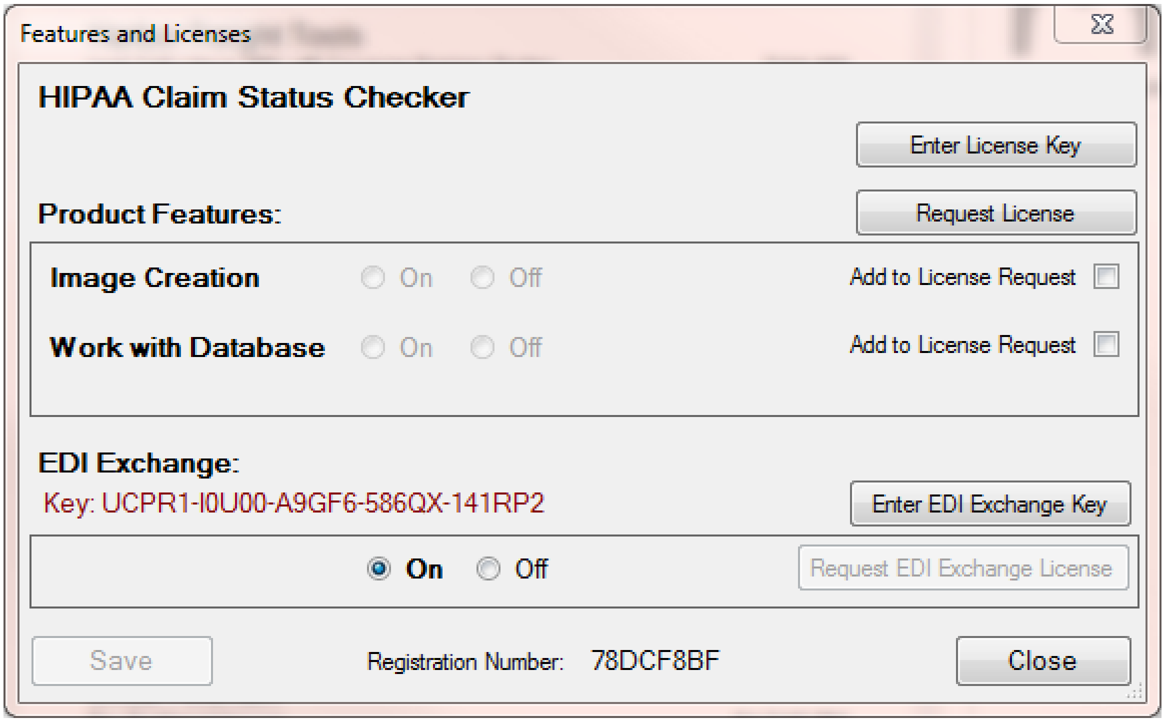
1. Launch the application.
2. Click on the "Ask for Trial Extension" button on the displayed window.



The "Ask for Trial Extension" button

Tip: You can see the registration number in the lower left hand corner. This number is needed for the registration as well as trial extension. It is unique to your computer and hardware. You can hover over the registration number and copy it to the clipboard, so that you can easily paste it into the email. This avoids human error. (The letter "O" is never used, only zeros.) Hovering over the number will give you the following floating menu:

3. Clicking on the "Ask for Trial Extension" button will bring up the feature control window.

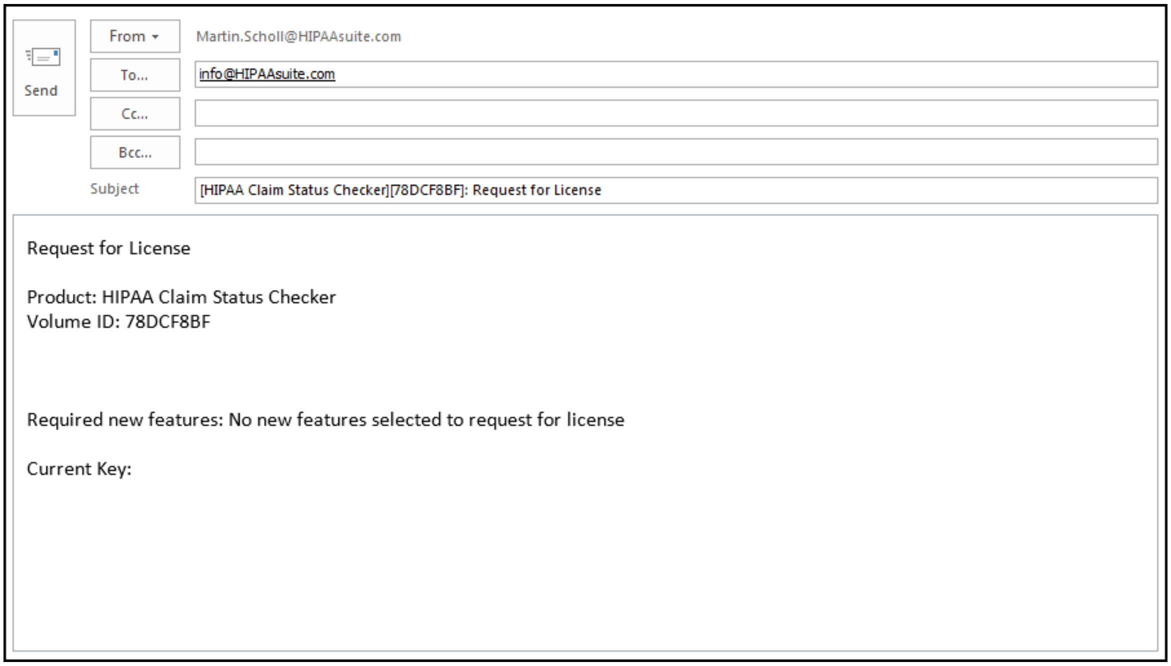


The "Features and Licenses" window

4. Select the features you need and click on "Request Trial license."

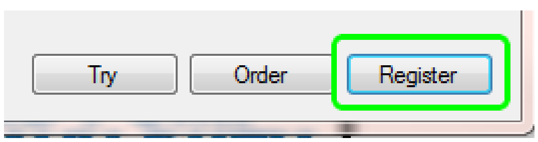
5. An email to HIPAAsuite will be created. The message will contain the registration number so they can then create the extension key. For example, this will open Outlook with the following data inserted:

   - To: info@HIPAAsuite.com
   - Subject: [HIPAA Claim Status Checker][123456789]: Request for Trial License Extension
   - Message: Volume ID: 123456789



The trial extension request email

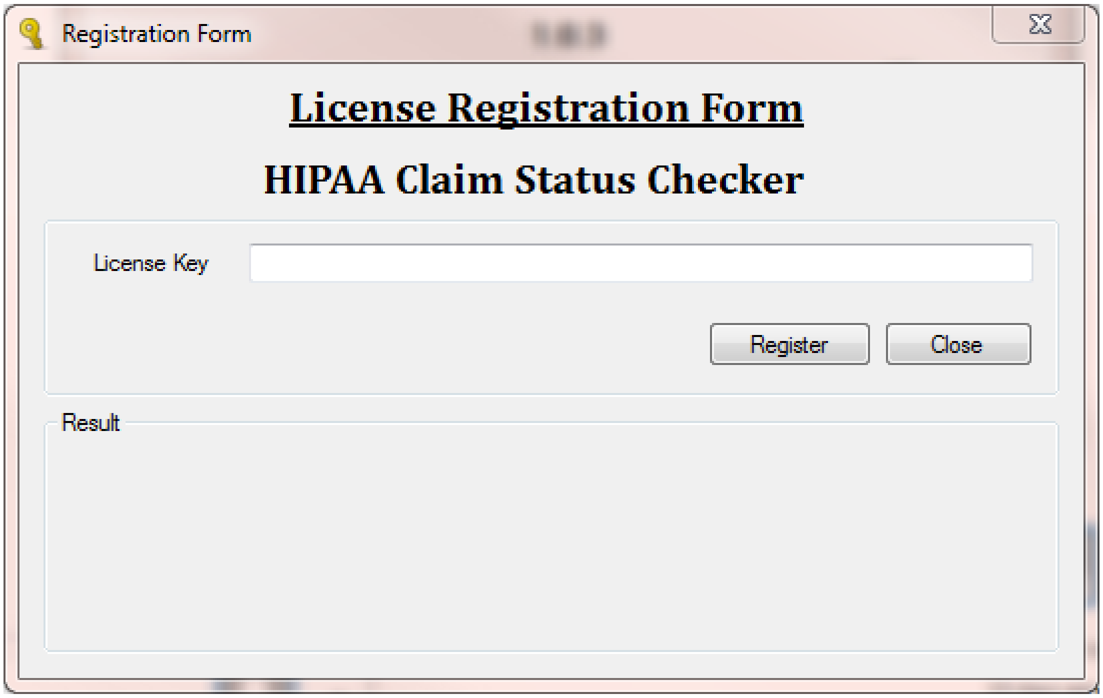
6. The response from the support team includes an activation key.
7. Once you have the activation/unlock key, click "Register" on the program welcome window.



The "Register" button

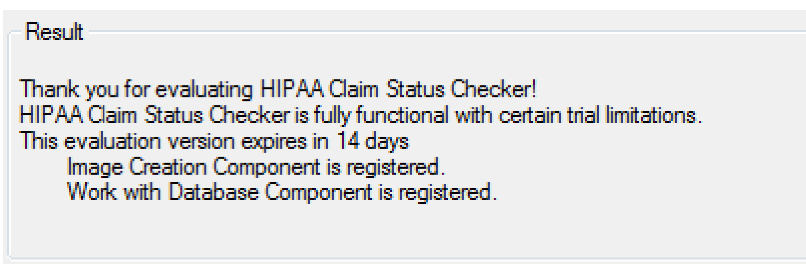
8. Paste the activation key into the field on the Registration Form and then click "Register."

   Tip: The field is case-sensitive. The best thing to do is to copy and paste the License Key from our email.



The "Registration Form" window with entered license key and highlighted "Register" button

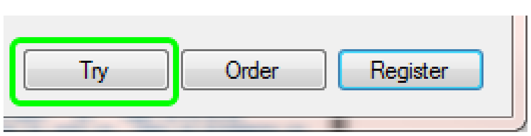
9. The success message will appear in the "Result" border. You will see what components have been registered.



The trial license activation result

Click "Close."

10. Once the license key has been entered, click "Try" on the welcome window to continue using the program for another 15 days.

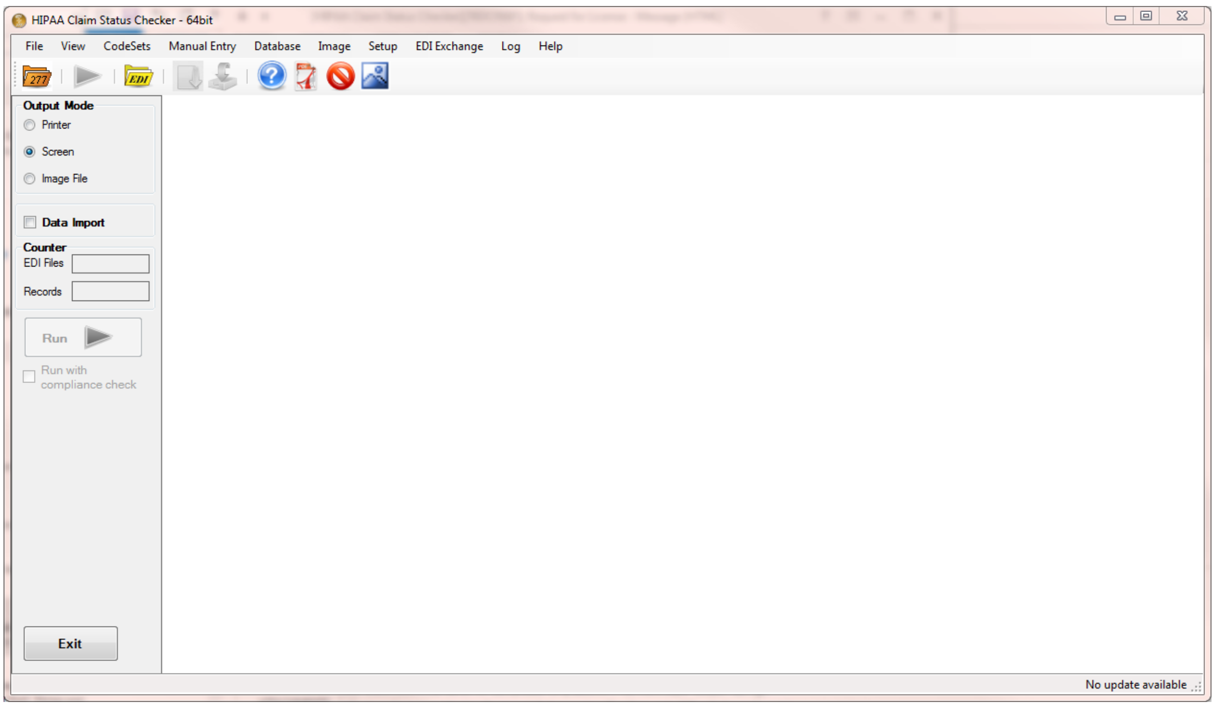


The "Try" button

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

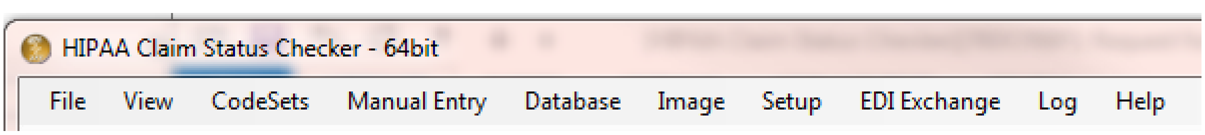
2.5 Starting the Application

When you start the HIPAA Claim Status Checker you will see its main screen



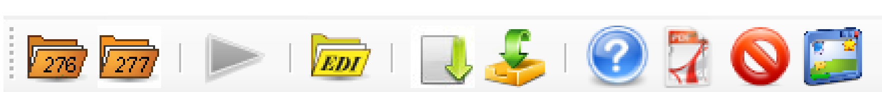
The main screen of the HIPAA Eligibility Checker

You see the menu bar on top of the screen



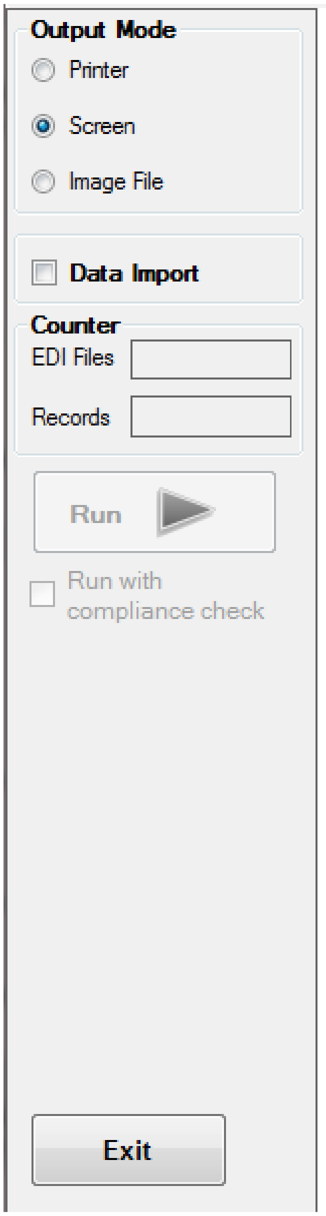
The main menu

and the task bar buttons below.



The task bar

On the left side is the Info bar that is important when you want to import EDI files.



The info bar on the left side of the main screen

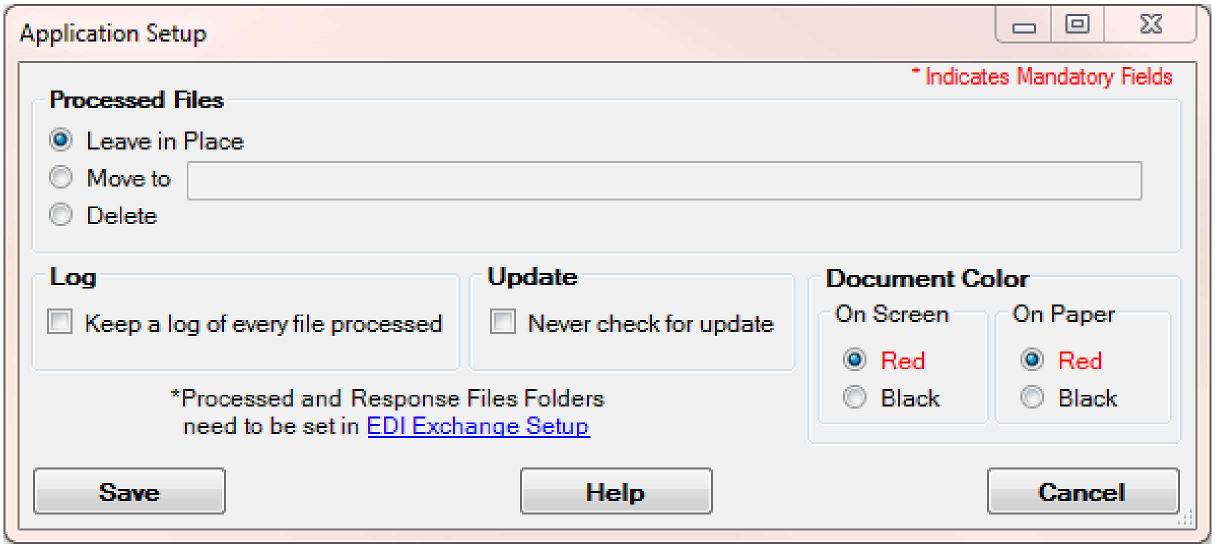
3 Setup

We have three sub item under the main menu entry "Setup"

- Application Setup
- Company Setup
- Delimiter Setup

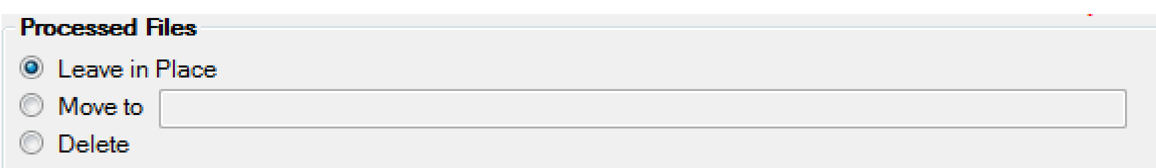
3.1 Application Setup

When you click on 'Application Setup, the following screen comes up



The Application Setup screen

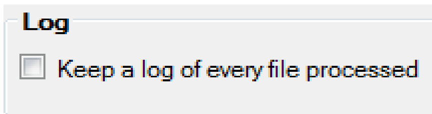
The first setting concerns the handling of EDI files after processing. In order to avoid the duplicate processing of EDI files, we recommend that you **move files after processing** into an archive folder so that they are not processed multiple times. If you work with a copy of files, stored somewhere else you might also delete files after processing but make sure that you have the original somewhere. EDI files are important business documents and you want to make sure that you can access the information in them at a later point in time for trouble shooting and other reasons.



Determining the handling of processed files

If you use EDI Exchange, the Processed File folder is given by the folder schema of EDI Exchange where each trading partner has a place for their folders.

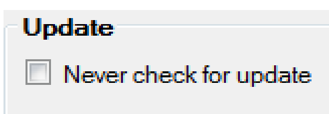
The next item is the **log**. The HIPAA Eligibility Checker keeps track of all the step of processing EDI files. When it is run through the command line, those messages will be saved in the log.



The log setting determines whether process messages will be saved to the log file at all times

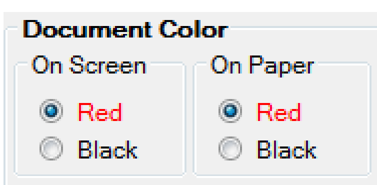
Checking the above check box ensures that all process messages are written to the log file regardless whether the application is run through the command line or the user interface.

The next item determines whether the application on start-up looks for the existence of updates and newer version. Some companies have a strict policy that all updates have to be thoroughly tested before they can be implemented and users should not be faced with an option of update the application. For this case we have the below check mark



Set if you want to suppress update messages

The last thing on the setup screen determines whether the back ground and labels on the printable eligibility form are in red to contrast them with the font color of black. When printing the forms to paper on a color printer you can save money and resources by choosing black. Otherwise it makes the forms much easier to read when you have background and labels in red.



Set the color of document background and labels.

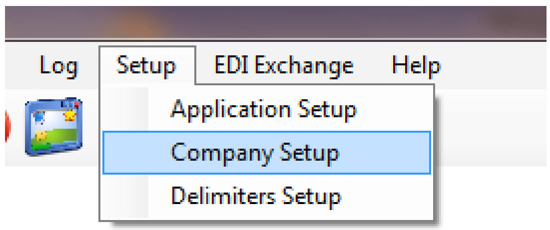
3.2 Company Setup

Creating EDI files will include a lot of information on you and your trading partners. The company setup screen is designed to enter all the necessary information for the EDI creation.When you create EDI files there are a few elements needed to identify your company as the sender, the producer of this EDI file. For this matter, use the company setup screen. You can specify your company information and other setting related to your company there.

If you have the EDI Exchange component licensed then all this information is stored in the data file "COMPANY_SETUP". If you don't have this component then this information is stored in the Windows registry.

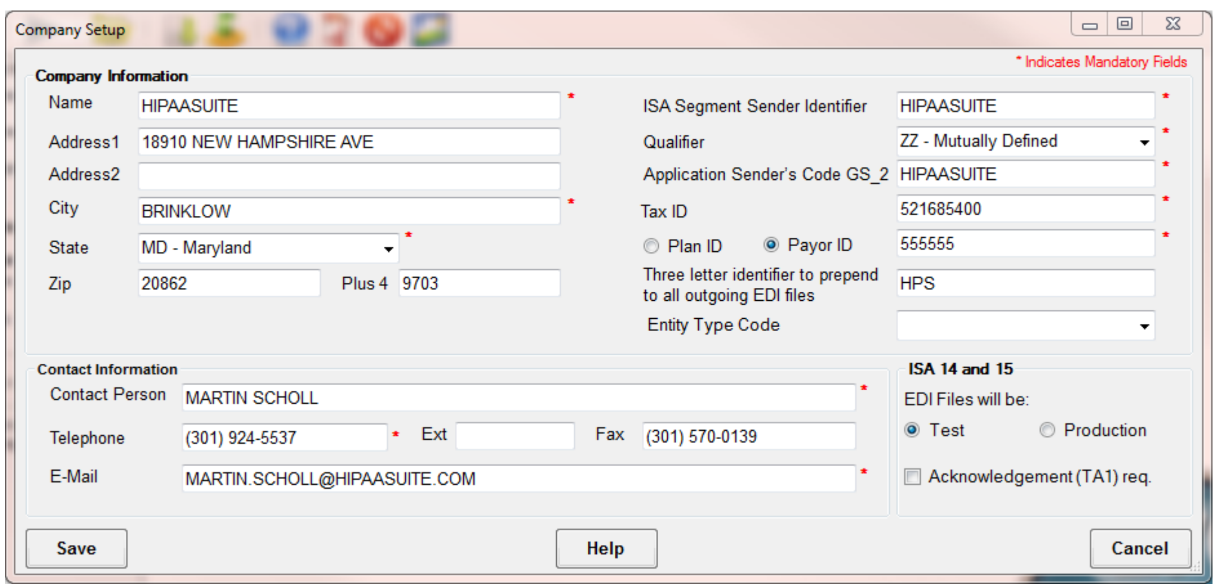
> Note: You need to configure the database first. See Setting up Database Connection.

1. To configure the company, select Setup -->*Company Setup* in the main menu.



The "Company Setup" menu

2. The following screen will appear.



The "Company Setup" window

3. You can configure the following options:

- **Company Information**
- **EDI Version**
- **Contact Information**
- **ISA 14 and 15**

Read the detailed descriptions further.

4. Once you have finished editing the options, click "Save."

Company Information

- **Name** — Company name. Obligatory option.
- **Address 1**
- **Address 2**
- **City** — Obligatory option.
- **State** — Obligatory option.
- **ZIP**
- **Plus 4**
- **ISA Segment Sender Identification** — It is the most important option to choose. It identifies your organization for all EDI transactions. Most commonly the Qualifier "ZZ" and a free form ID up to 15 character in length is chosen. Other options include your tax ID and the Dun & Bradstreet ID.
- **Qualifier** — 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 & Bradstreet)
    - 14 — Duns Plus Suffix
    - 20 — Health Industry Number (HIN)
    - 27 — Carrier ID Number (Identification Number as assigned by HCFA)
    - 28 — Fiscal Intermediary ID Number (Identification Number as assigned by HCFA)
    - 29 — Medicare Provider and Supplier ID Number (Identification Number as assigned by HCFA)
    - 30 — U.S. Federal Tax ID Number (Identification Number)
    - 33 — NAIC Company Code (National Association of Insurance Commissioners Company Code)

  - ZZ — Mutually Defined

- **Application Sender's Code GS_2** — The option represents the program or machine that created the file. Usually the same as the ISA Segment Sender Identification. You can select other ID if you need. Obligatory option. The GS_02 identifier is usually the same as the ISA identifier but you can also choose some other ID. It represents the program or machine that created the file, but the most common is a repetition of the ISA identifier.
- **Tax ID** — Obligatory option. Also called an Employer Identification Number (EIN).
- **Plan ID / Payer ID** — Fill in your Payer ID and Plan ID if you have one; this is only important for the 271 and 277 transactions. Optional setting.
- **Three letter identifier to prepend to all outgoing EDI files** — Optional setting. Makes your files easily identifiable.

EDI version

Specify EDI version:

- **only 4010**
- **4010 if in original otherwise 5010**
- **only 5010**

Contact Information

The contact information goes into the PER segment of outgoing transactions:

- **Contact Person**
- **Telephone**
- **Ext**
- **Fax**
- **E-mail**

ISA 14 and 15

- **EDI files will be** — ISA element 14 determines if the resultant file contains test or production data:

- **Test**
- **Production**

- **Acknowledgment (TA1) requested.** — ISA element 15 indicates whether you want a TA1 acknowledgement for files that you send out.

3.3 Delimiters 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.

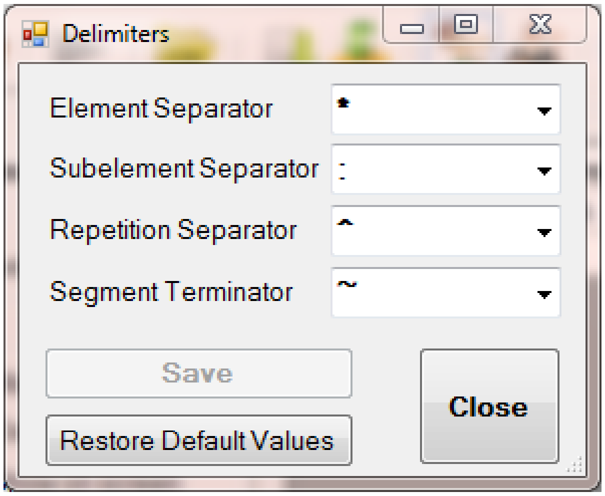
The element separator is the 4th byte of any EDI file. It separates the elements of the segments. All HIPAAsuite products default to * for the element separator.

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

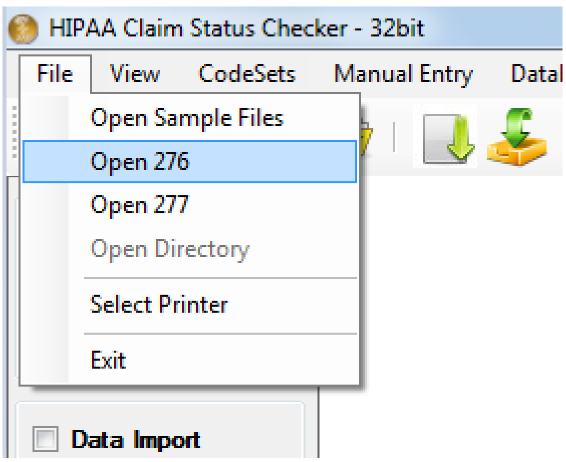


The delimiter screen

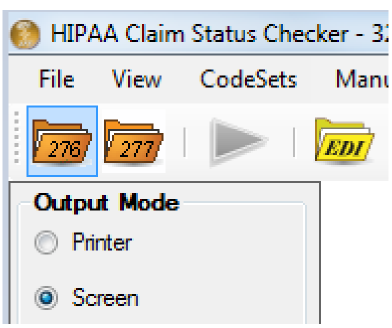
4 Working with Requests

4.1 Importing 270 request files

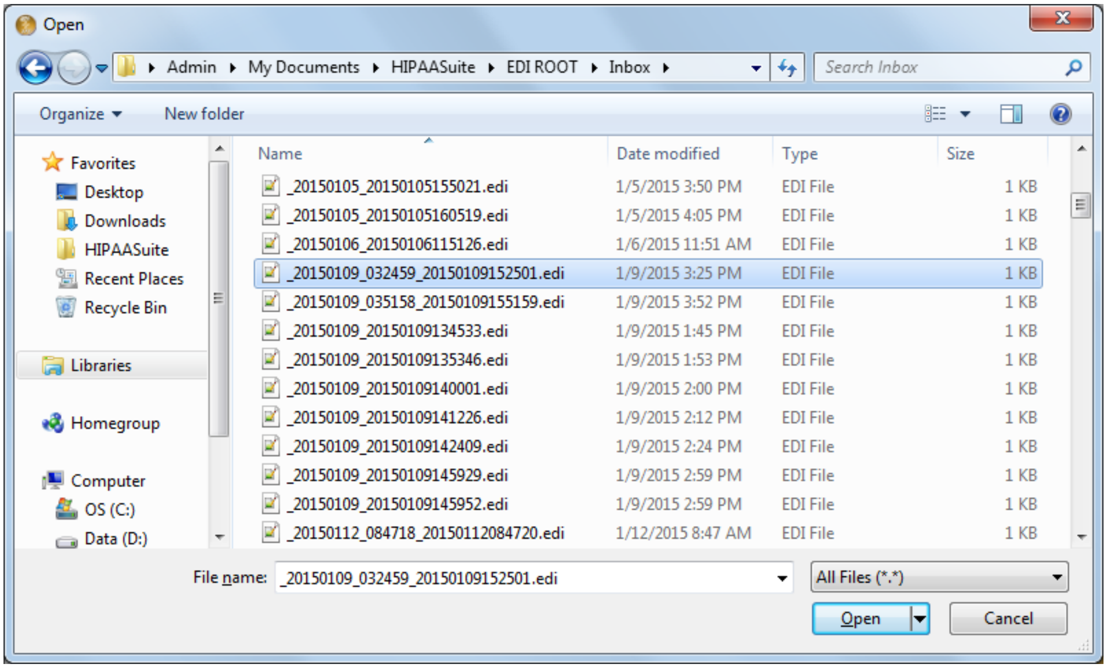
The 'File' menu has a sub menu "Open 276" with which we can open the explorer and select a file.



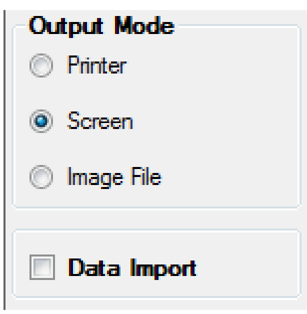
Alternatively we can use the "Open 276" toolstrip button to do the same.



Once a file is selected, we can decide what to do with it.

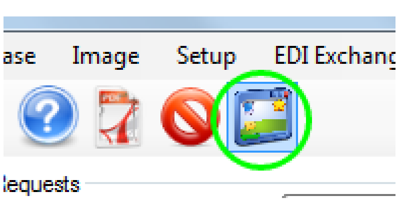


We have the option to print what we call a report to the printer, to view the request on screen, create an image file or load the requests into the workplace for further processing.



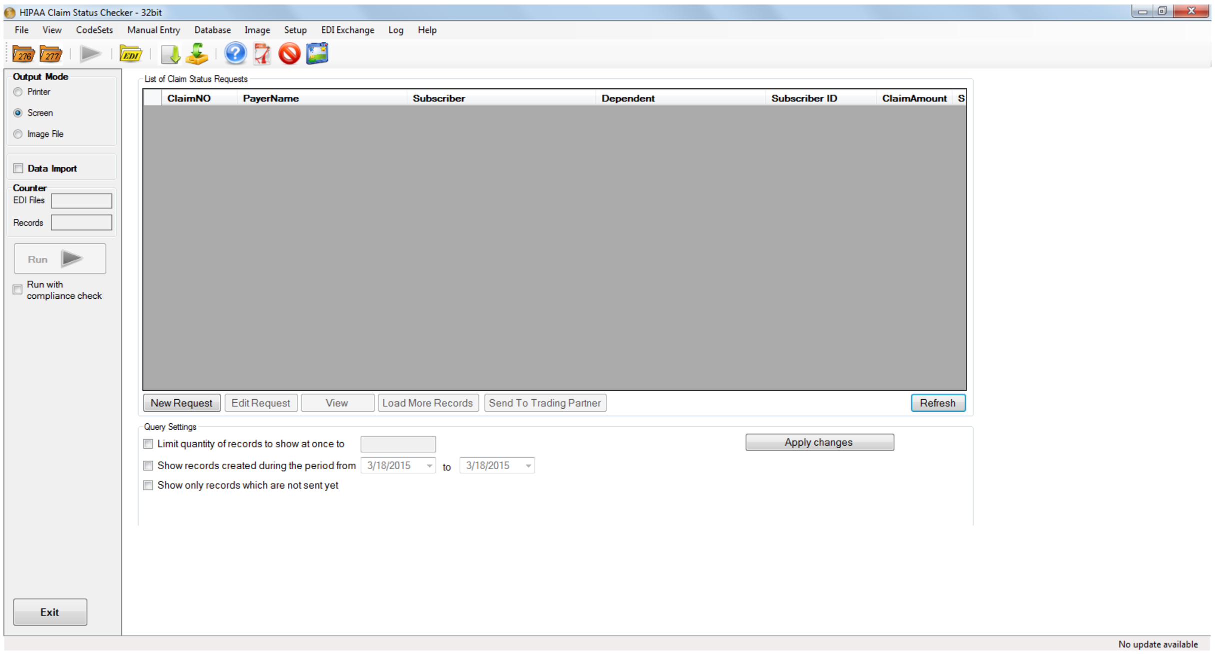
4.2 The Workplace Grid

The workplace grid is the area where requests and their responses are managed. We reach it from the tool strip menu by clicking the workplace icon



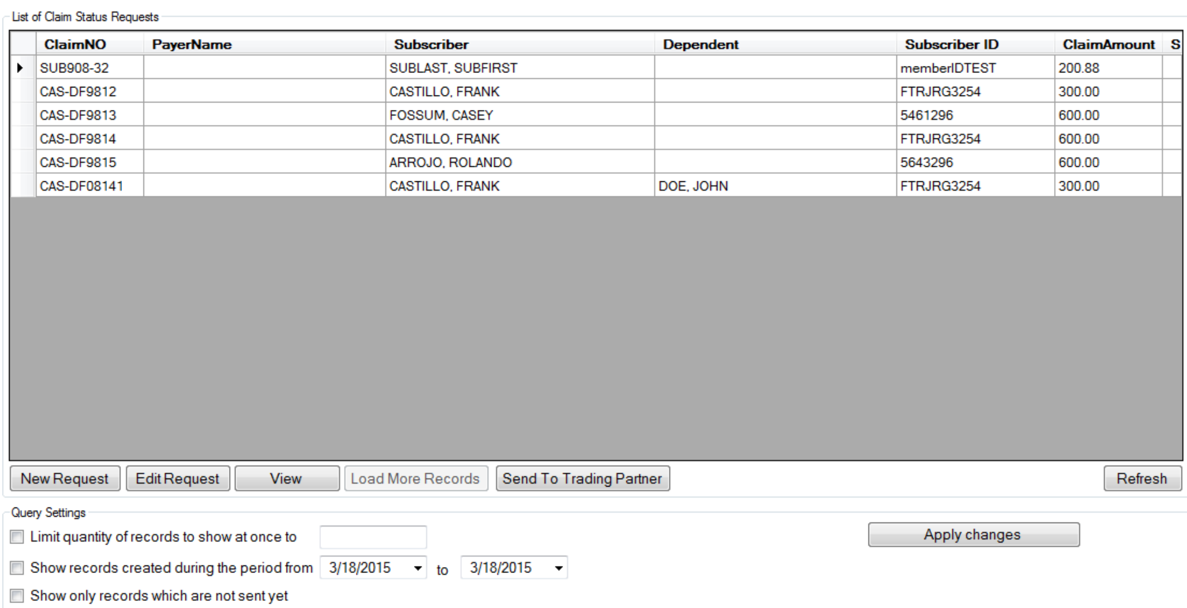
The workplace icon

Clicking the workplace icon opens the workplace

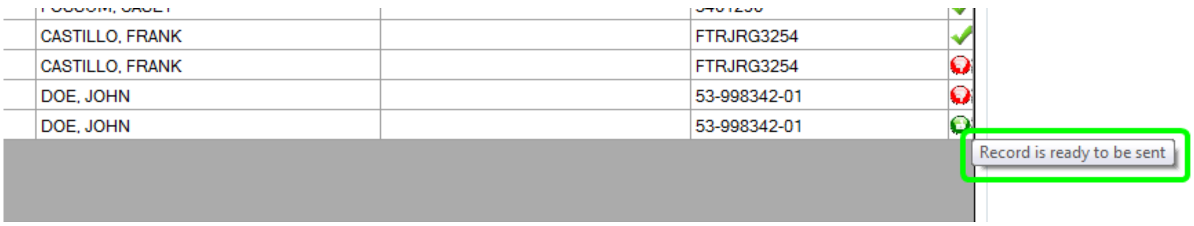


The workplace grid

When populated with a few requests, the workplace looks like this:



Each Claim Status request is presented as a single row. Columns identifying the Payor, Subscriber, Subscriber ID, and Subscriber's Dependent (if any) describe the Claim Status request each row represents. The column to the far right, the Status column, identifies the current state of the Claim Status request; that is, whether it has been sent, properly received and responed to, etc. The different statuses are described below. You can also verify what a status icon means by hovering the mouse pointer over it. A tooltip describing the request status will appear.



The request status tooltip clarifies what each status icon means.

Workplace Eligibility Request Status Icons

 **Record has errors -** Eligibility request has failed compliance check.

 **Record is ready to be sent -** Eligibility request has passed compliance check and is ready to be sent.

 **Record was not sent -** Eligibility request was not sent, sent incorrectly, or the receiving service did not acknowledge the request.

 **Record was sent successfully -** Eligibility request was correctly sent and a receipt confirmation was received. Not applicable to requests sent in RealTime mode.

 **999 received -** Eligibility request was answered with a 999.

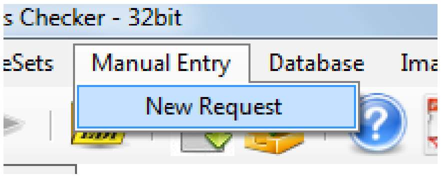
 **Record rejected -** Eligibility request has been rejected by receiving service.

 **Response received -** Eligibility request has been answered. Response is ready.

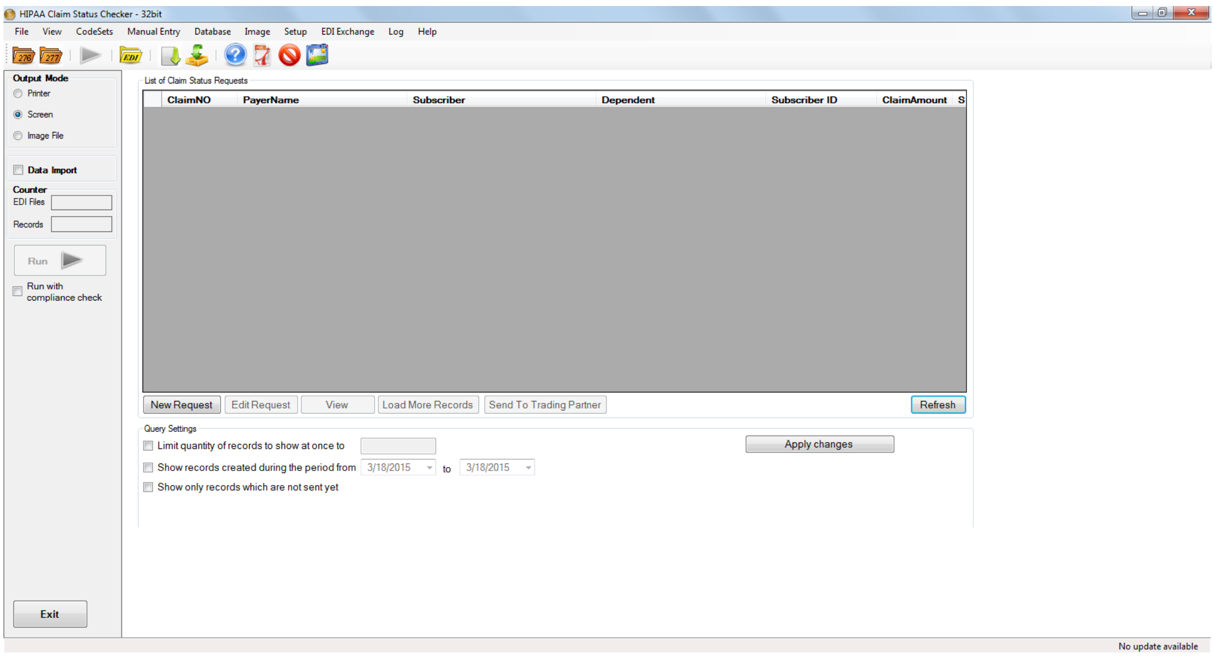
4.3 Manual Entry of Claim Status Requests

4.3.1 Manual Entry of Claim Status Requests

To create a Claim Status request manually, first click the "Manual Request" dropdown menu, then click "New Request"

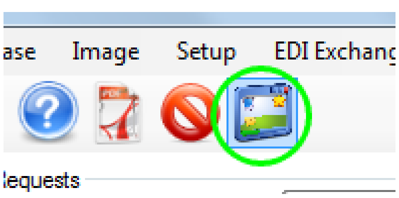


We click on New Request, the workplace grid appears. We call it work place because from the grid you control your requests and follow them through to the response.

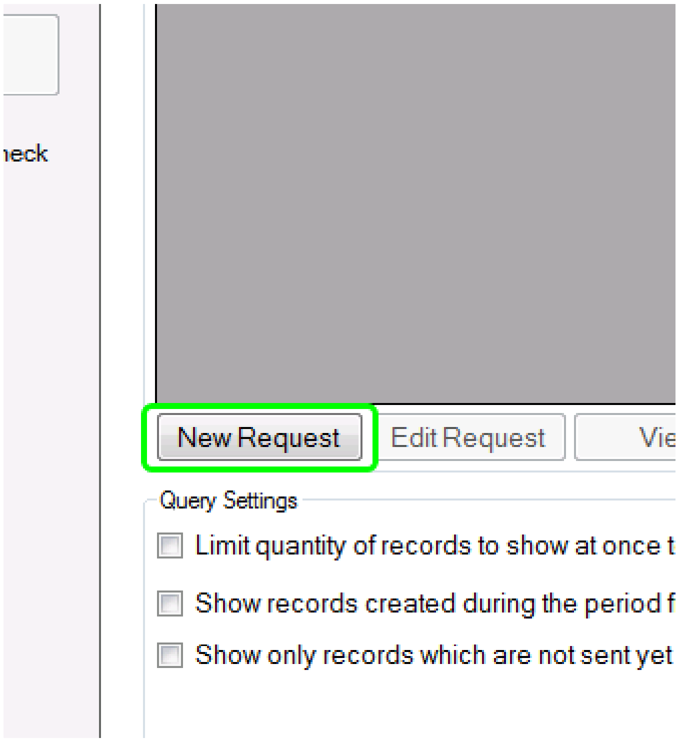


The workplace is blank because there are no requests in the database.

We can also reach the Workplace via the Workplace icon in the task bar

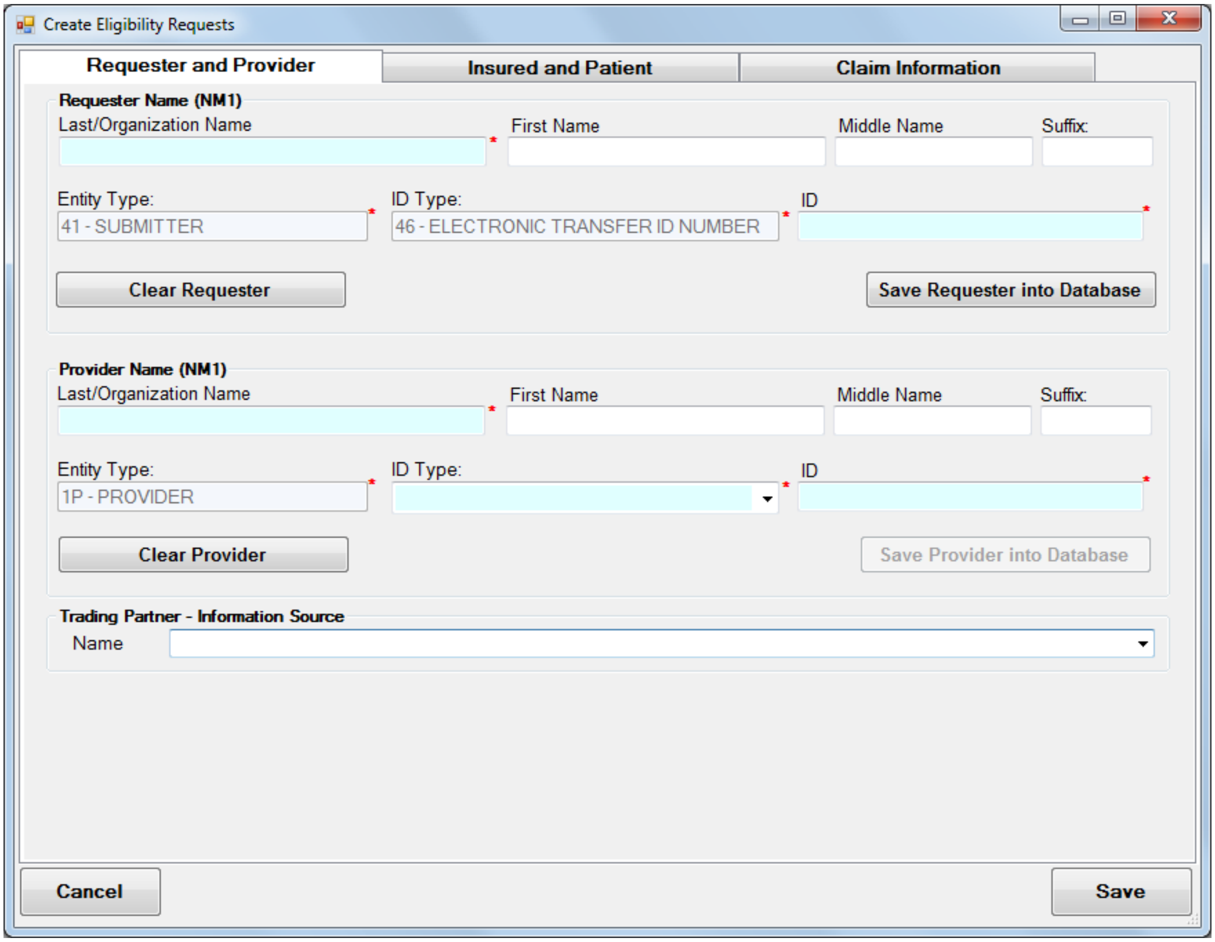


Now click on the "New Request" button in the workplace



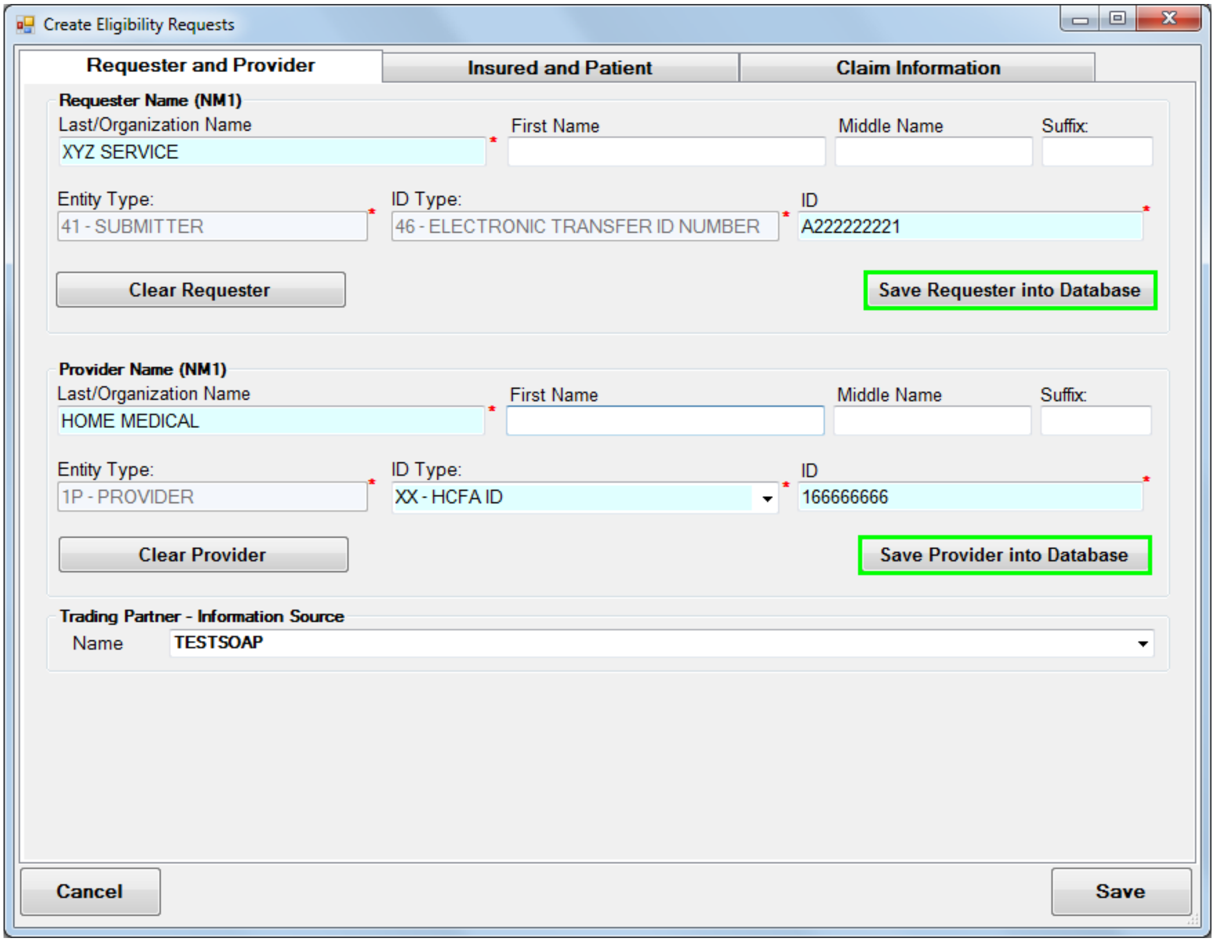
4.3.2 Entering Requester Information

When we click on "New Request" we see this screen



Information receiver and service provider tab.

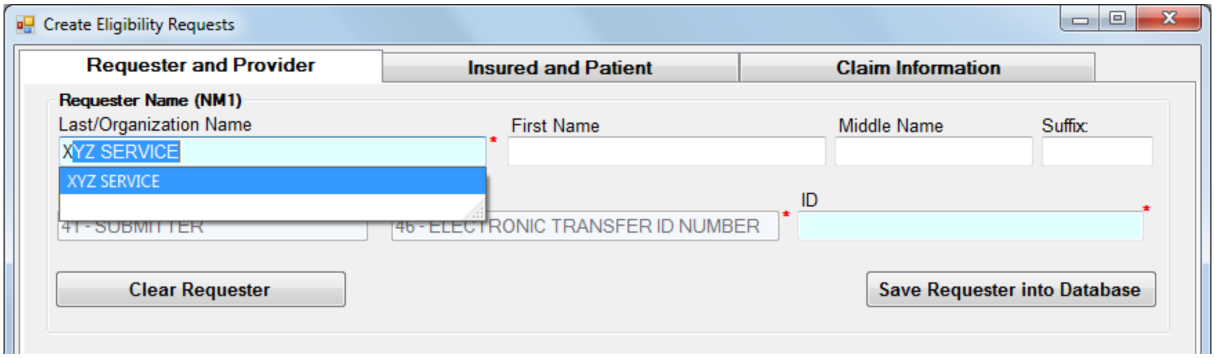
The first tab of the screen contains the requester, provider, and info source information. You have to enter information about the requester and provider only once and then you can save the information receiver or service provider information for future use by clicking on the "Save Receiver into Database" or "Save Provider into Database" buttons. The Information Source is filled with your previously configured Trading Partners.



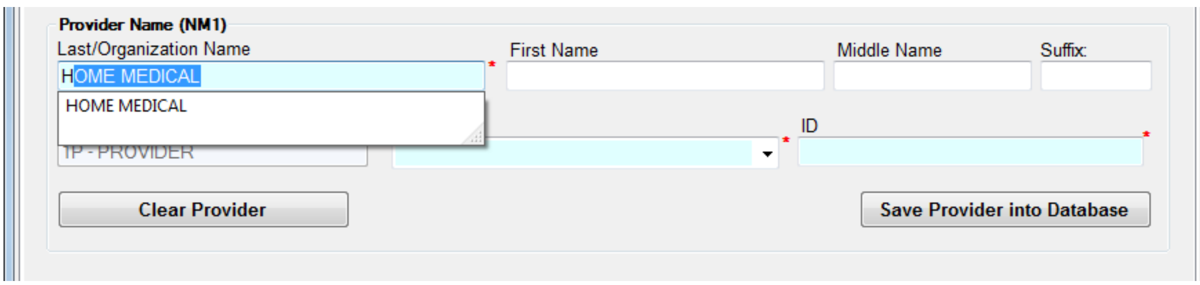
Filled receiver and provider tab. Save buttons are highlighted.

The first block of information contains the information requester's name and identification. The second block contains the service provider's name and identifier. We recommend that you enter the requester and provider information as completely as possible and save it so you don't have to enter any more information when you recall the requester for another request.

After saving, you need only input a few letters of the requester or provider's Last/ Organization Name or ID and the form will fill automatically with the saved information.



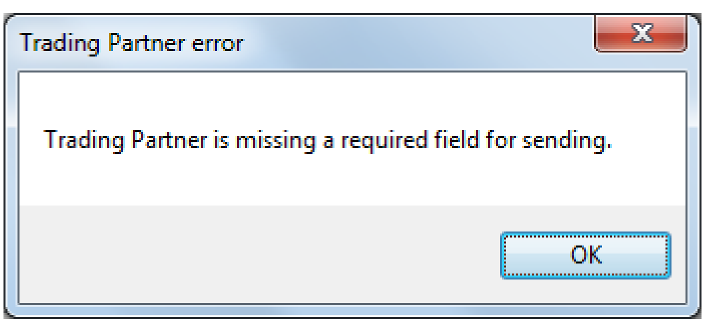
After saving a Requester, you can fill the entire form with a Requester's information with only the Name or ID.



After saving a Provider, you can fill the entire form with a Provider's information with only the Name or ID.

To edit a requester or provider's saved information, enter the name or ID to auto-fill the form, edit the necessary information, and click the associated Save button once more. The new fields will overwrite the older entry.

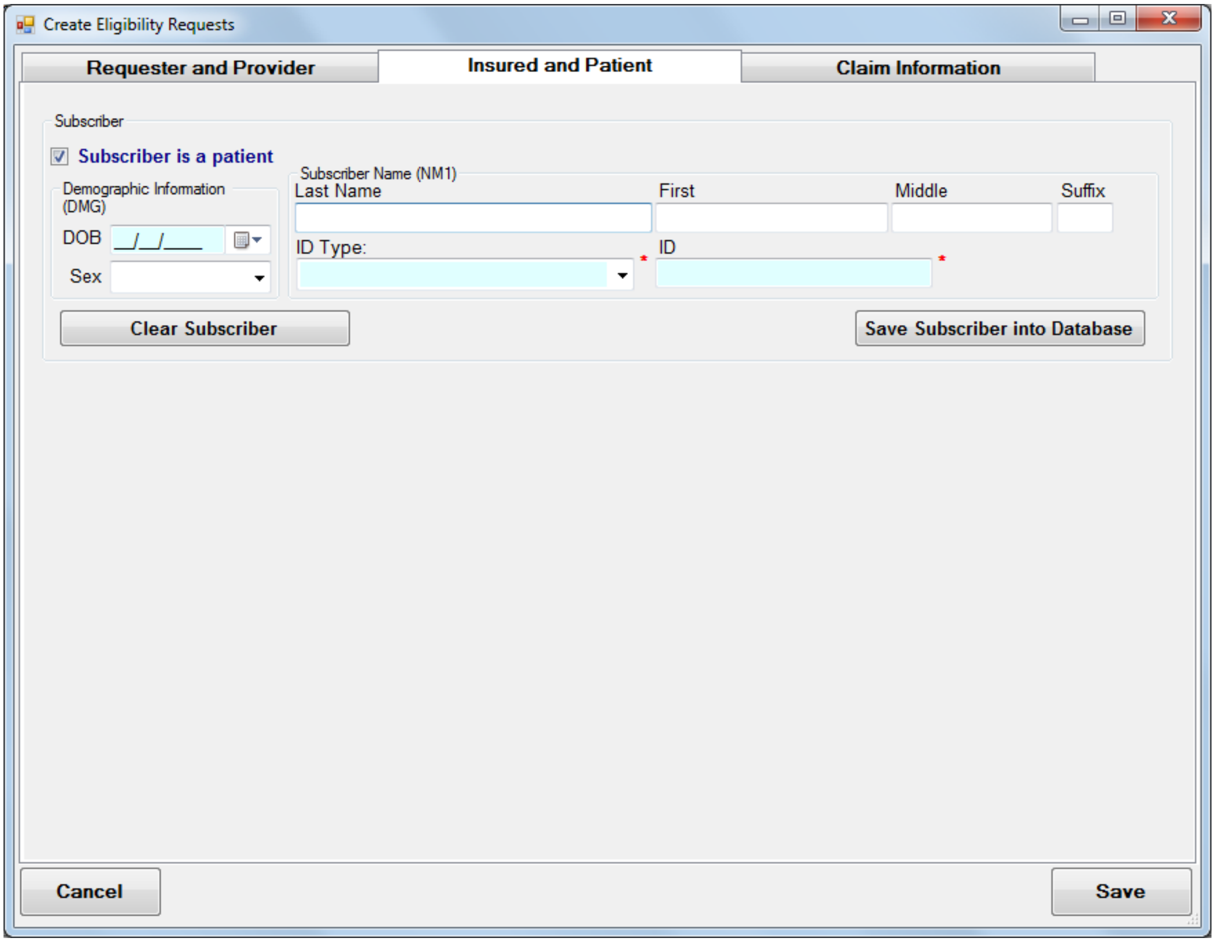
A claim cannot be saved if lacking a required field. A message similar to the one below will be shown. To save the claim status request, fill in all the required fields and click "Save".



Missing required field error for an empty Trading Partner field.

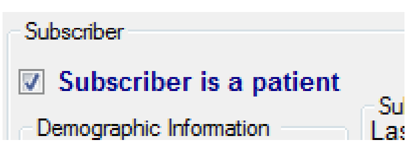
4.3.3 Entering Patient Information

The second tab on the manual entry form contains the insured and/or patient information.



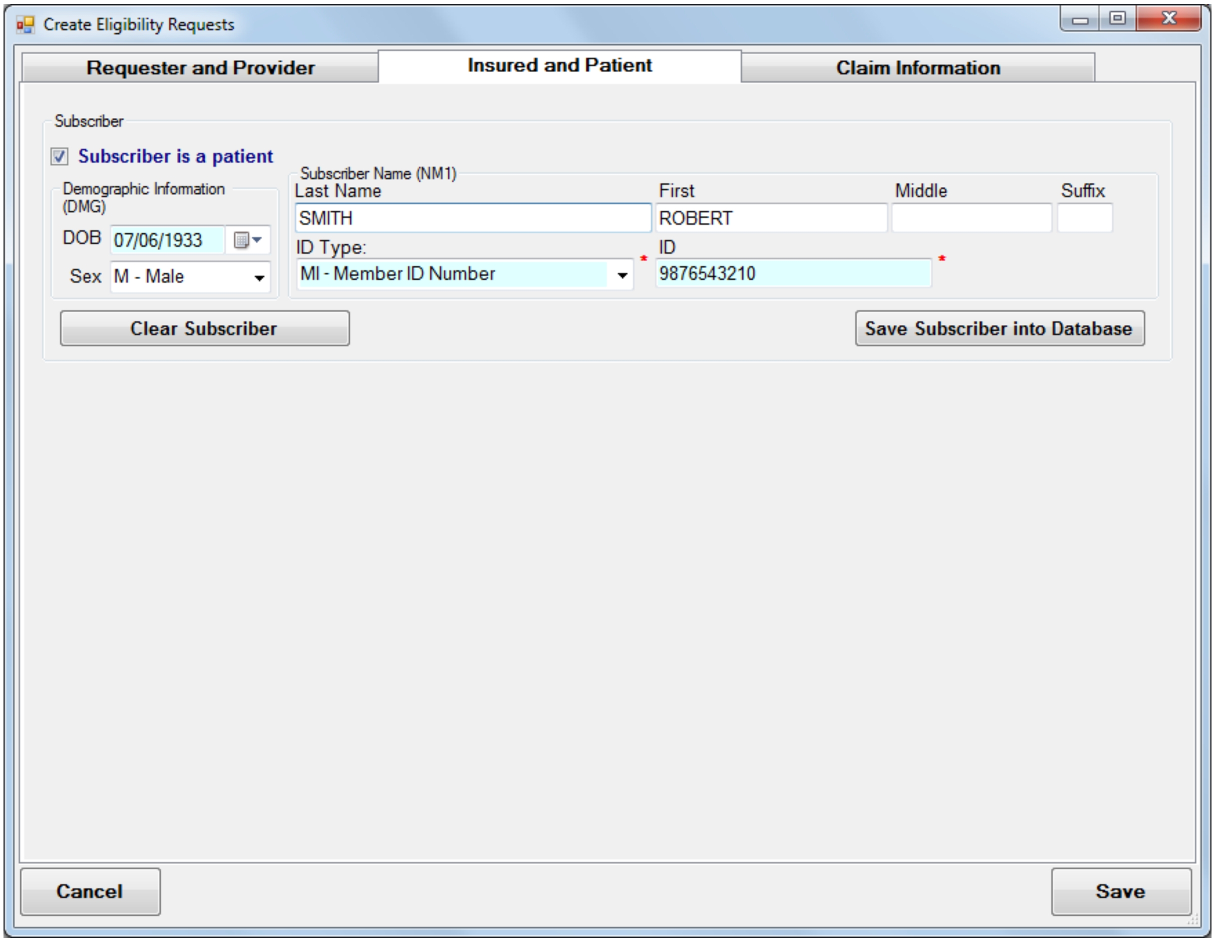
The patient information tab describes a Subscriber and/or dependent.

The subscriber is set as the patient by default. But if the patient is a dependent to the insured, then another tab with the dependent information will become visible.



The check mark indicates that the subscriber is the patient

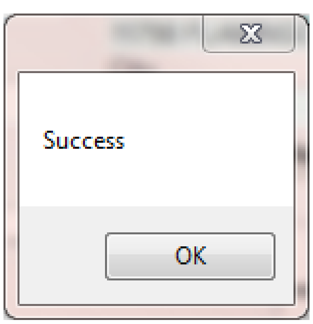
Let's take a look at a completed Subscriber screen



Filled patient tab. Subscriber is the patient.

To the right of the 'Subscriber is Patient' check box is the name and id of the insured. Below the check box is a block with demographic information, namely the patient's date of birth and gender.

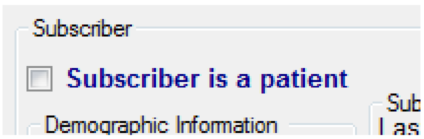
Like the Requester tab, the Patient tab allows you to save a subscriber's information for future use when you click on the 'Save Subscriber into Database' button. Once the record is saved you will see a positive affirmation of the save event.



Saving the Subscriber information

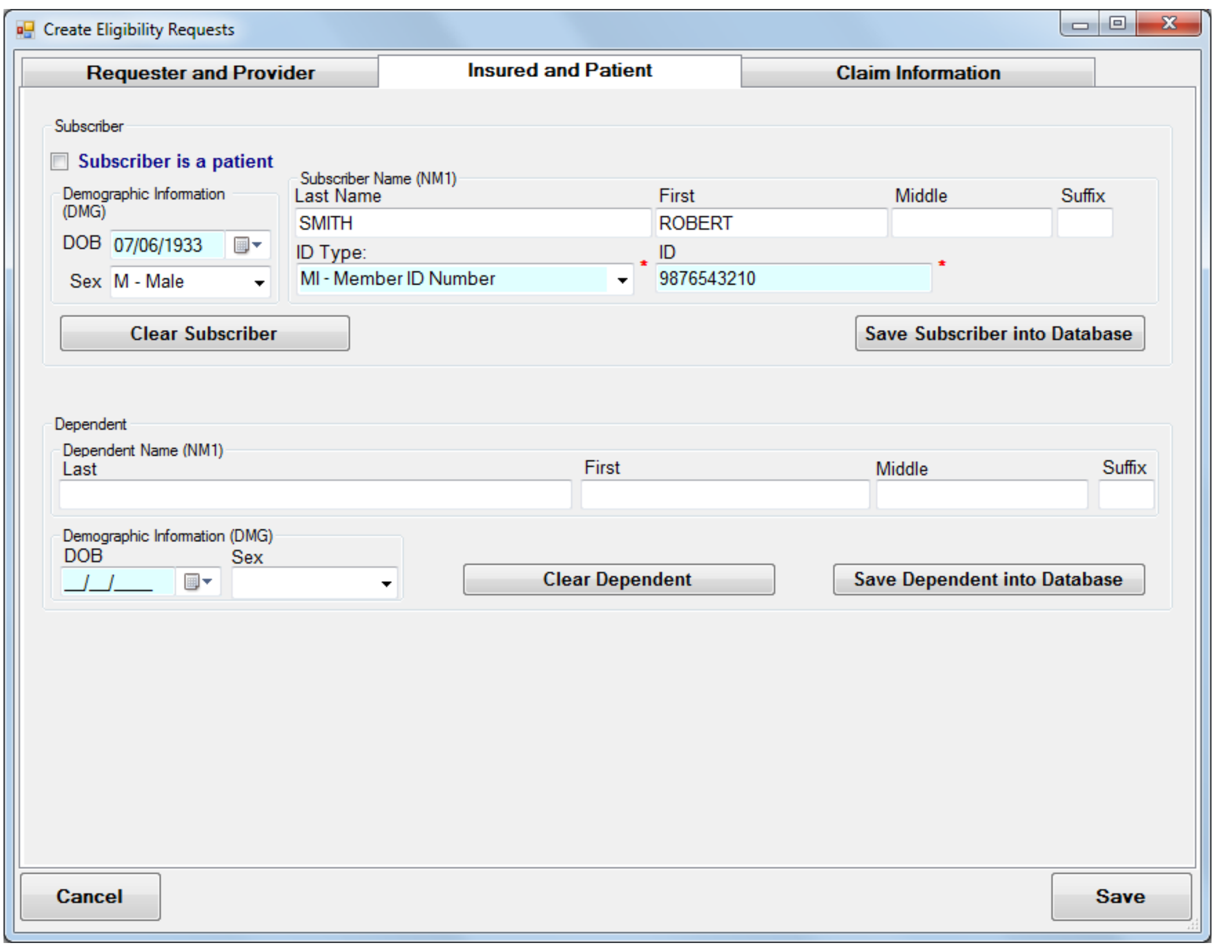
Entering Dependent Information

To request Claim Status information about a subscriber's dependent, first uncheck the "Subscriber is a patient" check box.



Unchecking the Subscriber is Patient check mark

Unchecking "Subscriber is a Patient" will present the dependent fields, where you can fill in a dependent's information. This field block, like the subscriber field block, also has a button to save the dependent information into a database and his/her info can be auto-filled the next time around.

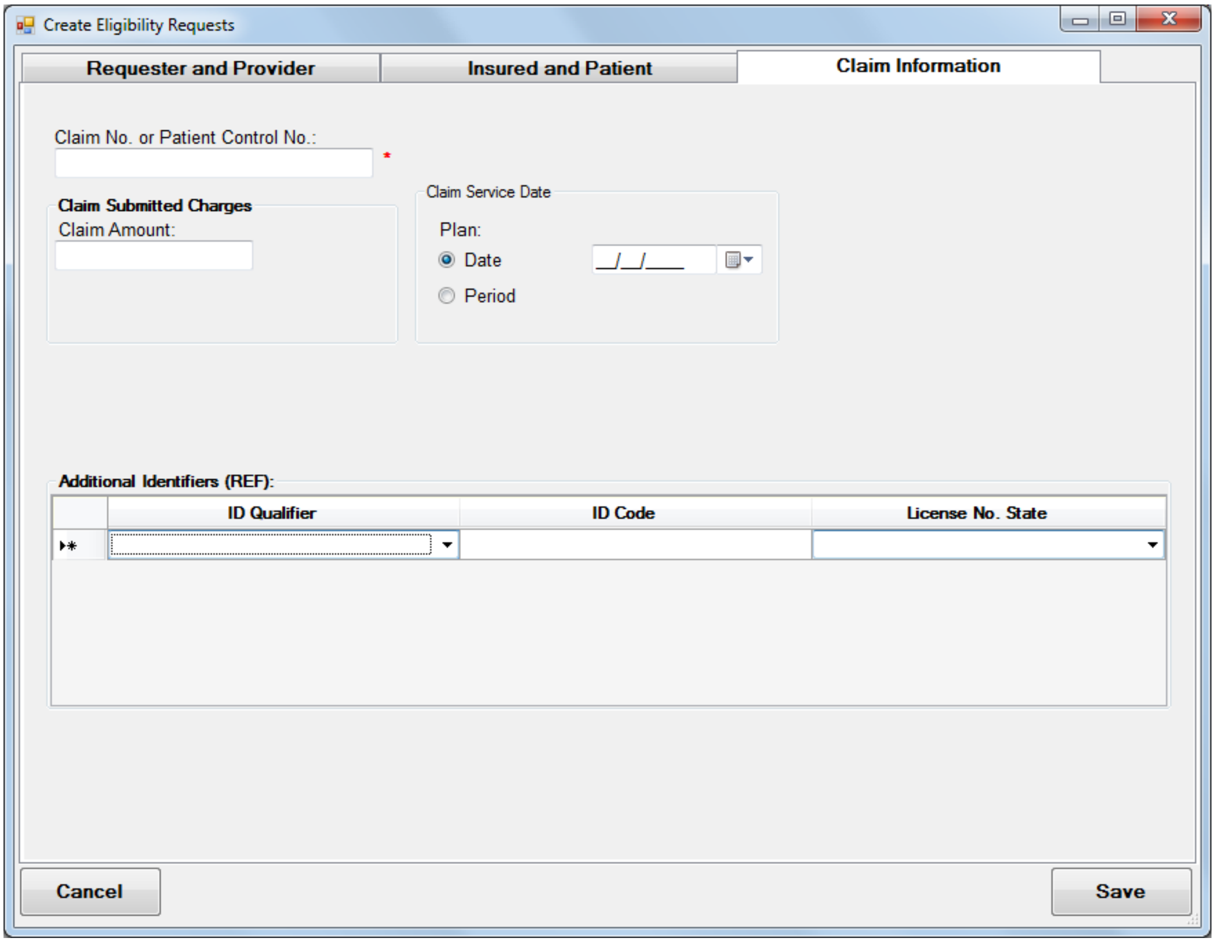


Blank Dependent entry fields.

The field entry and save procedure for the dependent is the same as for the subscriber.

4.3.4 Entering Claim Information

The third tab of the manual entry form contains the requested Claim Status information.

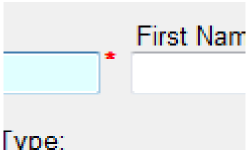


Claim Information tab.

Any new Claim Status request needs a Claim Number. The Claim Amount field is expressed in cents.

4.3.5 Saving the Manual Request

To send your new or edited request, you must first save it. The minimum required fields for a complete Claim Status request are marked with a red asterisk. They are the Requester's Last/Organization Name and ID, a Provider's Last/Organization Name, ID Type and ID, A Subscriber's ID Type and ID, and a Claim Number.



An asterisk marks a field as required.

After saving a Claim Status request, it will be added to the workgrid. This new row will present the Requester, the Subscriber, the Dependent (if any), the Subscriber's ID, and a symbol denoting the status of this particular request.

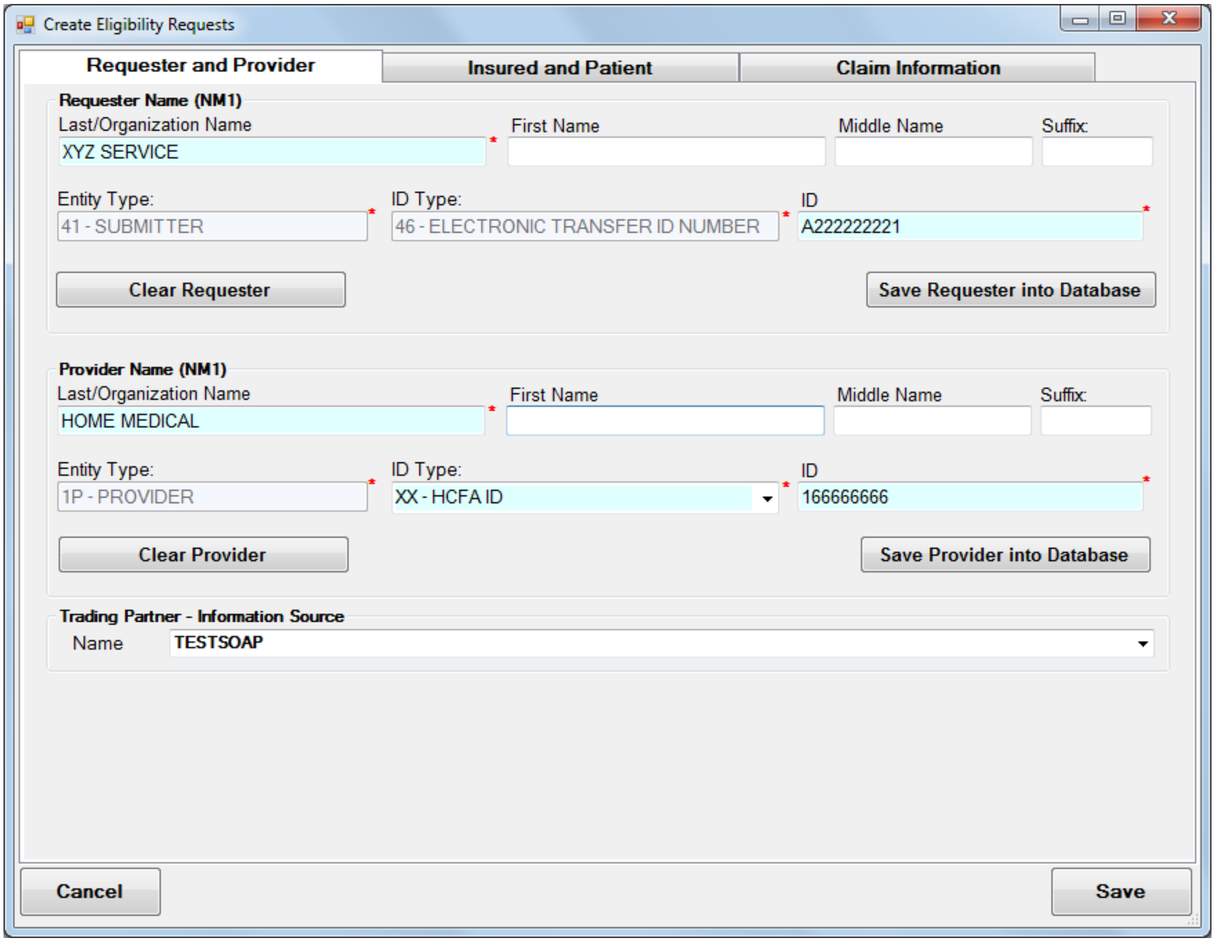
A new Claim Status request.

If you have the EDI Exchange module licensed and configured in addition an EDI compliance check will be performed. This check makes sure that your information is complete and in the right format when you compile the request information into the 270 request transaction. The results will be displayed on the rightmost column. A checkmark denotes the compliance check has passed, while a red crossed circle flags a request did not pass the compliance check.

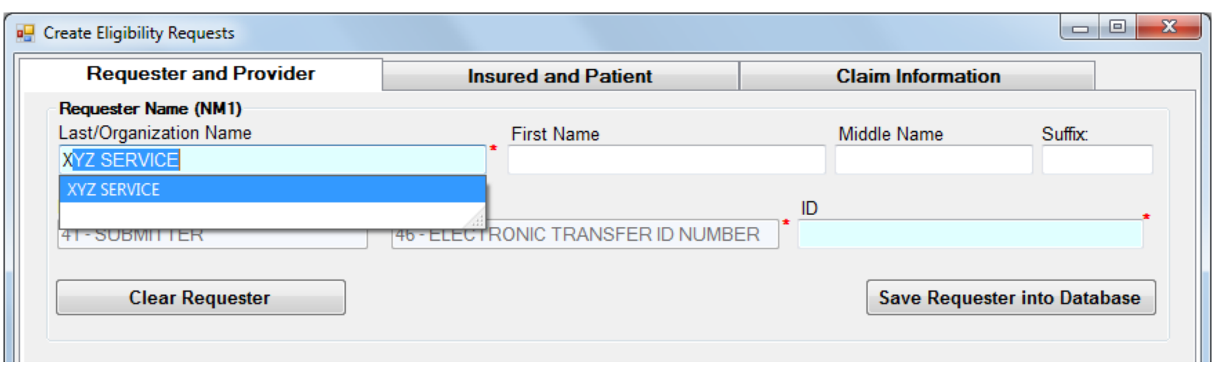
Example of Claim Status requests after a compliance check. The bottommost request passed, the request above it failed the compliance check.

4.3.6 Storing Requesters and Providers

Saving a request stores all the information in the request to the database. To avoid entering the same Requester, Provider, Subscriber, or Dependent multiple times, you can save them separately into their own database tables.



After saving a Requester, Provider, Subscriber, or Dependent to your Database, you only need to type a few letters of his/her/its Last Name or ID number to auto-fill the form.

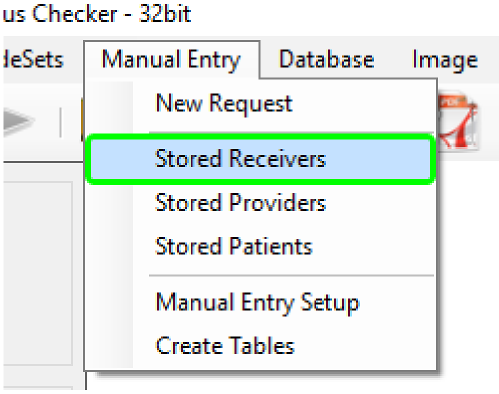


Selecting a previously saved Requester, Subscriber, or Dependent will fill the respective form for you.

4.3.7 Editing Requesters/Receivers

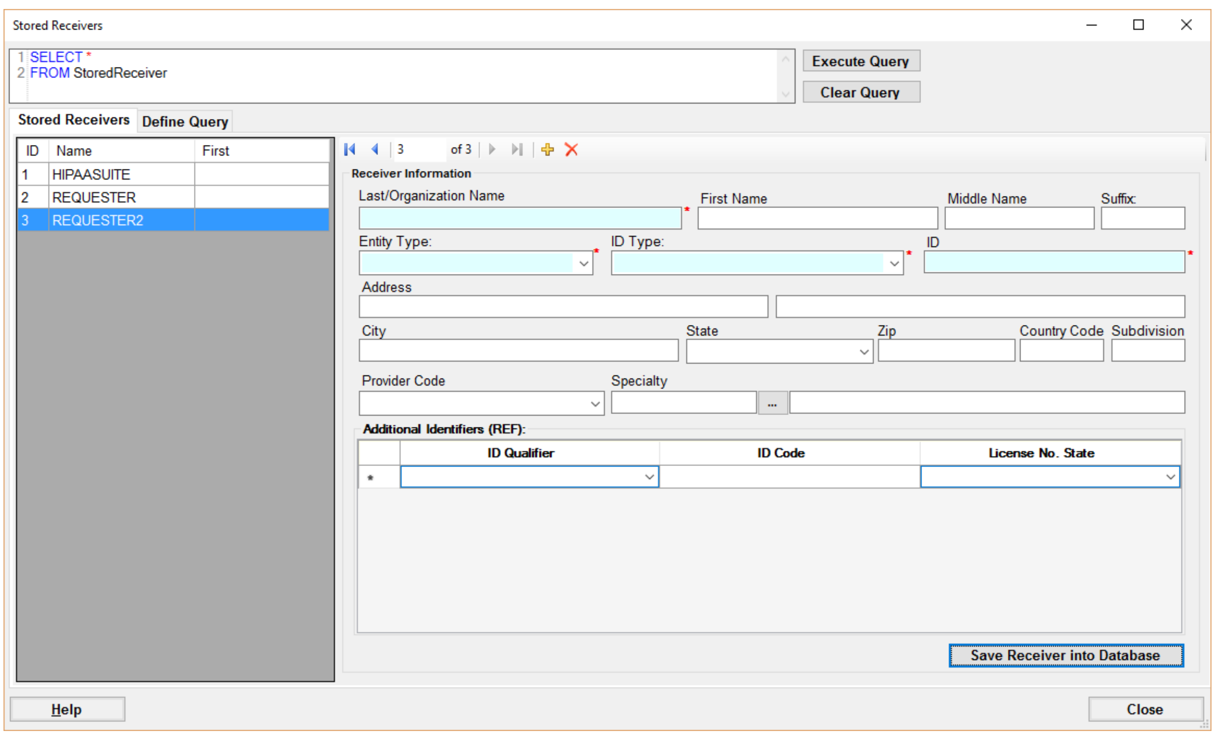
To access all currently stored Receivers click on the *Stored Receivers* option under the

Manual Entry menu.



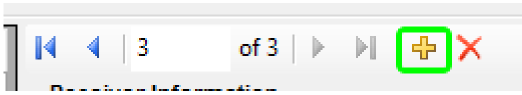
Manual entry menu

Clicking *Manual Entry* ▸ *Stored Receivers* will open the *Stored Receivers* editing window, where all receivers stored in the database are available for editing. Receivers can also be added or removed from the database.



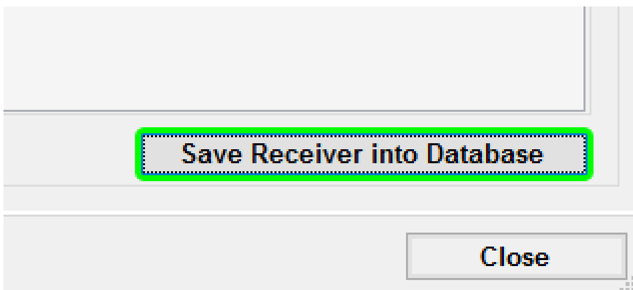
Adding a new Requester/Receiver

To add a new receiver, click the yellow plus symbol on the navigation bar



Adding a new receiver

The Receiver fields will be cleared. Fill in at minimum the required fields marked by a red asterisk. To save the new receiver to the database, click the *Save Receiver into Database* button.

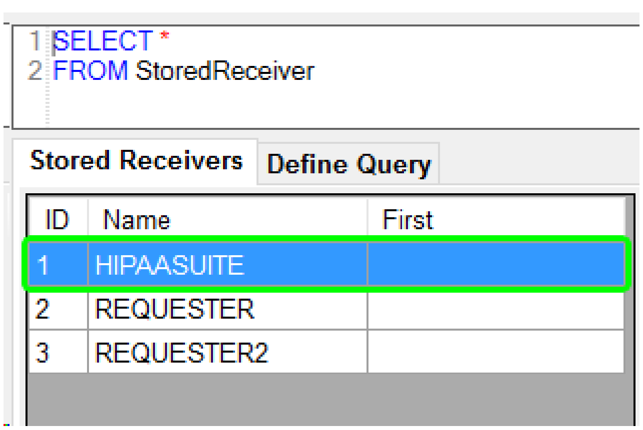


Saving a receiver

The new receiver will now appear in the list of receivers to the left of the screen.

Editing a Requester/Receiver

To modify an existing receiver, select the receiver on the list to the left of the screen. To narrow the selection of receivers, the query in the top of the screen can be modified and run again to populate the stored receivers list with a different set of receivers.

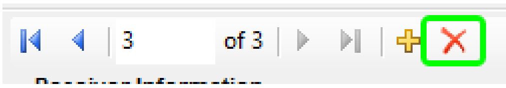


Stored receiver list

The selected receiver's details will be loaded into the form. These can now be edited. Clicking the *Save Receiver into Database* button will save any changes into the database.

Deleting a Requester/Receiver

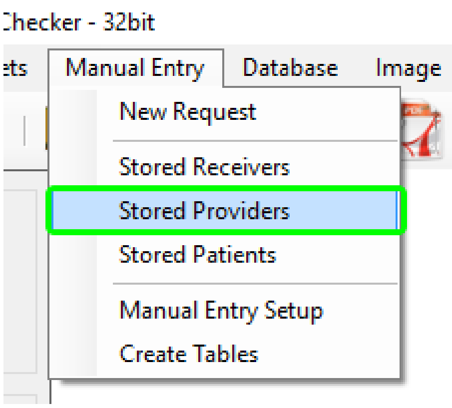
To remove a receiver from the database, select the receiver on the list to the left of the screen, then click the red 'X' in the navigation bar.



Delete button in navigation bar

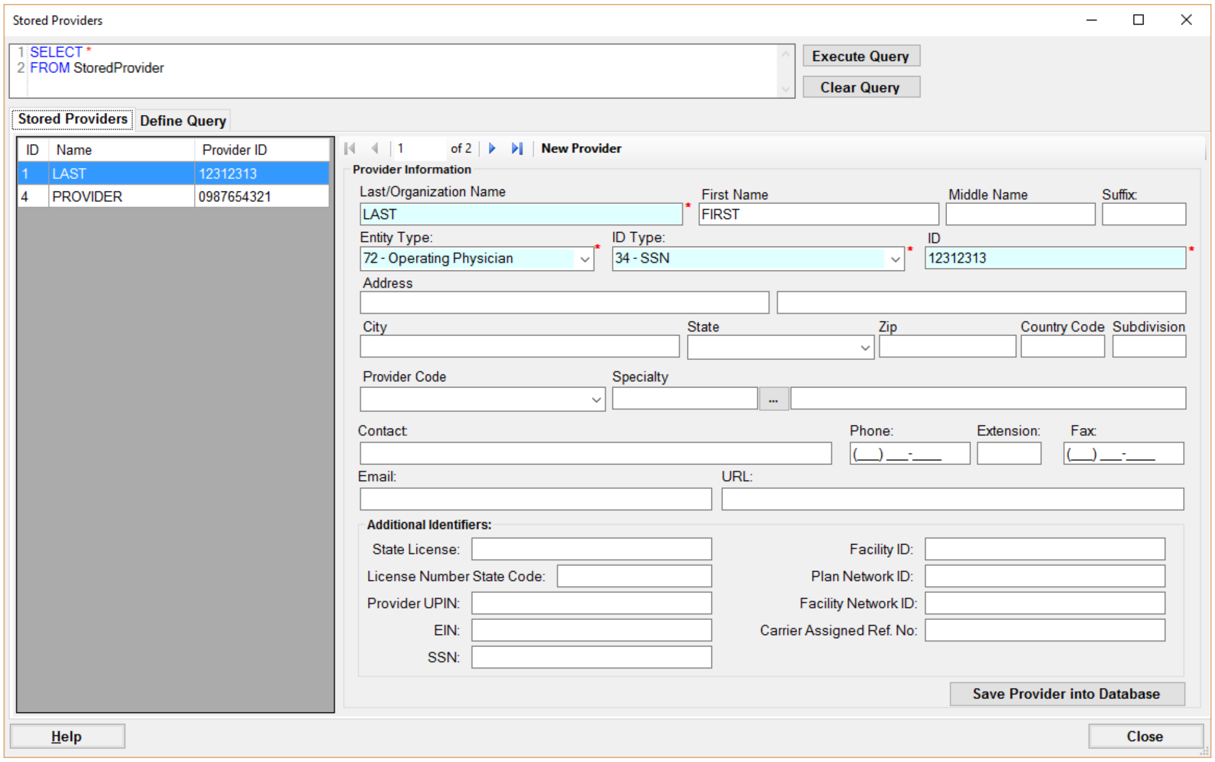
4.3.8 Editing Providers

To access all currently stored Providers click on the *Stored Providers* button under the *Manual Entry* menu.



Manual entry menu

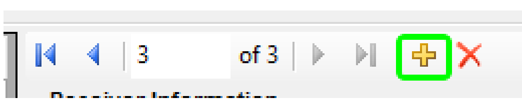
Clicking *Manual Entry* ▸ *Stored Providers* will open the *Stored Providers* editing window, where all providers stored in the database are available for editing. Providers can also be added or removed from the database.



Stored Providers editing window

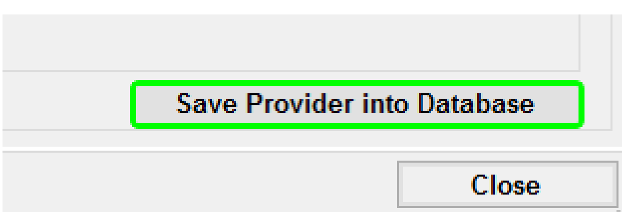
Adding a new Provider

To add a new provider, click the yellow plus symbol on the navigation bar



Adding a new provider

The Provider fields will be cleared. Fill in at minimum the required fields marked by a red asterisk. To save the new provider to the database, click the *Save Provicer into Database* button.

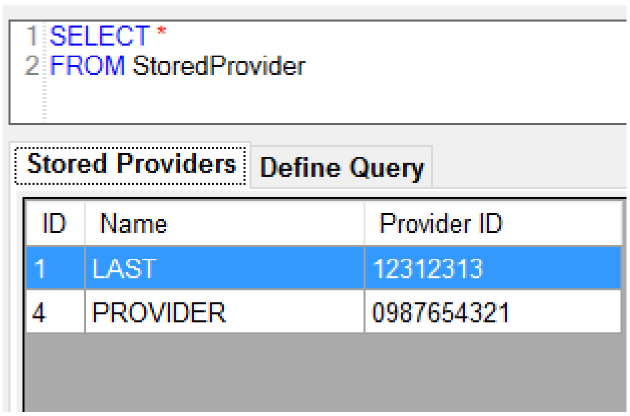


Saving a provider

The new provider will now appear in the list of providers to the left of the screen.

Editing a Provider

To modify an existing provider, select the provider on the list to the left of the screen. To narrow the selection of providers, the query in the top of the screen can be modified and run again to populate the stored providers list with a different set of providers.

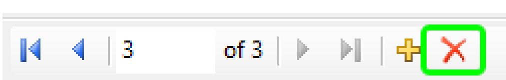


Stored providers list

The selected provider's details will be loaded into the form. These can now be edited. Clicking the *Save Provider into Database* button will save any changes into the database.

Deleting a Provider

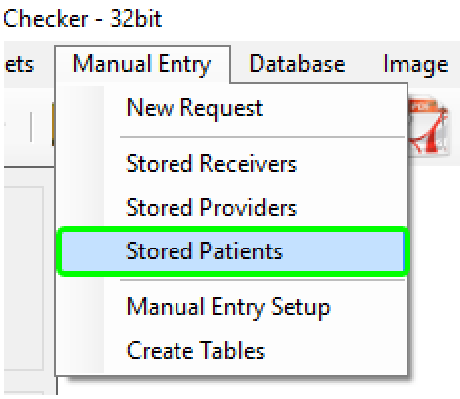
To remove a provider from the database, select the provider on the list to the left of the screen, then click the red 'X' in the navigation bar.



Delete button in navigation bar

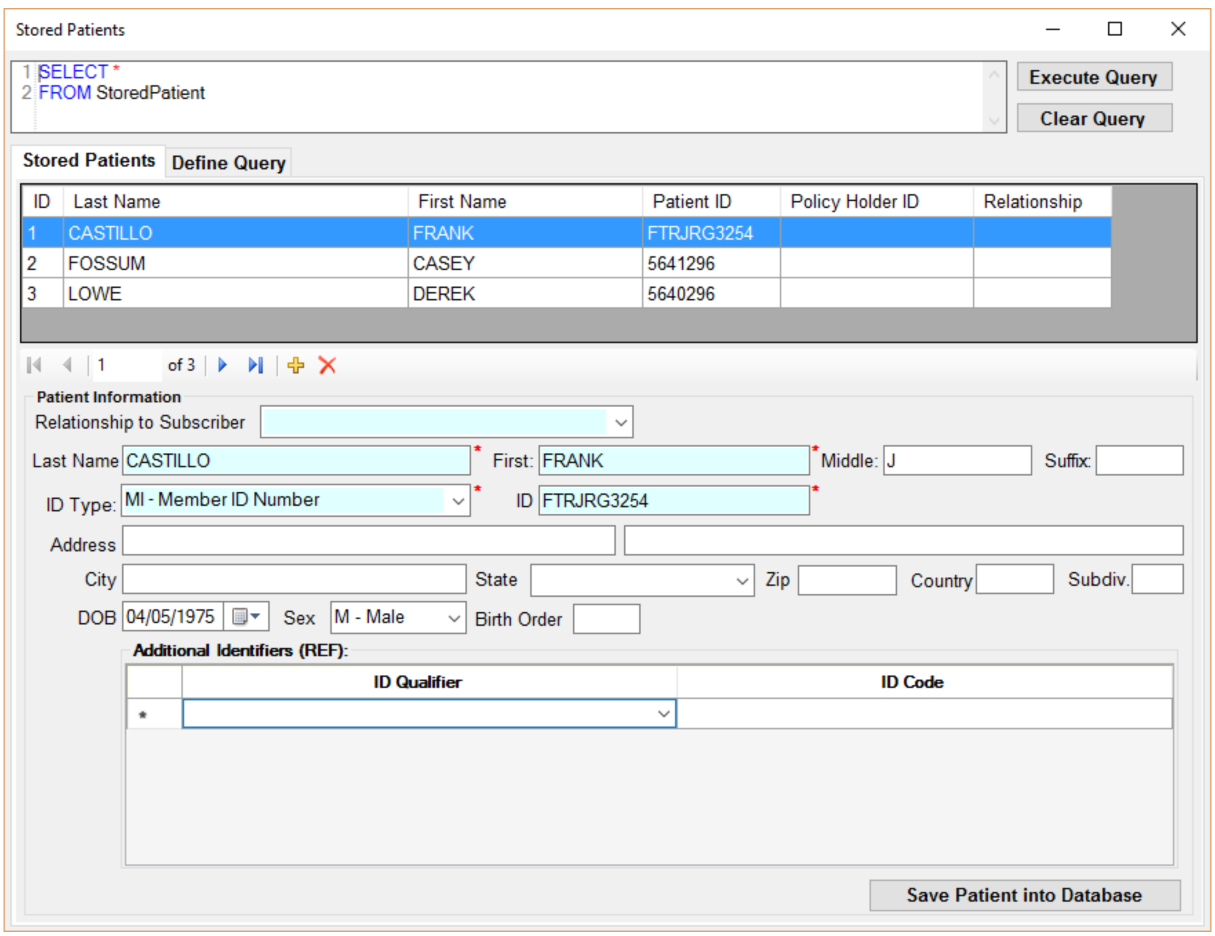
4.3.9 Editing Patients

To access all currently stored Patients click on the *Stored Providers* button under the *Manual Entry* menu.



Manual entry menu

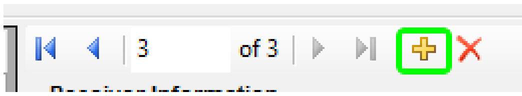
Clicking *Manual Entry* ▸ *Stored Patients* will open the *Stored Patients* editing window, where all Patients stored in the database are available for editing. Patients can also be added or removed from the database.



Stored Patients editing window

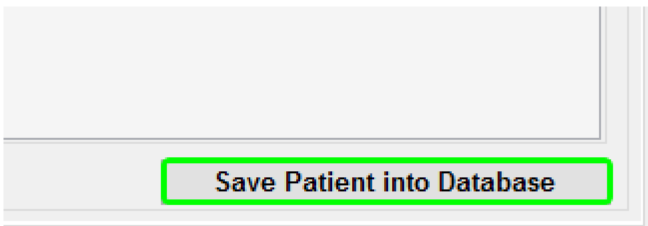
Adding a new Patient

To add a new Patient, click the yellow plus symbol on the navigation bar



Adding a new Patient

The Patient fields will be cleared. Fill in at minimum the required fields marked by a red asterisk. To save the new Patient to the database, click the *Save Provicer into Database* button.

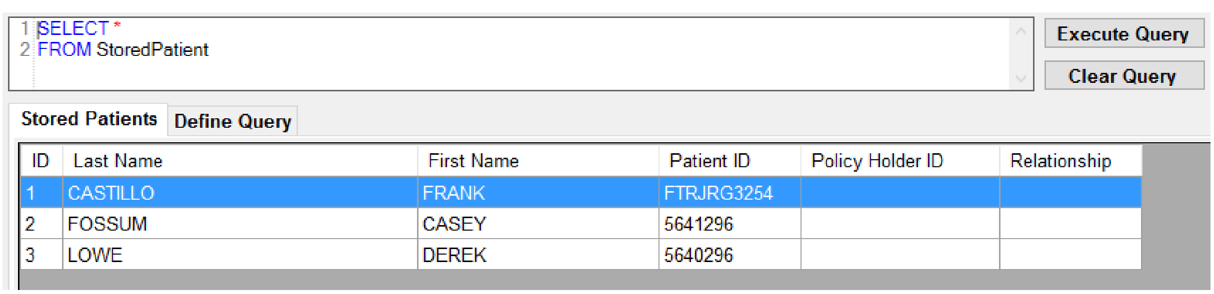


Saving a Patient

The new Patient will now appear in the list of Patients under the query window.

Editing a Patient

To modify an existing Patient, select the Patient on the list under the query window. To narrow the selection of Patients, the query in the top of the screen can be modified and run again to populate the stored Patients list with a different set of Patients.

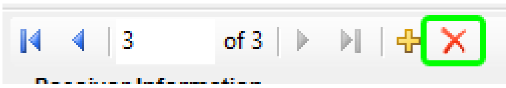


Stored Patients list

The selected Patient's details will be loaded into the form. These can now be edited. Clicking the *Save Patient into Database* button will save any changes into the database.

Deleting a Patient

To remove a Patient from the database, select the Patient on the list under the query window, then click the red 'X' in the navigation bar.

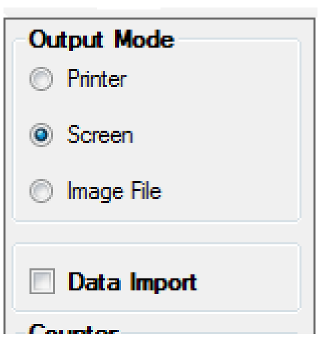


Delete button in navigation bar

4.4 Viewing Requests

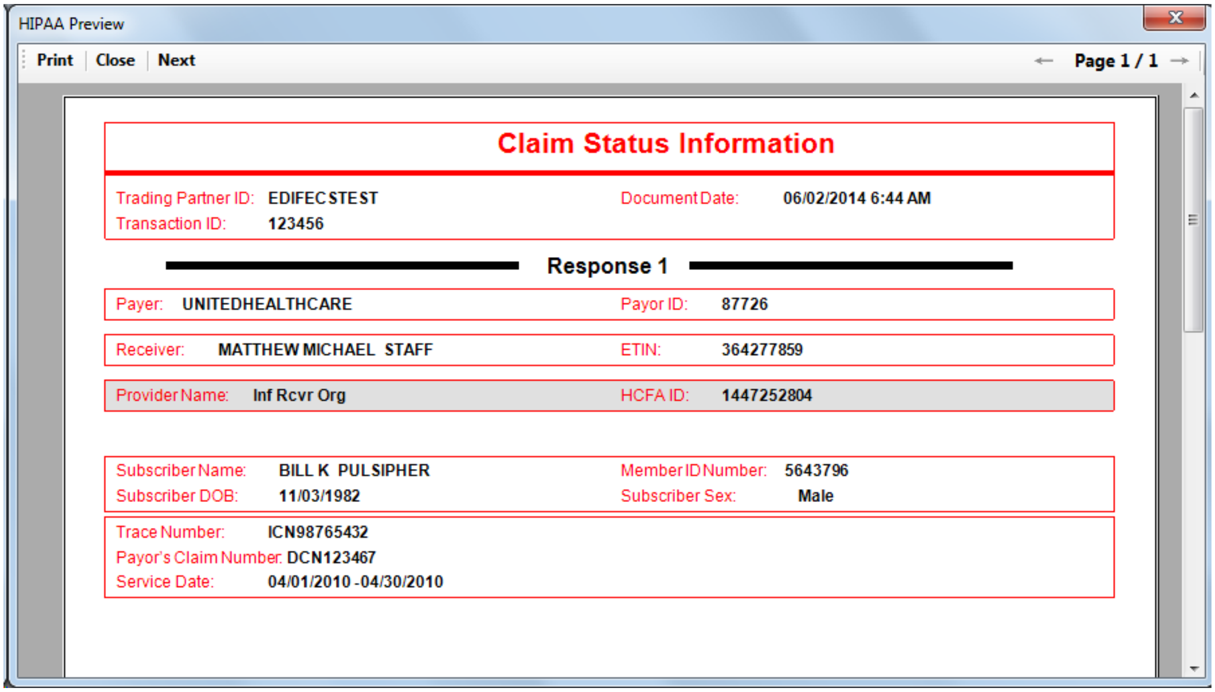
EDI is notoriously hard to read and understand. For that reason we developed forms that show the complete content of the file, translate cryptic codes into their description and help even non EDI experts to read and understand the data.

When we open an 270 file we have as an output mode option 'Screen'.



Screen output mode selected.

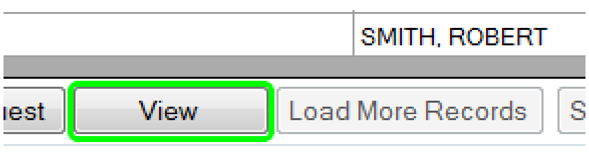
So when we select this mode and click on Run, the file is parsed and displayed on screen.



The result of the output mode 'Screen'

Here we can see all the information in the file, from the file header to the requester, the payer, the subscriber and claim number for the requested claim's status.

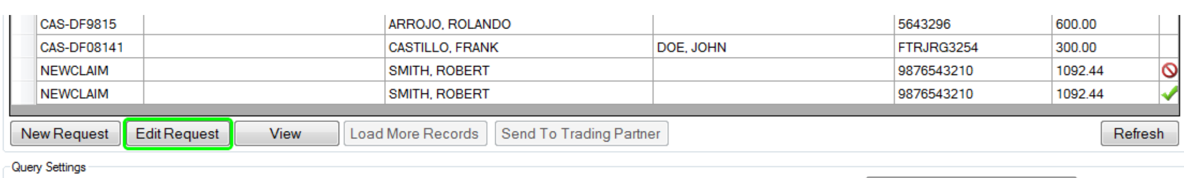
Requests can also be viewed from the workplace. After opening the workplace, select the desired Claim Status request and click the "View" button.



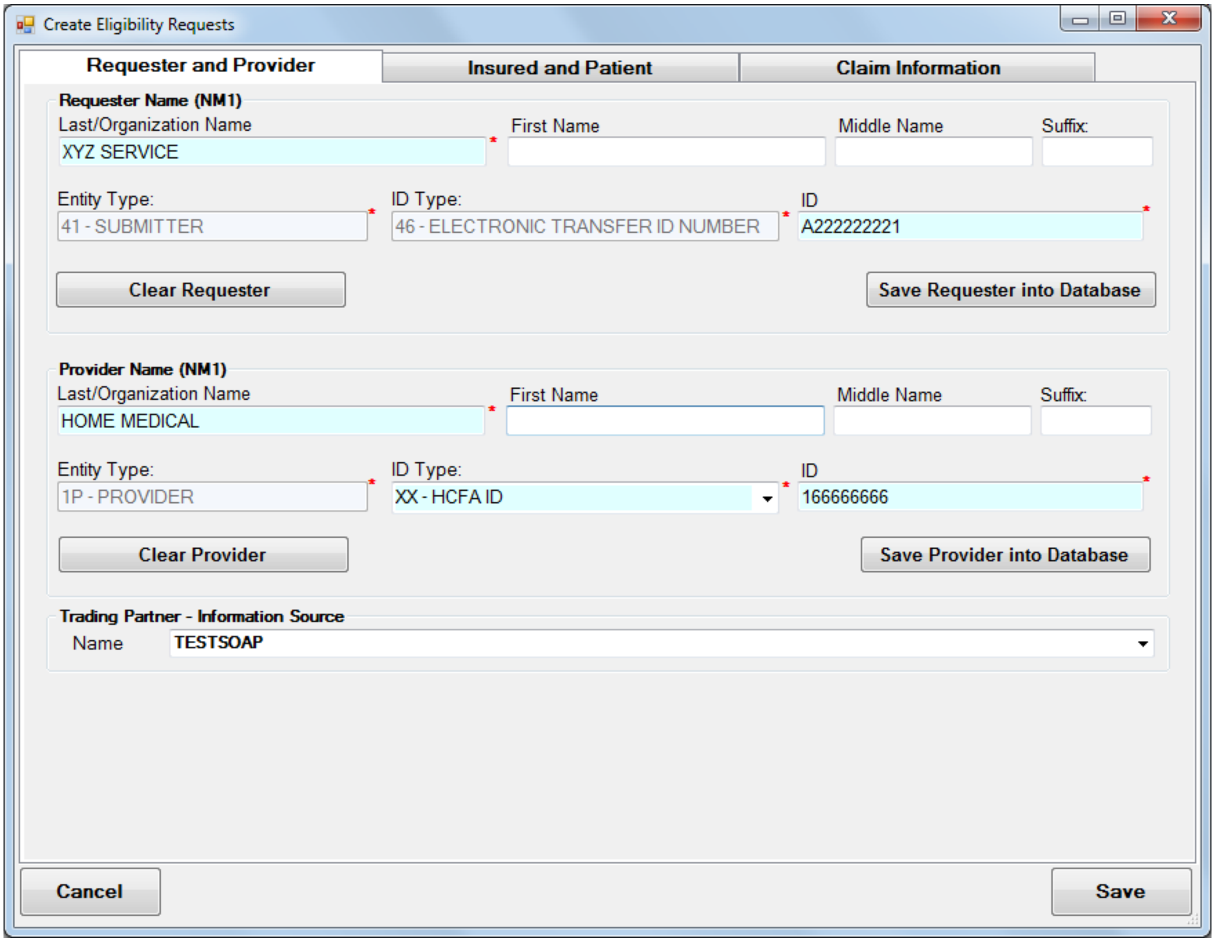
The workplace's "View" button will also lead you to the screen output mode for a selected request.

4.5 Editing Requests

Request records that are loaded into workplace grid can be edited to change information or whatever other reason there might be.



Highlight a row in the grid and press the 'Edit Request' button and the record will be loaded into the manual entry forms.

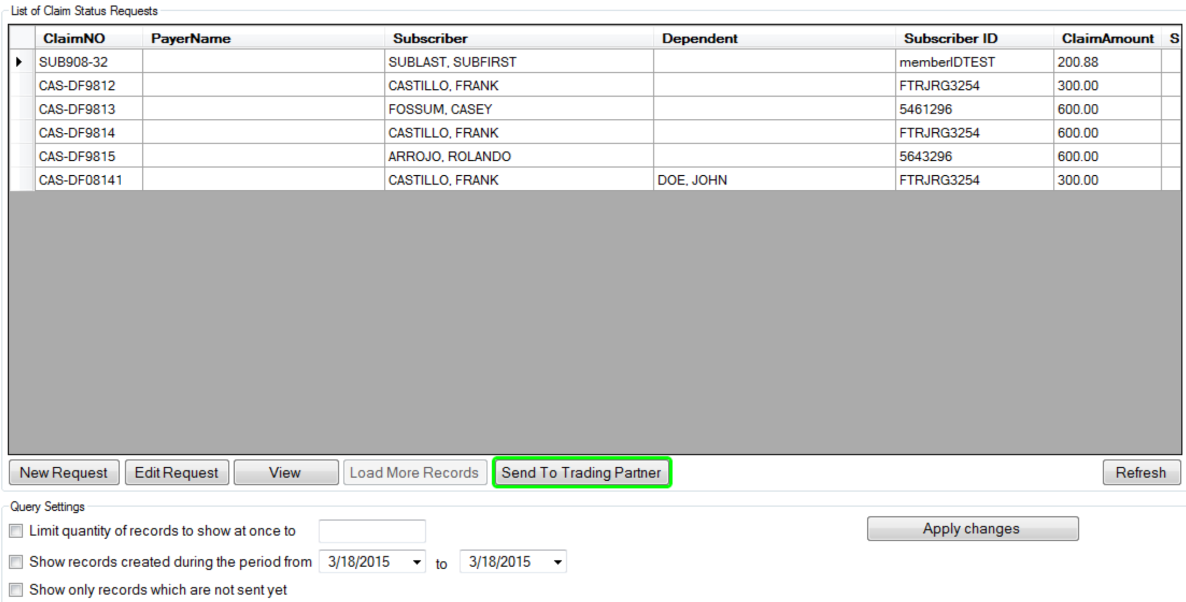


A Claim Status request loaded for editing.

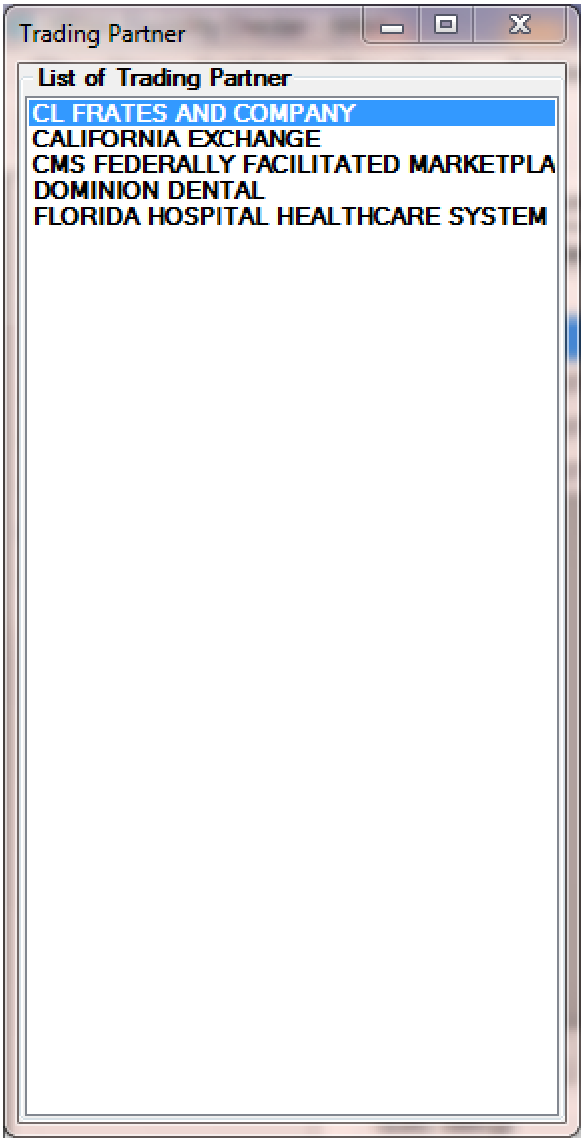
After saving the request, the record you are editing will be overwritten.

4.6 Creating 276 Files

Each row in the workplace represents a single EDI Eligibility request with a single subscriber or dependent. EDI files only make sense when we have a receiver for the file since in the very first segment, the ISA segment, there is a place for the receiver ID and qualifier. The Trading Partner is filled in while sending the request; you will be prompted to select a trading partner during the send process. Clicking "Send To Trading Partner":

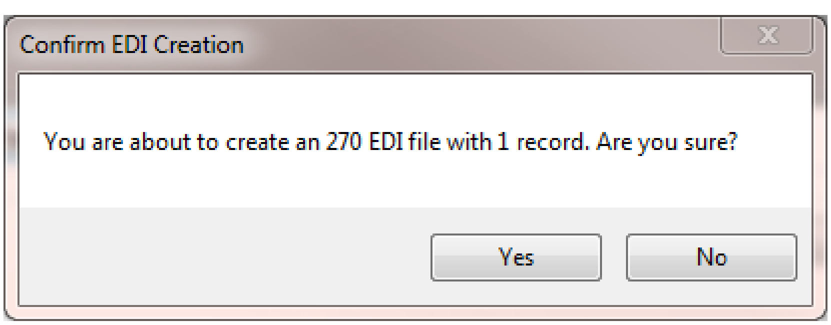


Clicking "Send To Trading Partner" will prompt you to select a saved Trading Partner to send the EDI request to:



The screen to select the trading partner

We double click and thereby select the trading partner you will be prompted once more to create the EDI file with the selected record after which the EDI request will be sent to the selected trading partner.

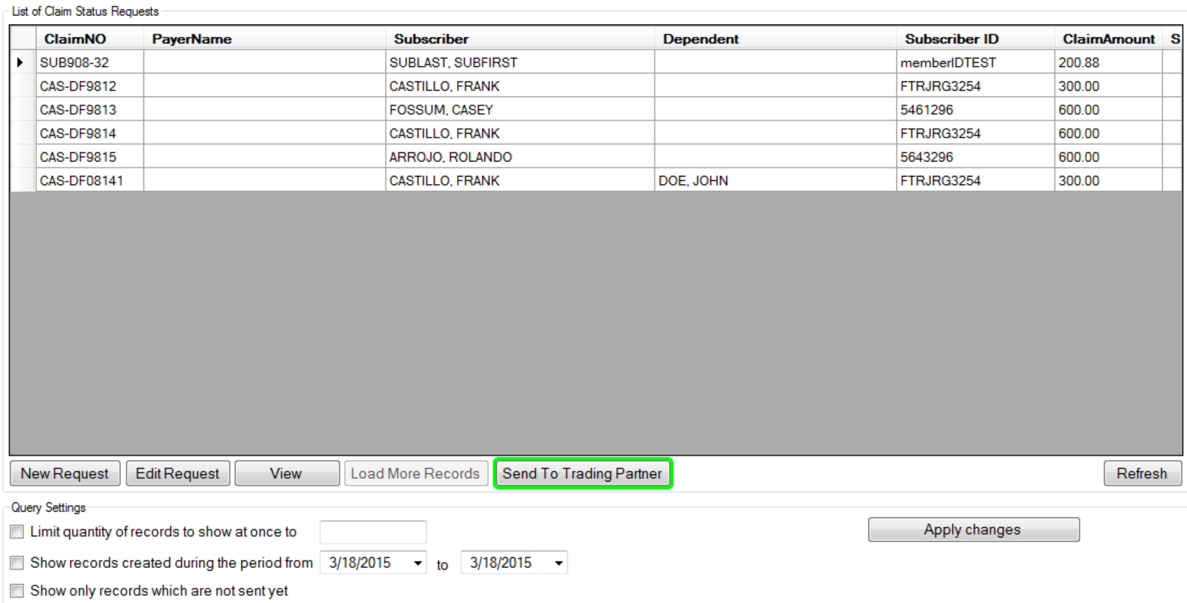


Confirming the creation of the file

At this point the EDI file has been written to the outbox and is being sent to the trading partner. The send process is described in greater detail in Sending 276 Requests.

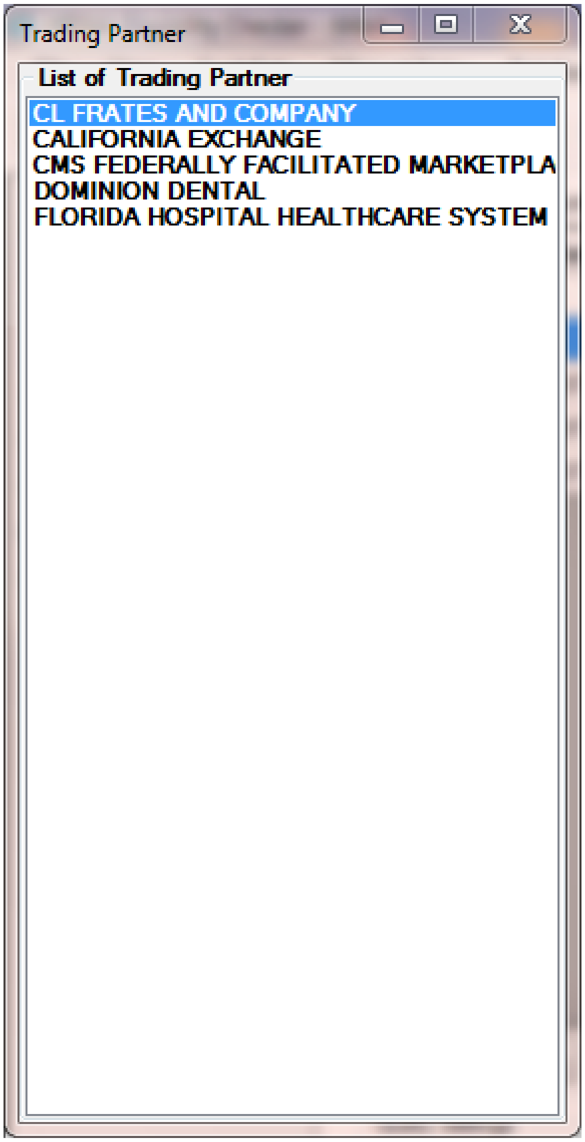
4.7 Sending 276 Requests

As covered in Creating 276 Files, clicking "Send To Trading Partner" will initiate the process of sending a Claim Status request.



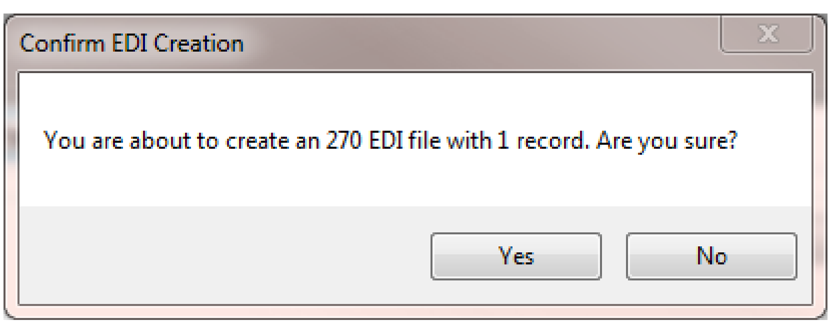
The workplace grid with a record highlighted, emphasis is placed on the 'Send to Trading Partner' button

Clicking "Send To Trading Partner" will prompt you to select a saved Trading Partner who will receive the EDI request. Double click the desired Trading Partner to select it.



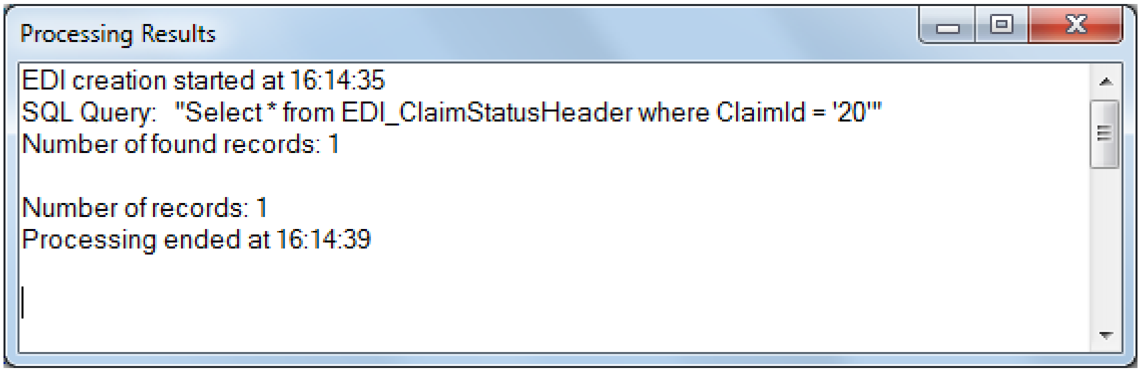
The screen to select the trading partner

We double click and thereby select the trading partner you will be prompted once more to create the EDI file with the selected record after which the EDI request will be sent to the selected trading partner.



Confirming the creation of the file

Next we see the process results window detailing the query used to build the record from the database and the processing status.



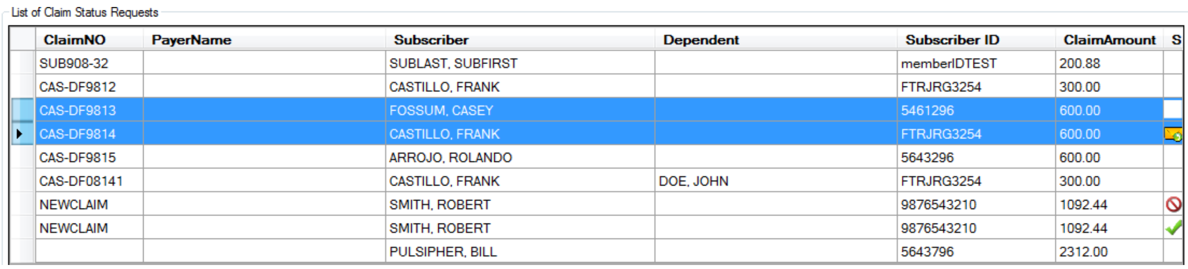
Process results of the file creation and sending to trading partner.

Upon receiving a response from the trading partner, the status icon is updated. In RealTime mode, which is used when sending single requests, the statuses after sending a request are:

- send failed  ,
- 999 received 
- response received 

Sending multiple requests

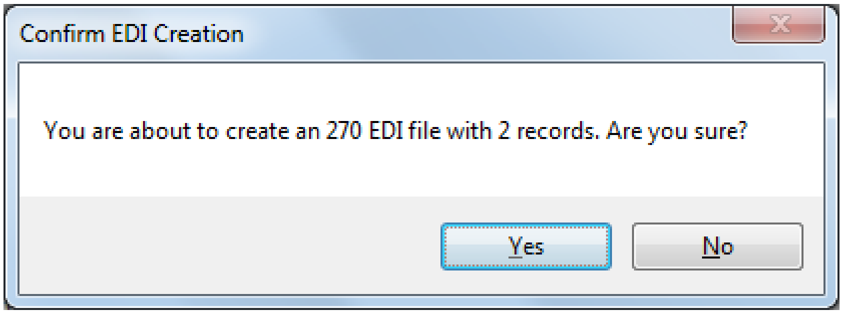
An EDI file with multiple transactions can be created by first highlighting multiple rows.


List of Claim Status Requests

ClaimNO	PayerName	Subscriber	Dependent	Subscriber ID	ClaimAmount	S
SUB908-32		SUBLAST, SUBFIRST		memberIDTEST	200.88	
CAS-DF9812		CASTILLO, FRANK		FTRJRG3254	300.00	
CAS-DF9813		FOSSUM, CASEY		5461296	600.00	
CAS-DF9814		CASTILLO, FRANK		FTRJRG3254	600.00	
CAS-DF9815		ARROJO, ROLANDO		5643296	600.00	
CAS-DF08141		CASTILLO, FRANK	DOE, JOHN	FTRJRG3254	300.00	
NEWCLAIM		SMITH, ROBERT		9876543210	1092.44	
NEWCLAIM		SMITH, ROBERT		9876543210	1092.44	
		PULSIPHER, BILL		5643796	2312.00	

The workplace grid with two records highlighted.

The rest is the same as sending a single request. Click on "Send to Trading Partner" to build and send the EDI file. By selecting multiple rows, an EDI file with multiple transactions is created and sent to the Trading Partner selected in the method assigned during the Trading Partner's setup. The EDI creation confirmation prompt will present the number of transactions to be created. If the Trading Partner's selected transfer mode is MIME or SOAP, the file will be sent in Batch Mode.

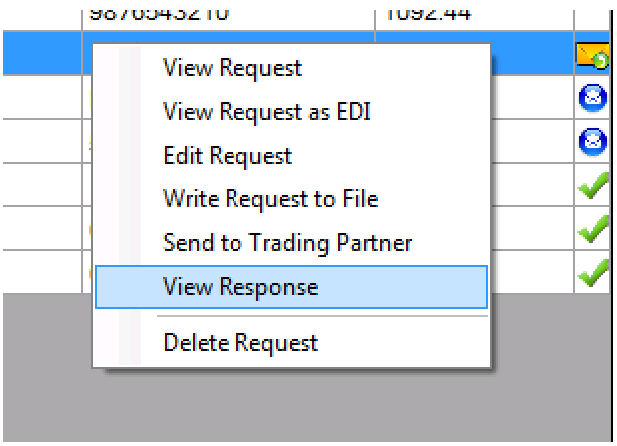


Confirming the creation of the file

Clicking "yes" will build the 276 EDI request and send it. Afterwards the process window will be shown. If the Trading Partner's send method is SOAP or MIME, Claim Status Checker will send a SOAP or MIME EDI request in BatchMode. Batch mode requests do not have to be processed until the next business day.

4.8 Receiving 276 Response files

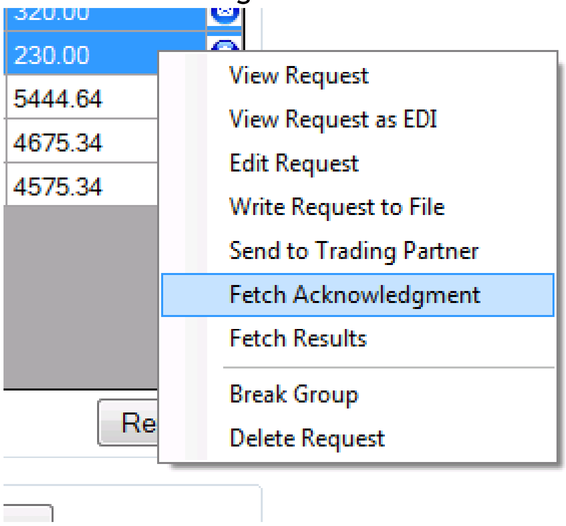
Requests made from a single row in the workplace are sent in RealTime mode. A response will usually be received in under 20 seconds. Upon receiving a response, double-click the row or right-click it and select "View Response" to view the response file.



View Response right-click menu option

Requesting ACK

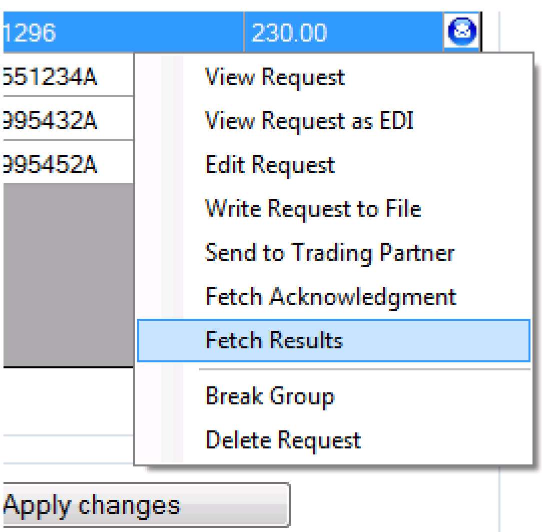
If a request group was sent in batch mode, an acknowledgment for the group may be requested. The 999 ACK file should be ready no later than an hour after submission. To request an ACK for a request sent in batch mode, right-click the request row and select "Fetch Acknowledgment"



Fetch Acknowledgment right-click menu option

Requesting Response

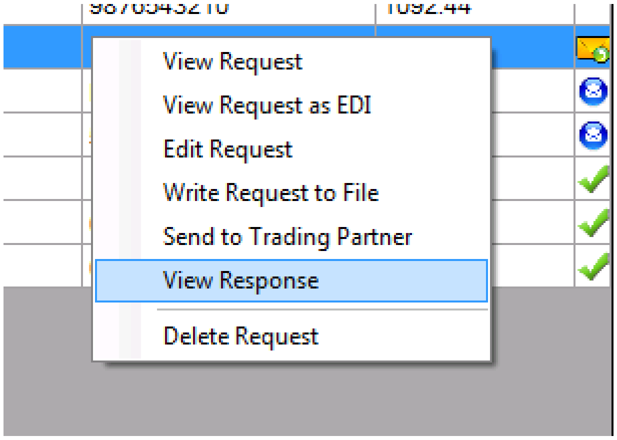
Requesting a response for a batch claim status is similar to requesting an acknowledgment. A response should be ready within one business day of sending a request and is requested by right-clicking any of the relevant batch rows and clicking on the "Fetch Results" option.



Fetch Results right-click menu option

4.9 Viewing Responses

To view a response from a real-time or batch claim status request, double-click the row of the relevant claim status request or right-click it and select "View Response" to view the response file. A response for the selected request must have already been received.



"View Response" option of the right-click menu

5 Image Files

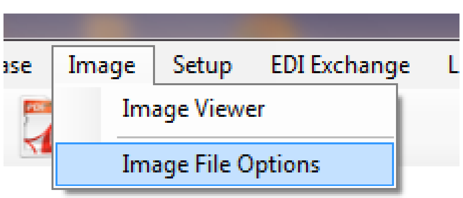
5.1 Creating Image Files

The HIPAA Claim Status Checker displays the content of EDI files as humanly readable forms on screen and those forms can be printed in the basic version of the software. An additional feature is to create image files in either TIFF and PDF format that can be stored and viewed at any time.

This feature is available at additional cost and can be added at any time.

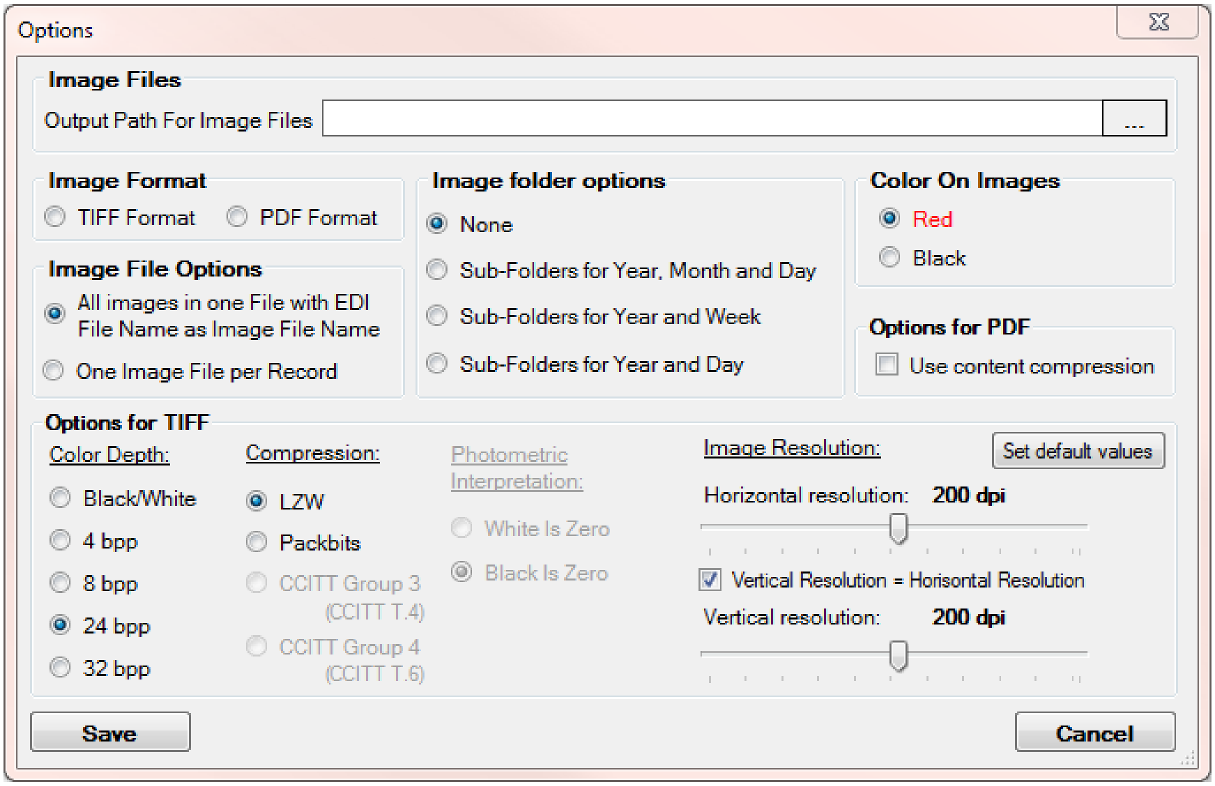
5.2 Image File Setup and Options

Under the menu item 'Image' we see two sub menus, 'Image Viewer' and 'Image File Options'



The image menus

When we click on Image File Options the following setup screen comes up



The Image File Options screen

You can configure the following options:

- Set the directory where image files will be saved
- Set image file and folder options
- Determine image format
- Determine options for PDF and TIFF files
- Determine the document background color for images

Read the detailed descriptions further.

3. Once you have finished editing the options, click "Save."

The settings are saved to the Windows registry and will be retained for the next time you run the program. Check your permissions to write to the registry if you encounter any problems with saving settings. Your administrator might help you.

Image Files

- **Output Path for Image Files** — Define the destination folder where the images will be stored. See also Creating Image Files.

Image Format

Choose whether to create PDF or TIFF files.

- **TIFF**
- **PDF**

Image File Options

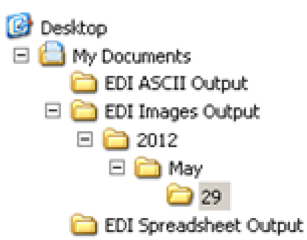
The following options are available:

- **All Images in One File with EDI File Name as Image File Name**
- **One Image File per Enrollment Record**

Image Folder Options

When you create a lot of images, it is important not to place them all in the same folder. Microsoft Windows has issues handling more than 1000 files in a folder. That is the reason why the HIPAA Claim Payment Master can hash the image files over many sub-folders. You have the following choice to use:

- **None** — Default value.
- **Sub-folders for Year-Month and Day** — The sub-folders will be created within the Image File Location. Example: `\2012\February\29\`.



The folder structure in "Year, Month and Day" mode

- **Sub-folders for Year and Week** — The sub-folders will be created within the Image File Location. Example: `2012\9\`.
- **Sub-folders for Year and Day** — The sub-folders will be created within the Image File Location. Example: `2012\20120229\`.

Color on Images

- Choose a color for the form when saving claims to image files. You have the choice to render the form in red or in black.

Note: The data is always black.

Options for PDF

- **Use Content Compression** — Checking this option does result in considerably smaller files.

Options for TIFF

- **Color Depth** — You can change color depth of the image (black / white, 4 bpp / 8bpp / 24bpp / 32bpp).

Note: TIFF in Window's GDI library does not work with 16 bpp (bits per pixel). Color depths set lower than 16 bpp results in some losses in image quality.

- **Compression Algorithm** — You can use compression with TIFF files: LZW and Packbits is used for all Colors, CCITT4 for black and white.

- **Image Resolution** — You can change the resolution of image from 96 to 300 dpi (dots per inch).

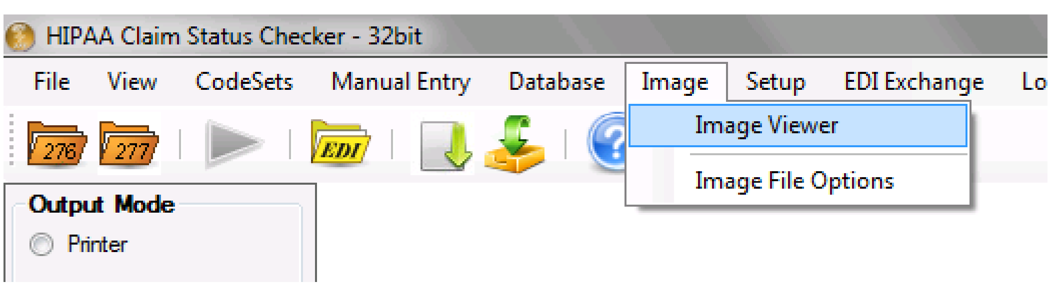
Note: Theoretically we could use even higher resolutions, but it will slow down processing significantly and result in approximately the same result in quality.

5.3 Viewing Image Files

HIPAA Claim Status Checker's Image Viewer allows you to view images stored in the output folder, defined in the image options. See Adjusting Image.

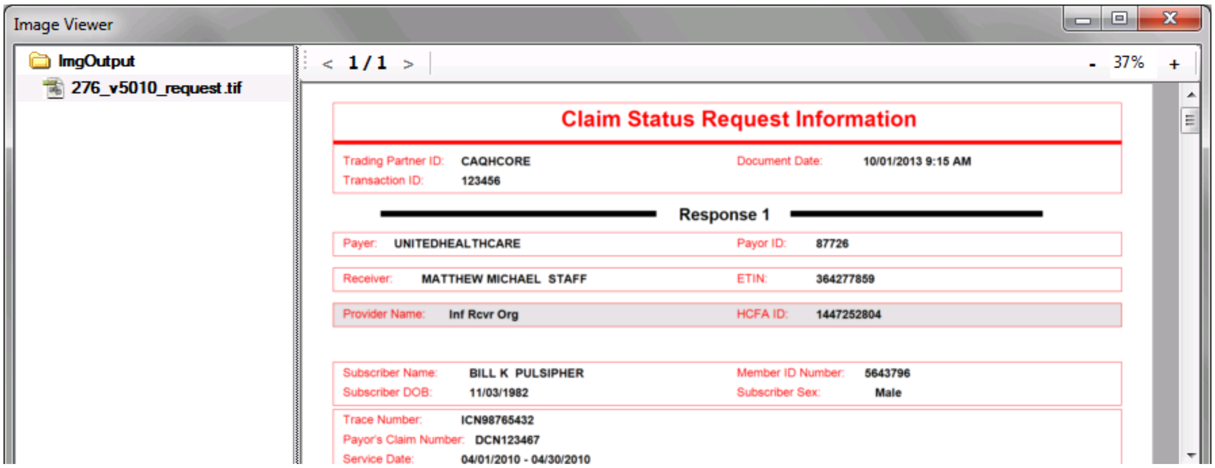
Follow the instructions below to view images.

1. To access Image Viewer, select the "Image Viewer" option under "Image" menu item.

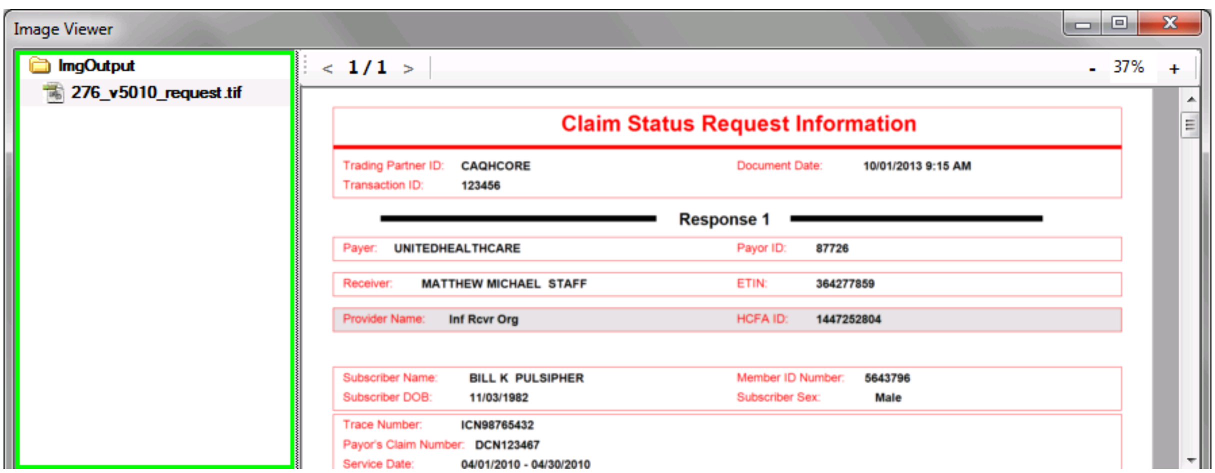


The "Image Viewer" menu

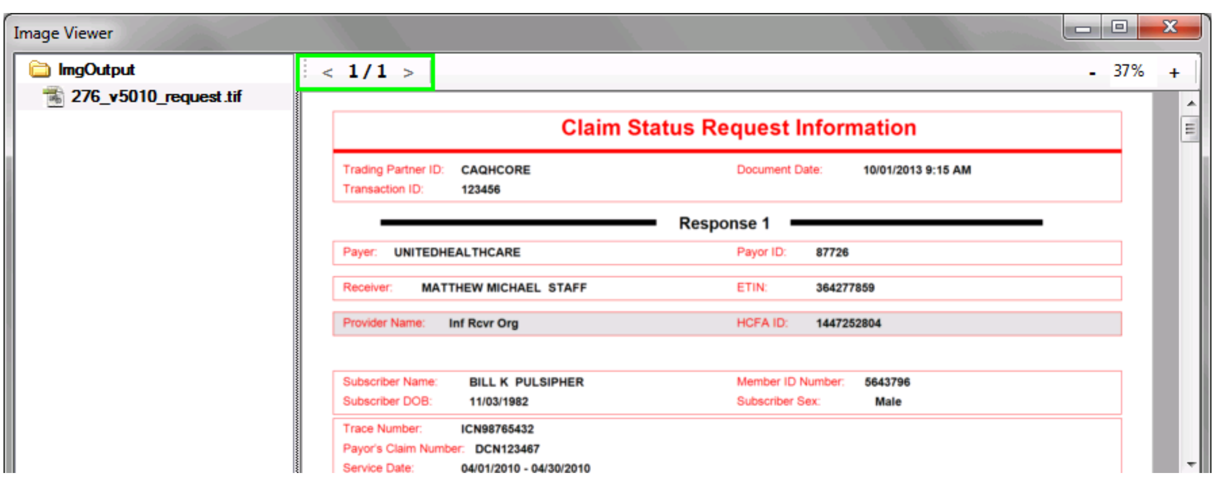
2. The "Image Viewer" window will open.



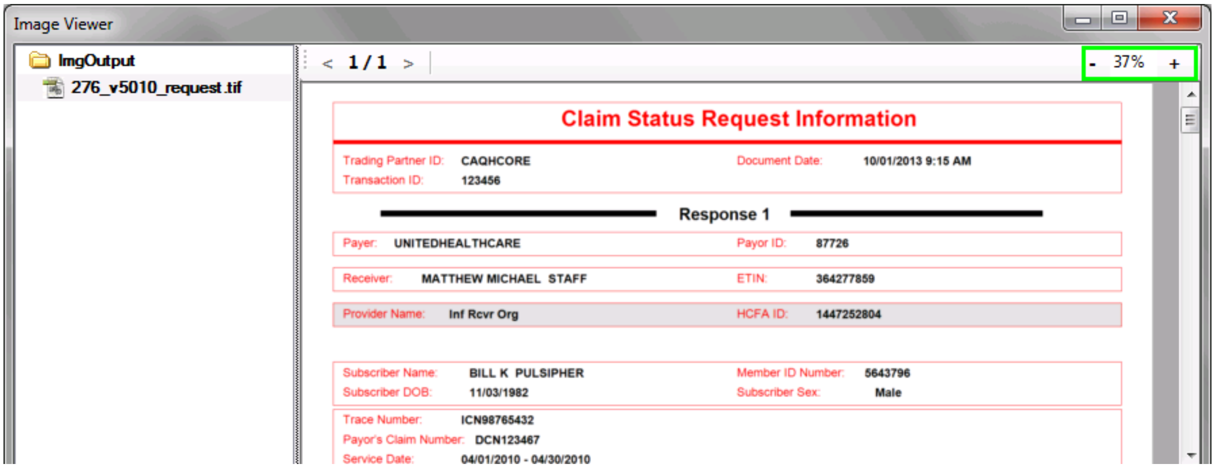
3. Select the necessary image in the left navigation pane.



4. For page navigation on forms with multiple pages, use the arrow buttons.



5. To scale the image, use "+" or "-" buttons or define the percent manually.



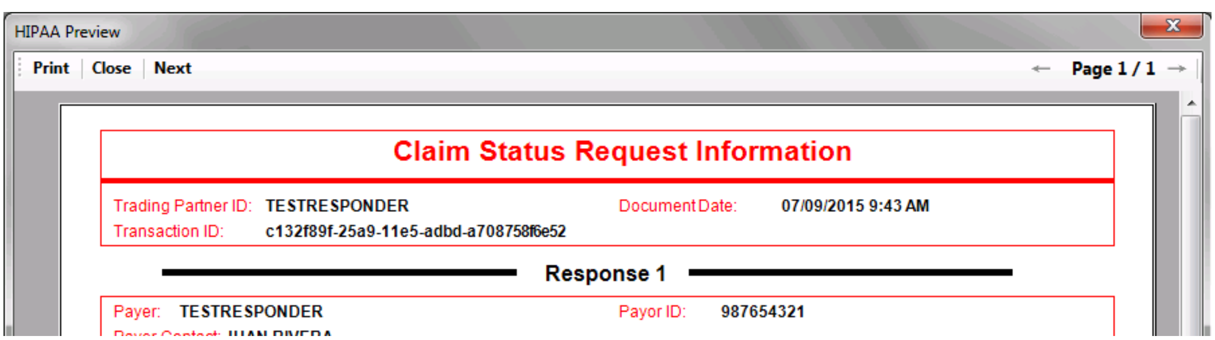
6 Autoprocessing

6.1 Using Command Line Arguments

The HIPAA Claim Status Checker 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**. If not applicable (such as when querying the database), leave blank.

If this is the only argument used, the file will be shown on screen:



2a. The second argument or combination of arguments contains the processing options. Querying database in order to create a 276 EDI file requires additional arguments.

P - Print.

X - Export to database.

I - TIFF file.

Note: using multiple processing options is possible.

Example: To both export a Claim Status Response to the database and print it:

```
C:\Program Files\HIPAAsuite\HIPAA Claim Status Checker>HIPAAClaimStatusChecker.e
xe D:\EDI\Inbox\277_2.edi,XP
```

2b. Building a 276 Claim Status request will require arguments 3, 4, 5, and 6 to be filled.

Q - Database query.

E - Create EDI in conjunction with Q. The query results will be used to generate a 276 Claim Status Request.

Example:

```
C:\Program Files\HIPAAsuite\HIPAA Claim Status Checker>HIPAAClaimStatusChecker.e
xe edi,qe,D:\EDI\TEST726.edi,"SELECT * FROM edi_ClaimStatusHeader",LOCALTRADINGP
ARTNER
```

This query will use all the Claim Status Requests in the EDI_ClaimStatusHeader table to create a 276 Claim Status Request EDI file.

3. The third command line argument is the **output filename**. A relative address can be used and will be based on your default Output Directory.

4. The fourth argument is your Query should you should have "Q" as a second argument.

5. The fifth argument is the target trading partner. This works only with the EDI Exchange module enabled. If omitted, the last receiver used in the Create 276 Files window.

6. In the sixth argument you specify whether to use "T" Test or "P" Production database connection if you have "Q" for query as the second argument.

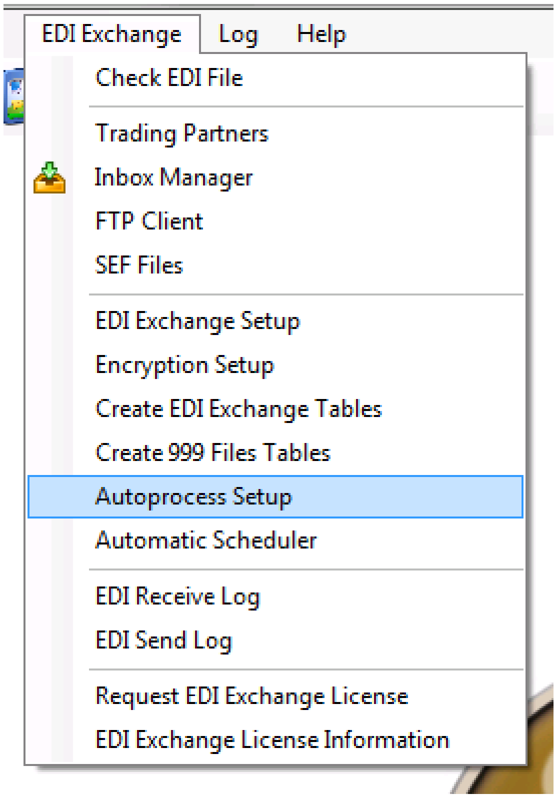
6.2 Autoprocessing with the EDI Exchange Module

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.

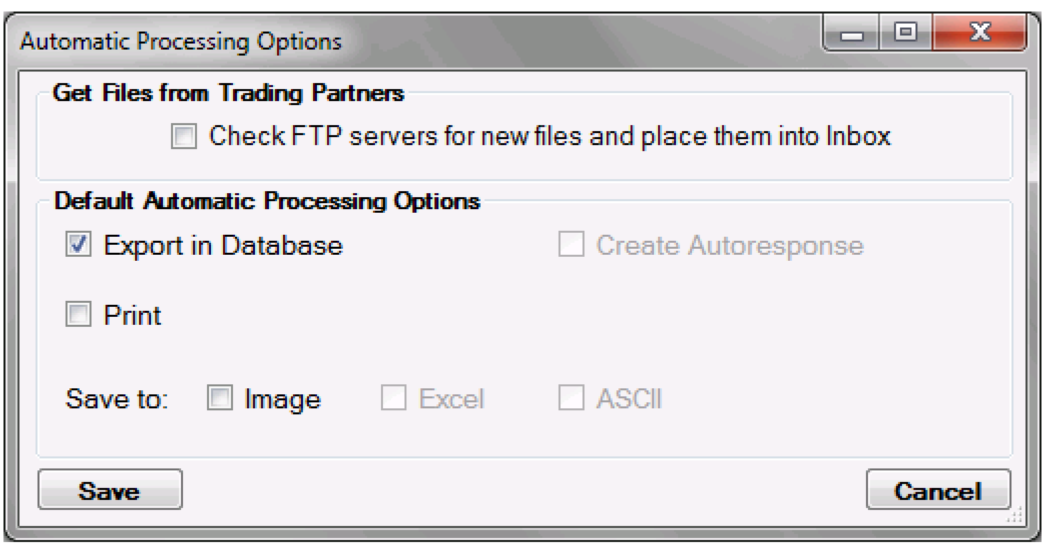
```
C:\Program Files\HIPAAsuite\HIPAA Claim Status Checker>HIPAAClaimStatusChecker.e
xe auto
```

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.

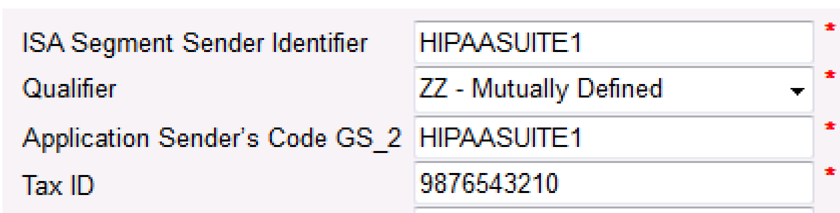
```
C:\Program Files\HIPAAsuite\HIPAA Claim Status Checker>HIPAAClaimStatusChecker.e
xe auto, D:\EDI\Inbox\276_2.edi
```

Command to autoprocess a single file.

6.3 Changing the Default Company

The default company is the identity you assume as the sender when creating EDI files. This affects the ISA, GS, and NM1 sender segments. A single entity may have a need to act as multiple sender identities and so has a need to change the information in the EDI envelopes.

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

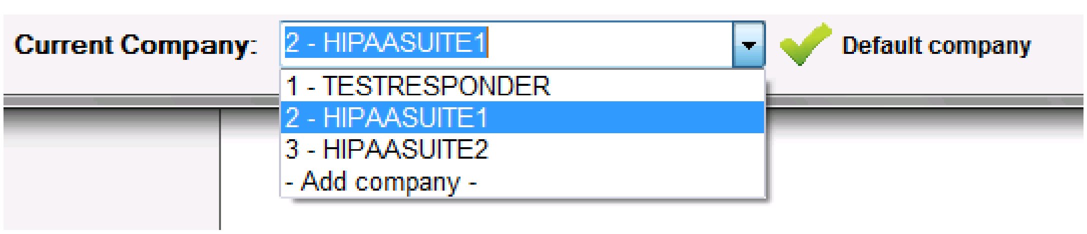


Sender ID segments in Company Setup

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 Checker>HIPAAClaimStatusChecker.e
xe 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

```
Set default company with ID 3
        Company # 3 is set as a default company
```

Excerpt from log. Default company changed.

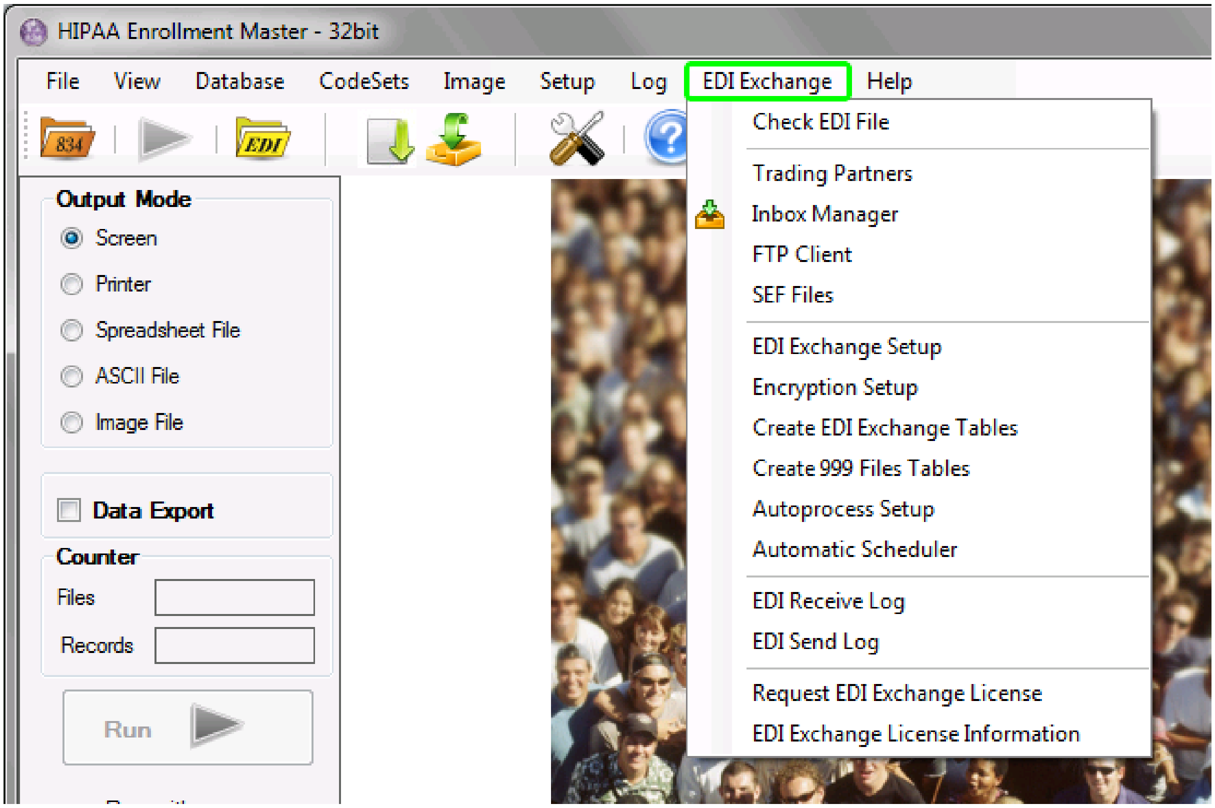
7 EDI Exchange

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**

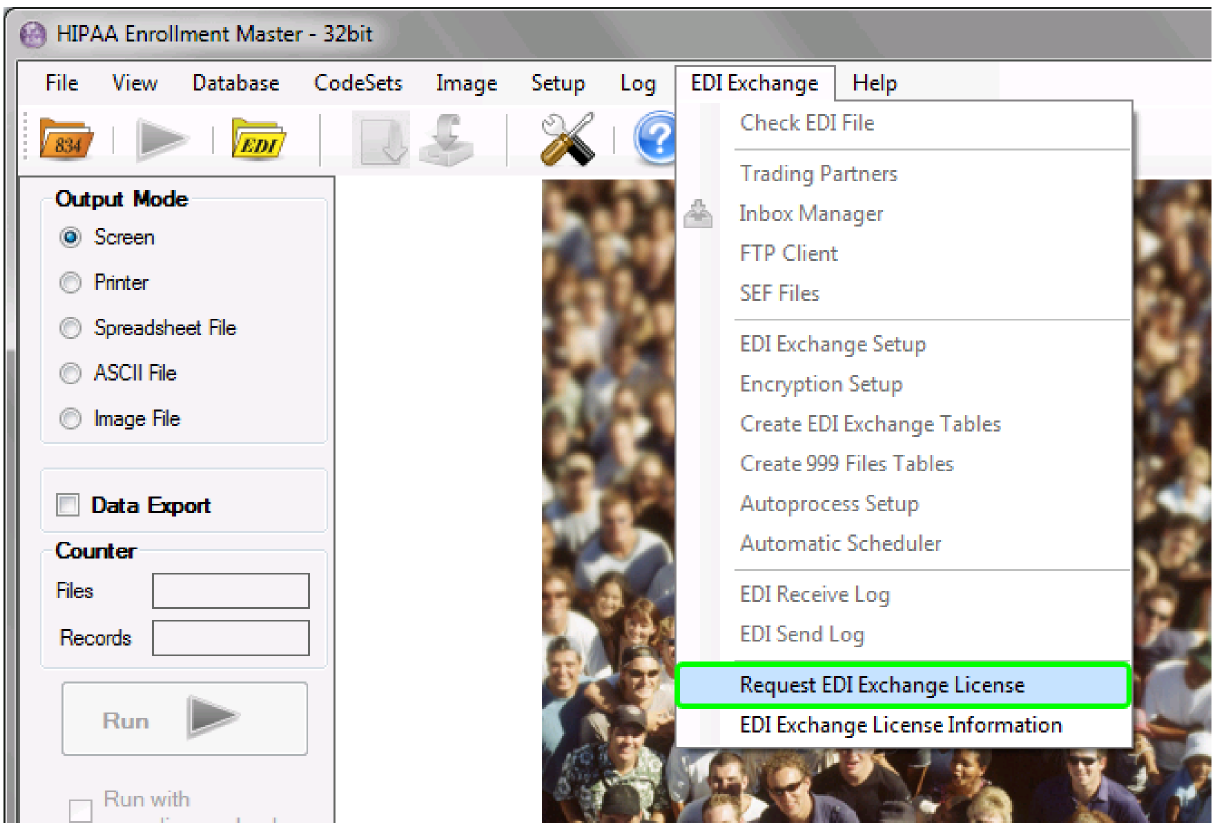
7.1.2 Requesting EDI Exchange License

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.

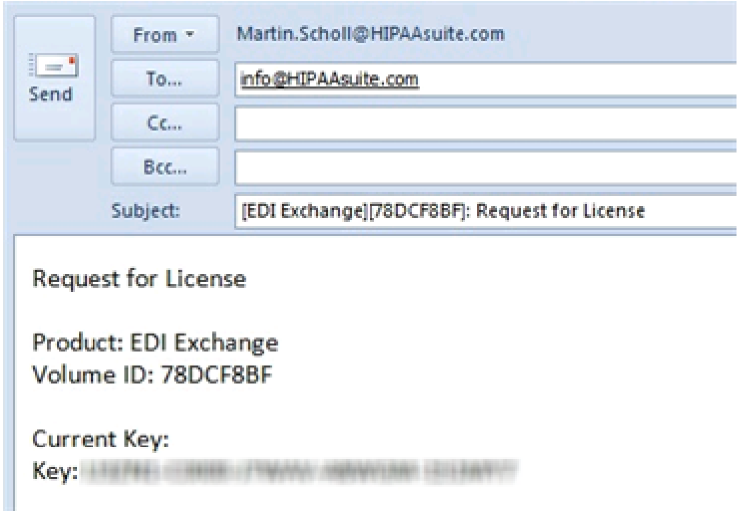
Follow the instructions below to request a trial or final license key.

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



A menu item to request a license key

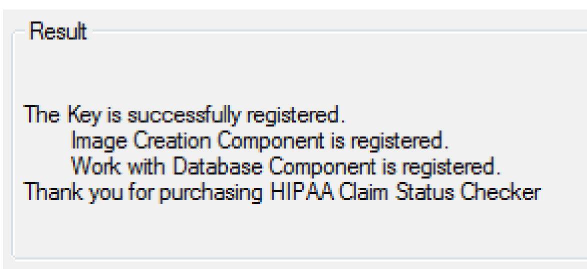
2. Once you have clicked this menu item, your default email application appears. In our case, it is Microsoft Outlook. All information necessary to produce the key is automatically filled out.



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.

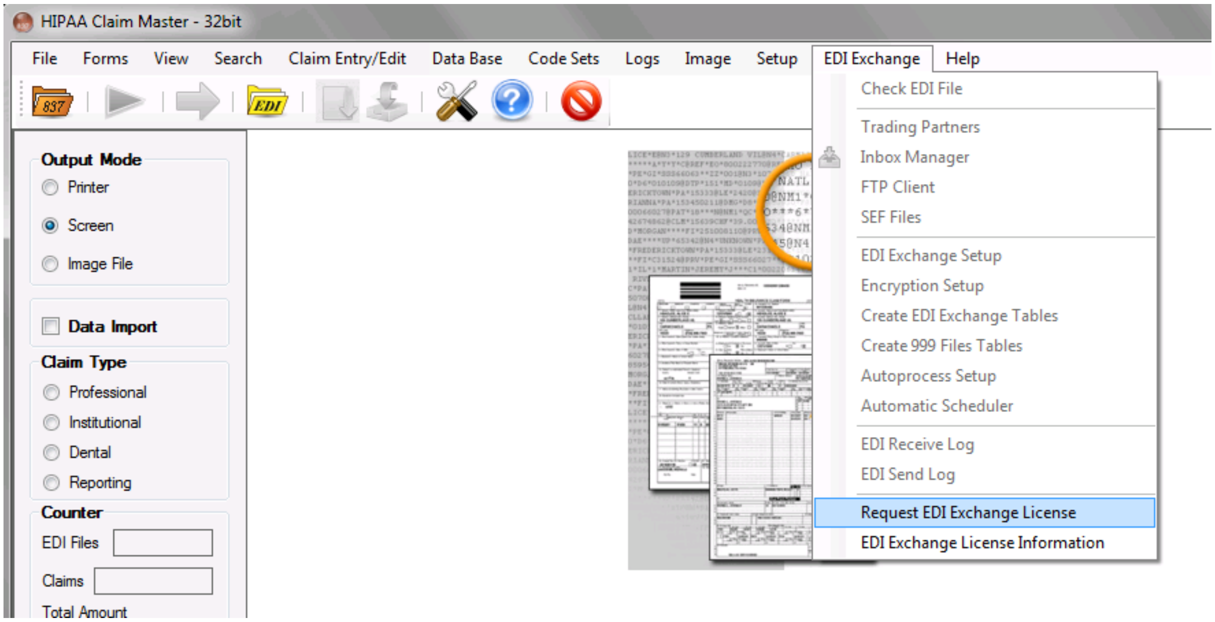


Entering the license key

7.1.3 Registering EDI Exchange

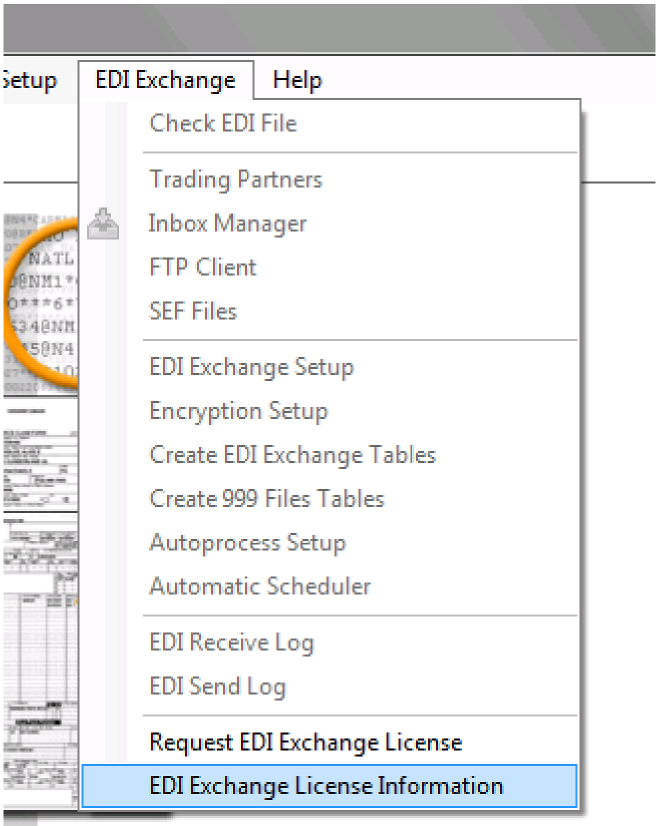
EDI Exchange is licensed separately from the host application, HIPAA Claim Master, for example. The reason is that EDI Exchange will work on all HIPAAsuite Products that are installed on your particular computer. For example, if you have HIPAA Claim Master and HIPAA Enrollment Master licensed, only one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



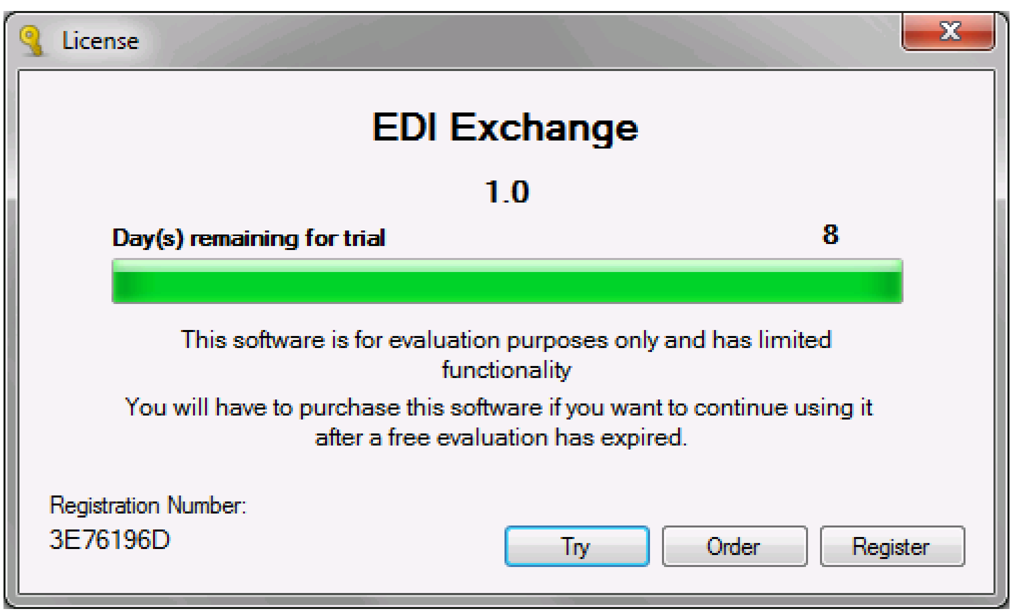
The "EDI Exchange" menu with menu items disabled

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



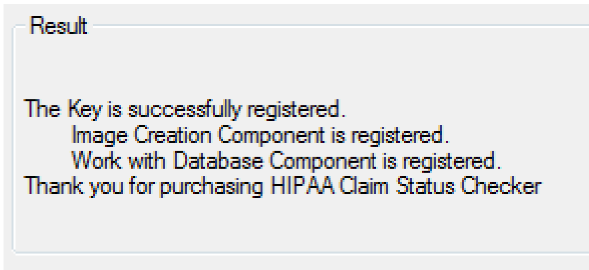
"EDI Exchange License Information" option under the "EDI Exchange"

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

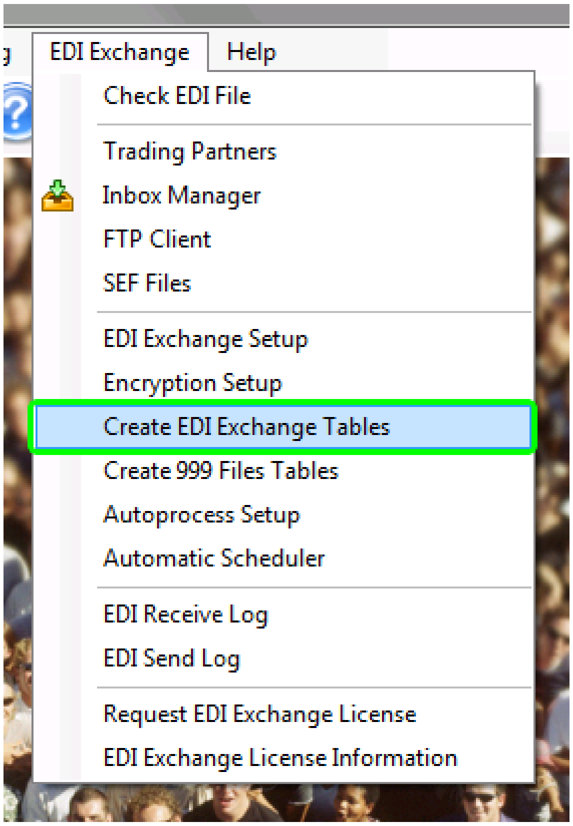
EDI Exchange work is based on the database connection that you define under *Database* ▸ *Connection and Data Fields* in the main menu of the HIPAA host application. Make sure the connection has already been set up and tested before proceeding with EDI Exchange.

Then proceed to the next step: Creating Database Tables.

7.2.2 2 Creating Database Tables

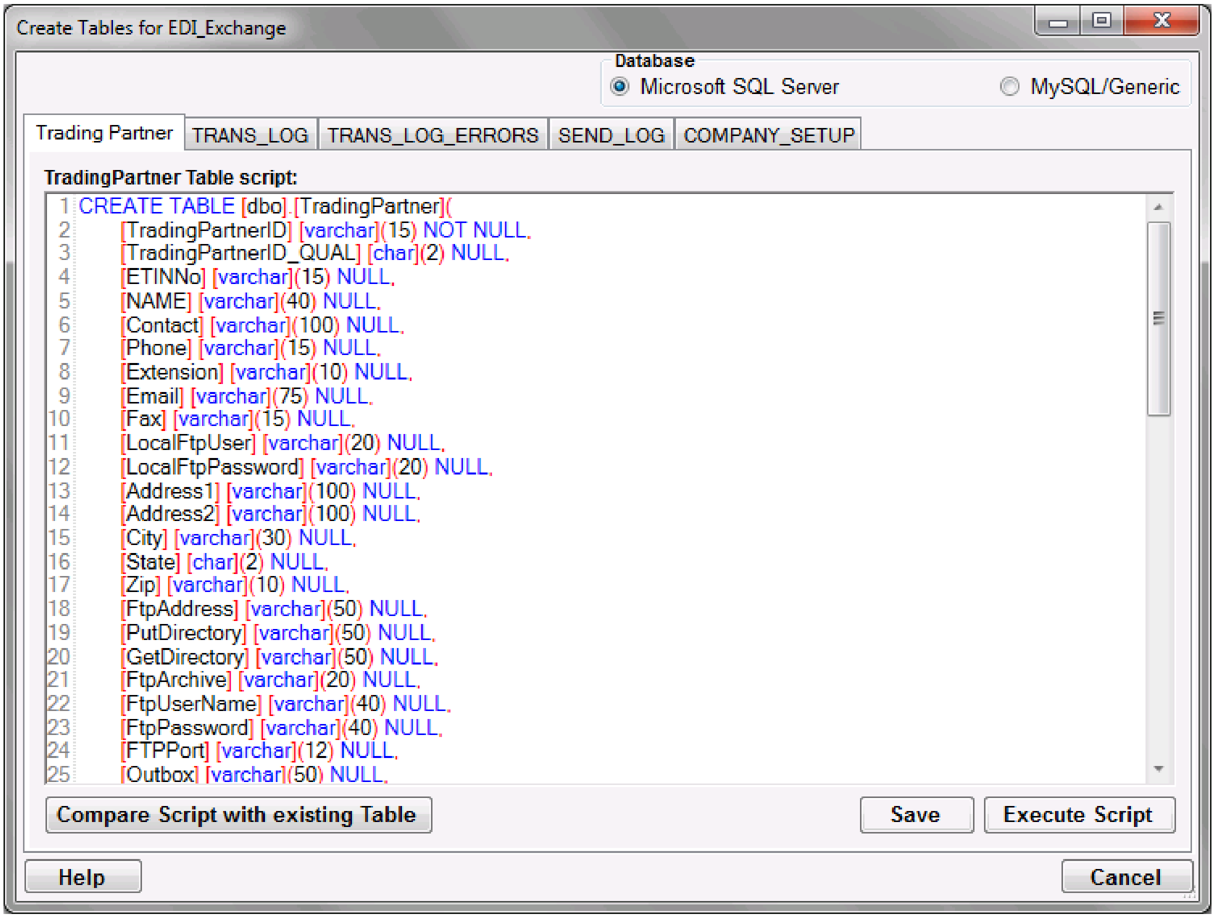
Once you have configured the database connection (Setting up Database Connection), follow the instructions below.

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.

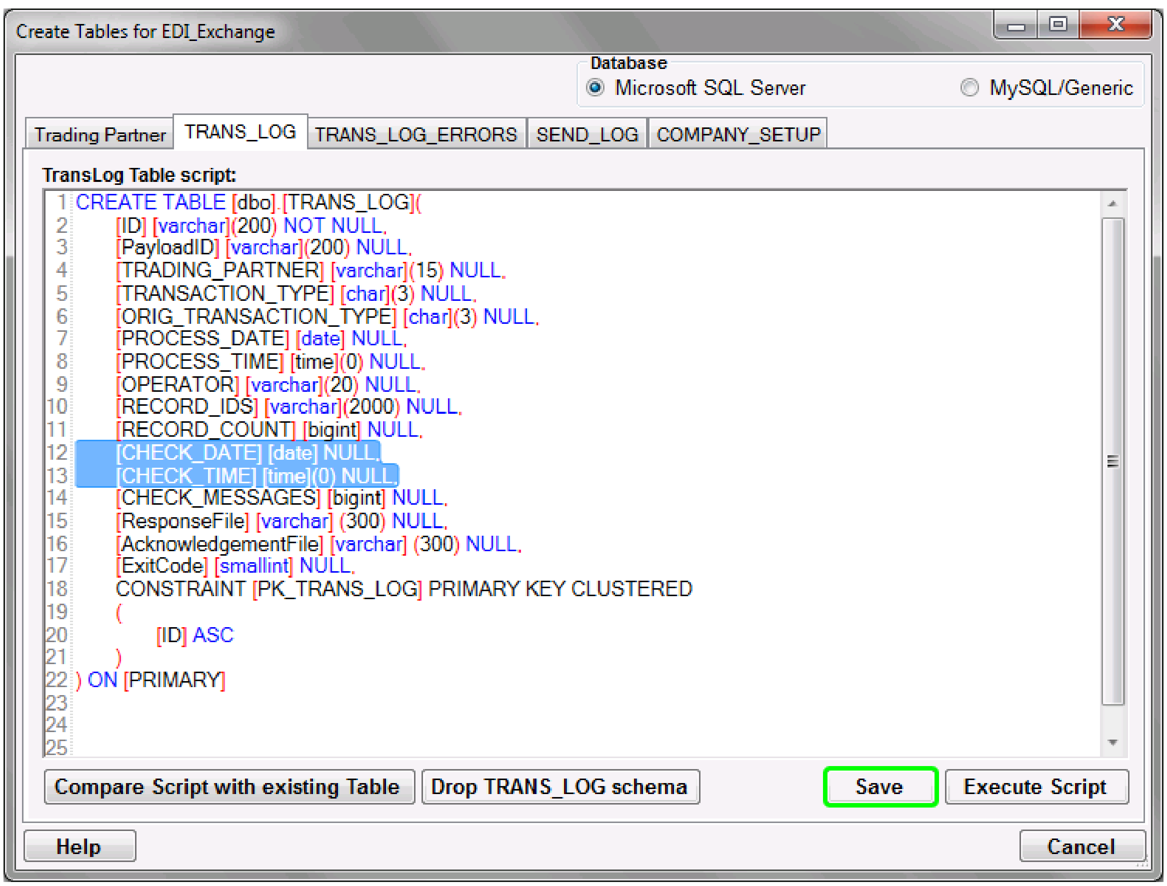
   - **Trans_Log** — SQL statements to create the "TRANS_LOG" table in your database. This table contains incoming file information, keeps track of all EDI files that you receive and the compliance check report.

   - **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.

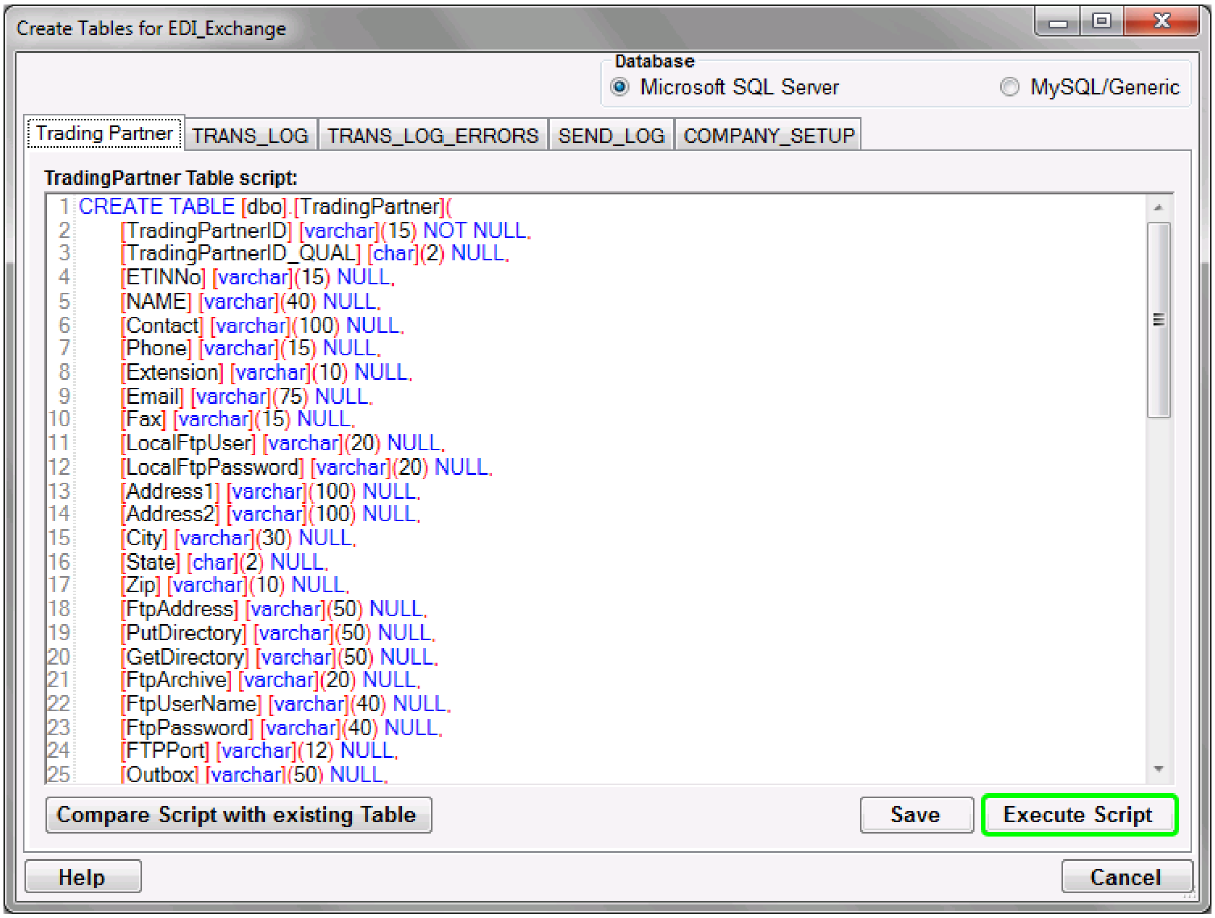
5. You can modify the scripts so that they run on your specific database. Once you have you modified the script, click "Save."

   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

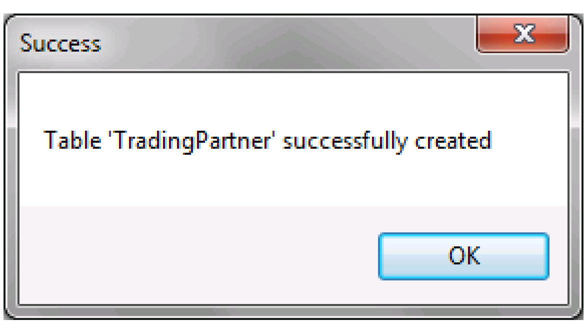
6. For **each** script on every tab, click "Execute Script" to create the corresponding table in the database.



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.

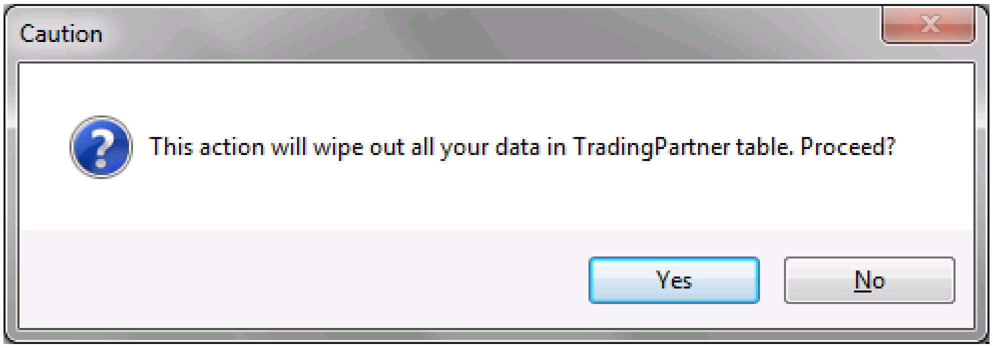
7. Once the table has been created successfully, you will see the following notification:



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

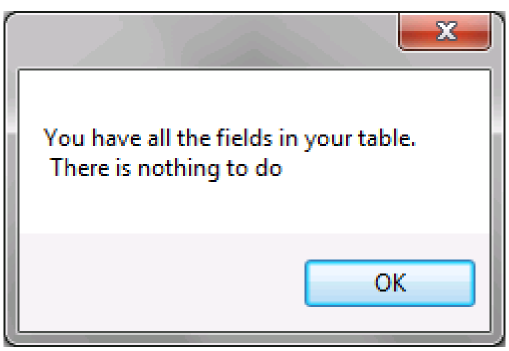
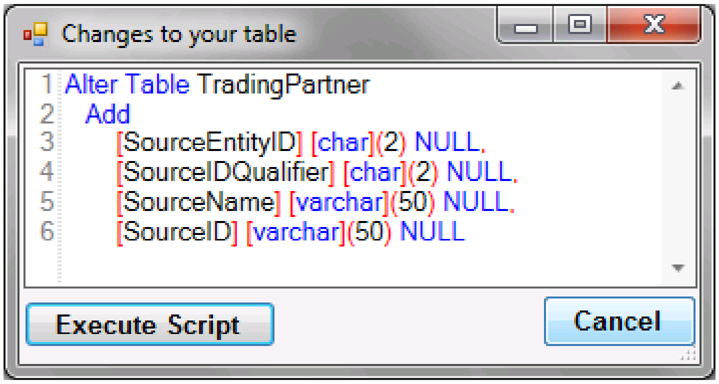


Table is up to date

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

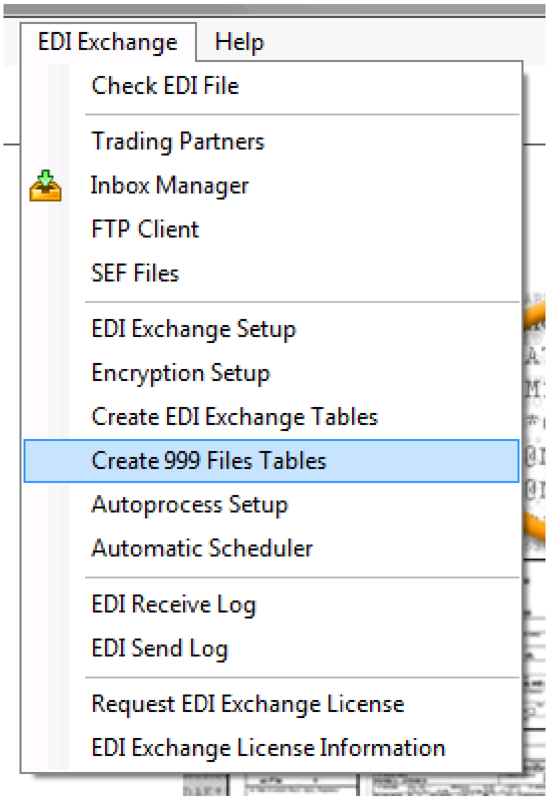
Alter Table statement successfully executed.

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

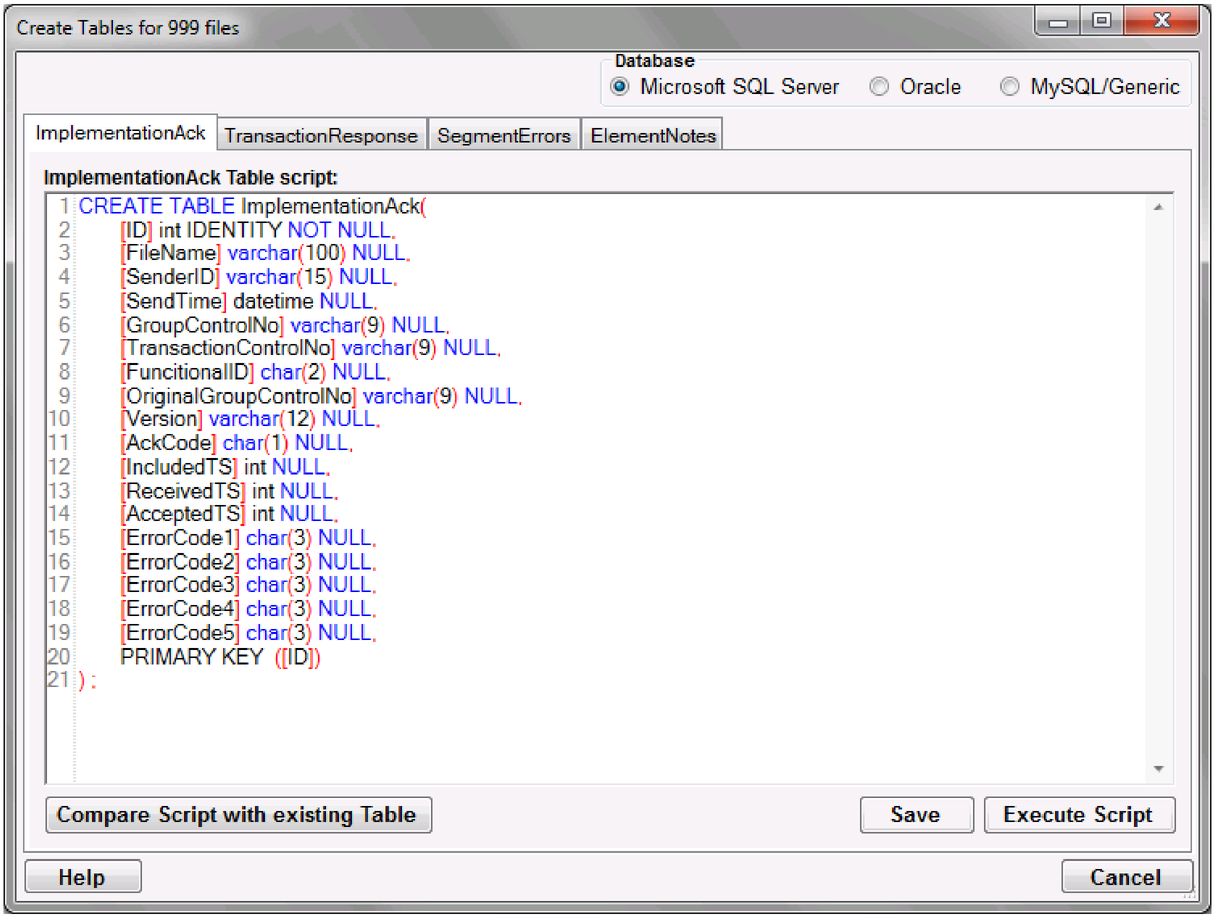
Once you have configured the database connection (Setting up Database Connection), follow the instructions below.

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.

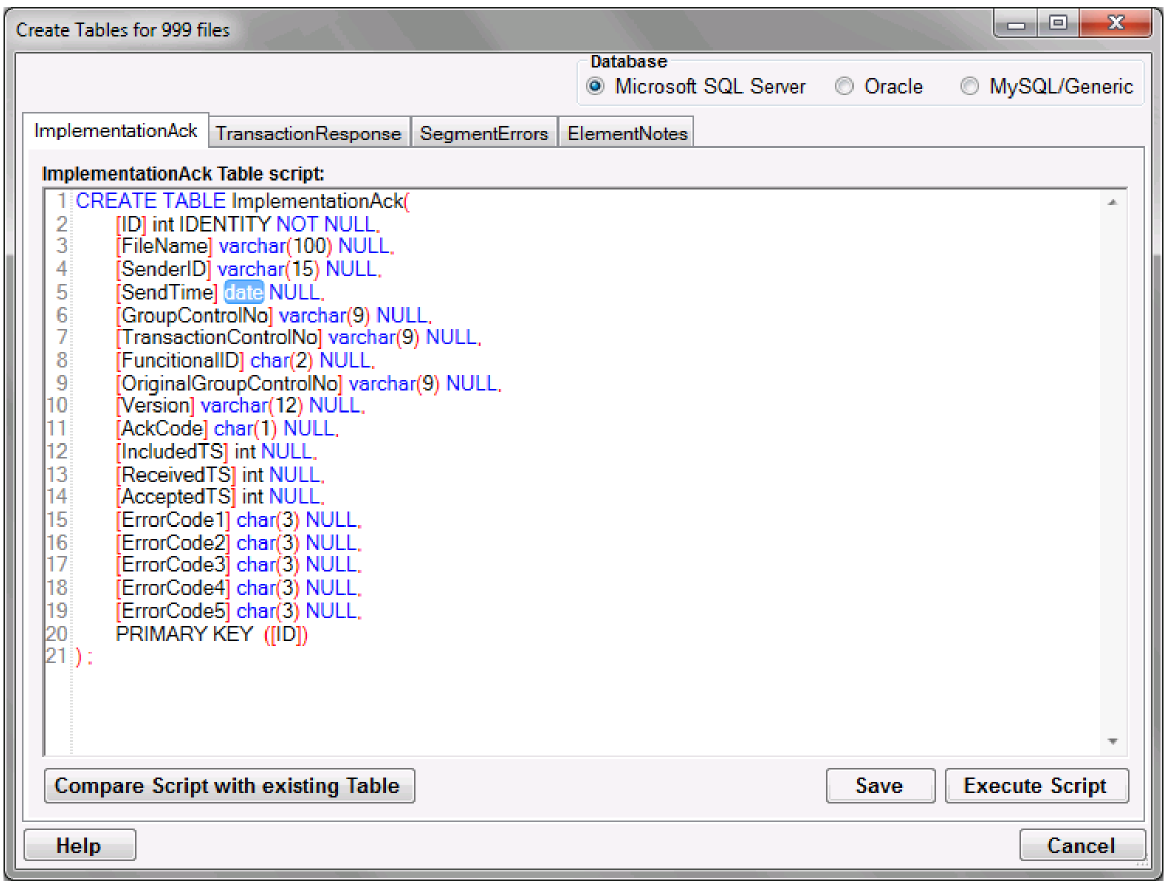
1. The following tables are part of EDI Exchange:

- **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.

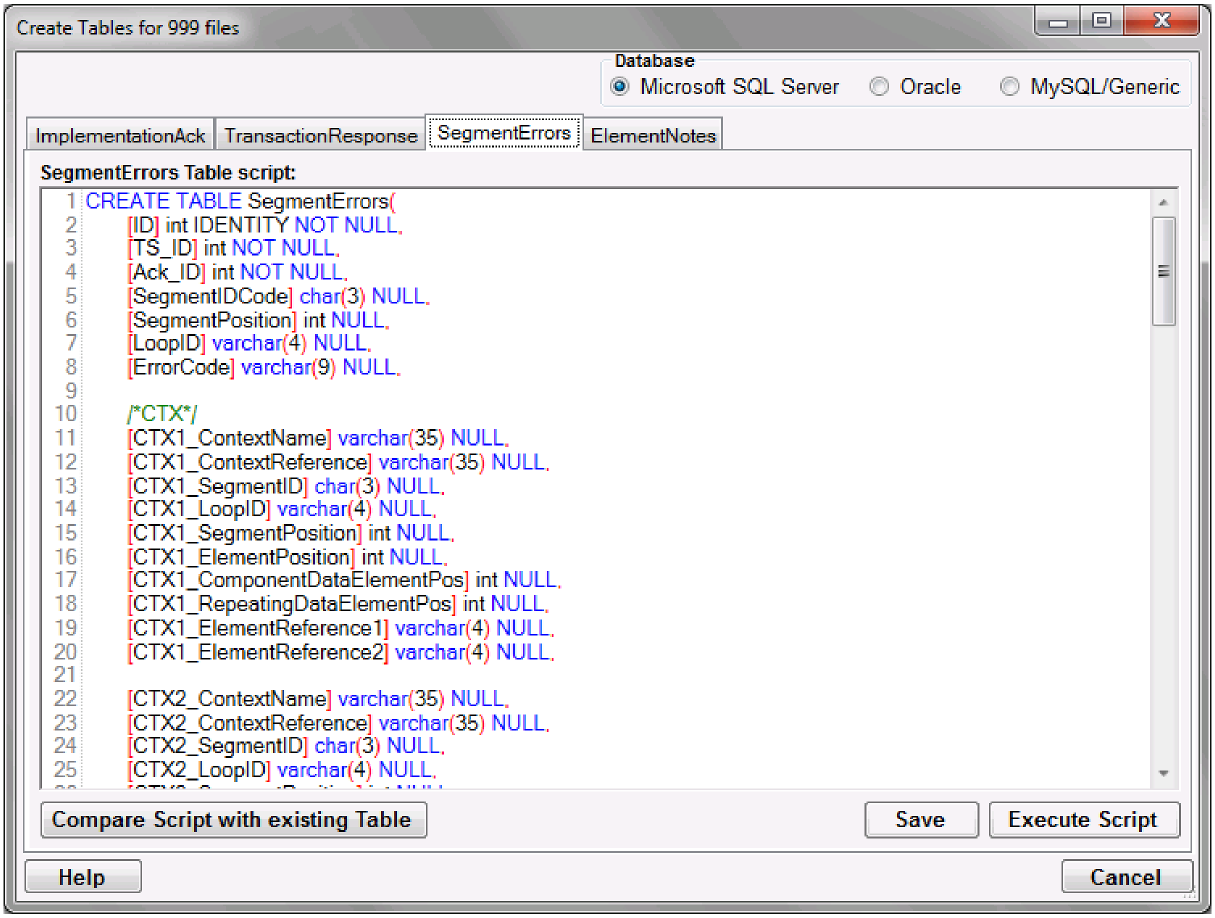
5. You can modify the scripts so that they run on your specific database. Once you have you modified the script, click "Save."

> 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

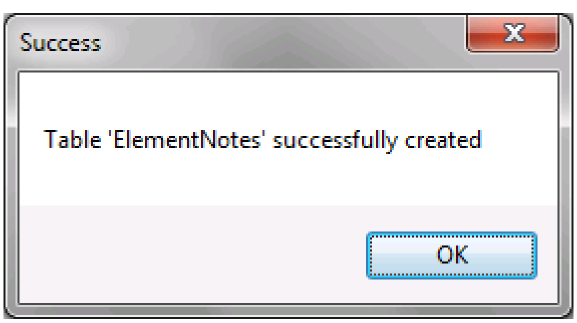
6. For **each** script on every tab, click "Execute Script" to create the corresponding table in the database.



The "Execute Script" button

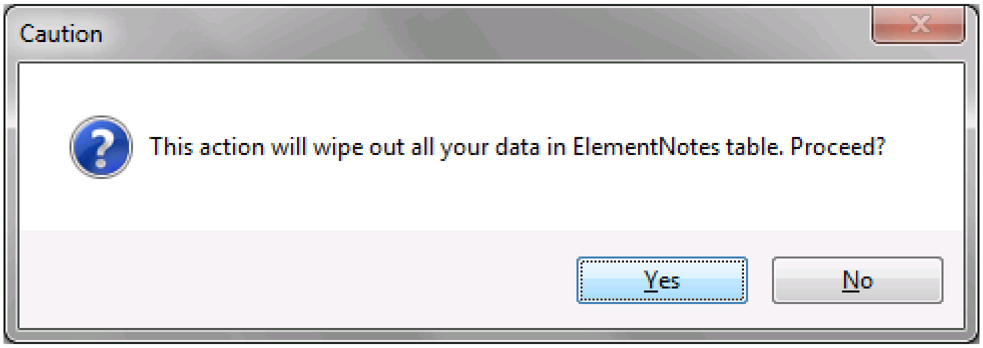
> Notice: Creating tables means clicking the "Execute Script" button in all four tabs of the "Create Tables for 999 Files" window. Then close this window.

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

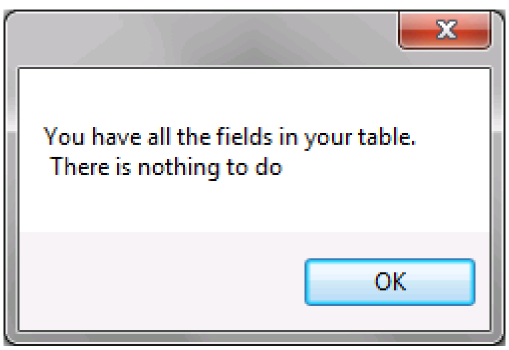


Table is up to date

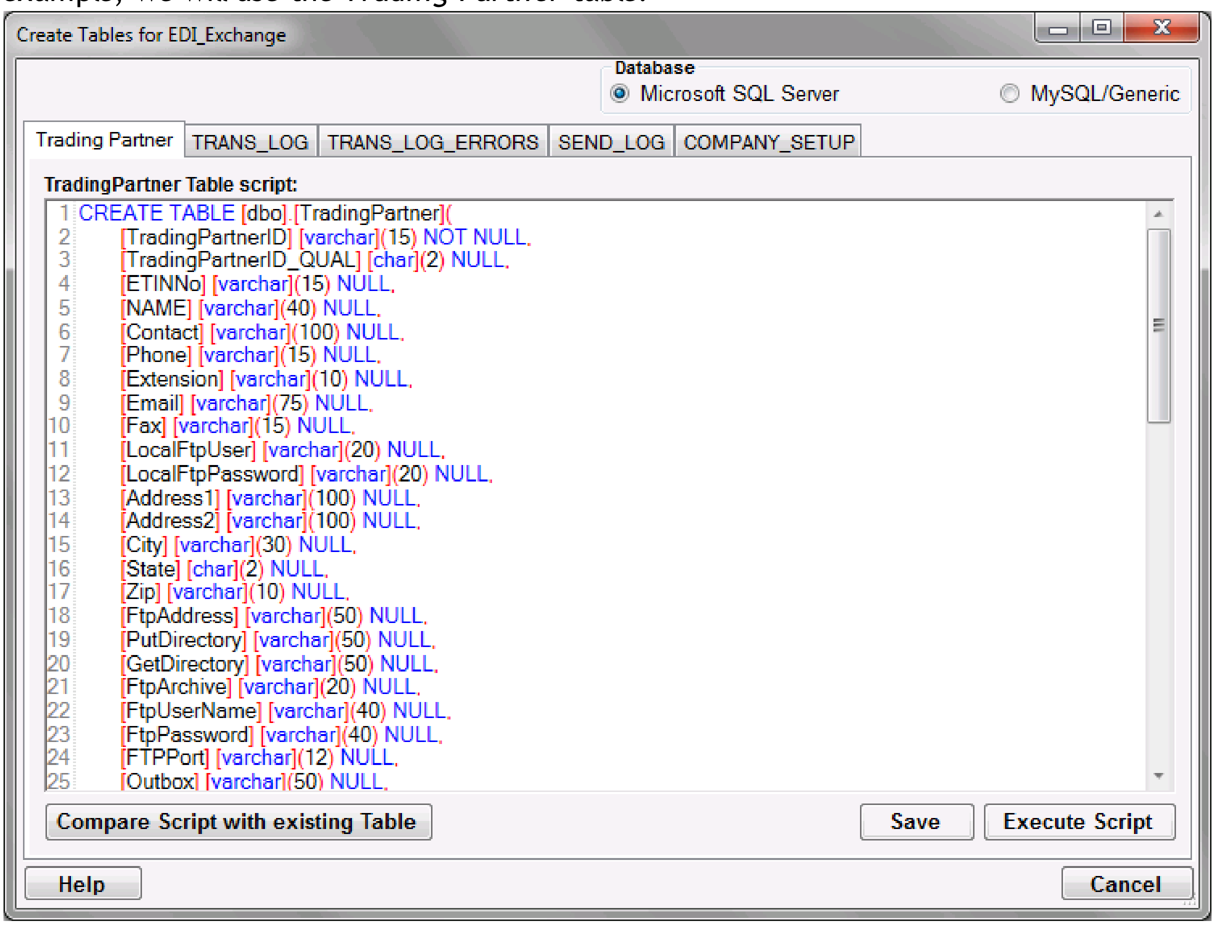
or if your table is missing recently added fields, you will see a window pop up that shows an 'Alter Table' script with which you can add those fields to the table without interfering with existing data. In the latter case, you can click the "Execute Script" button and the field will be added and a message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



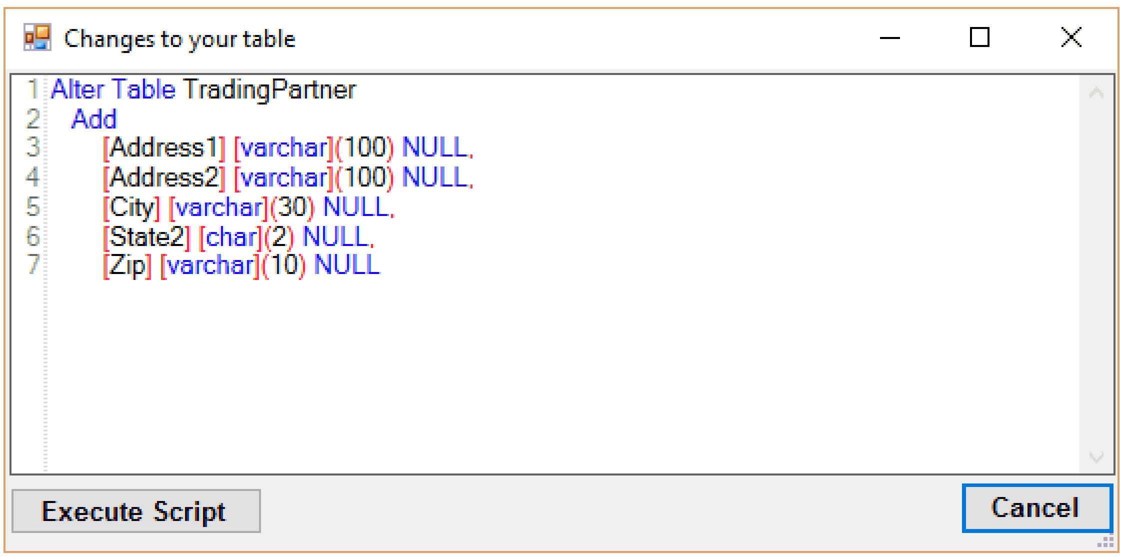
The table creation script for the Trading Partner table.

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.

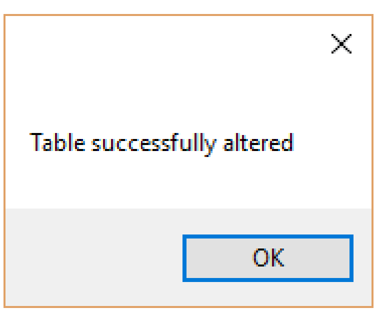


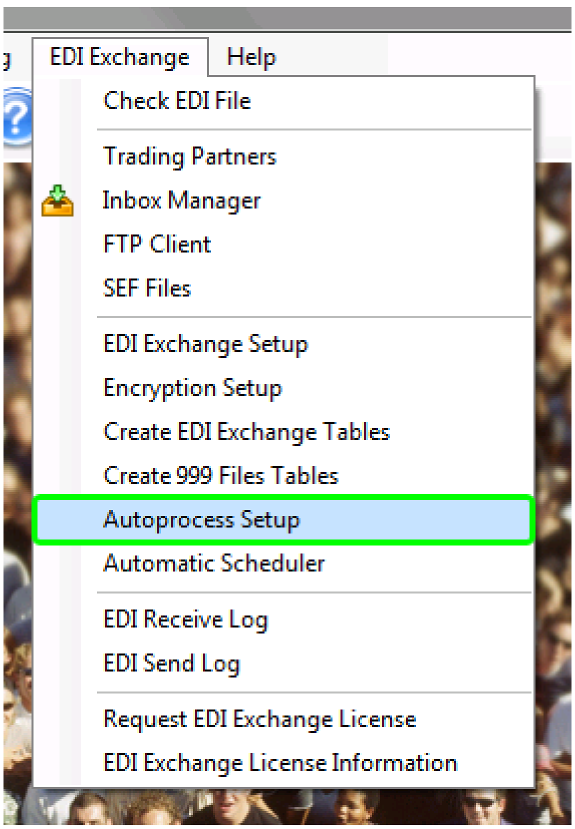
Table has been altered.

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.

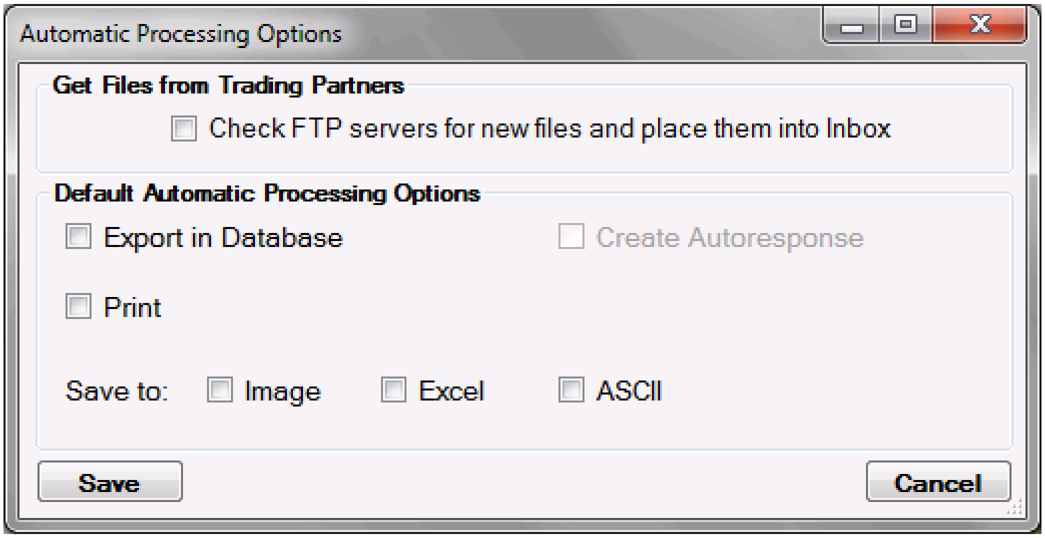
Follow the instructions below to specify the Auto Process Options.

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:

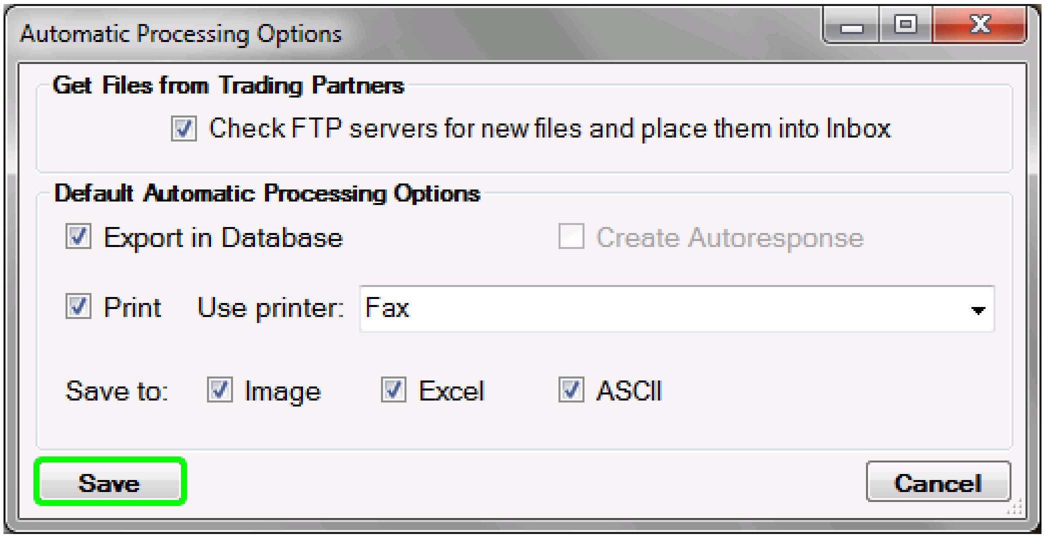
Check Path Options

- **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

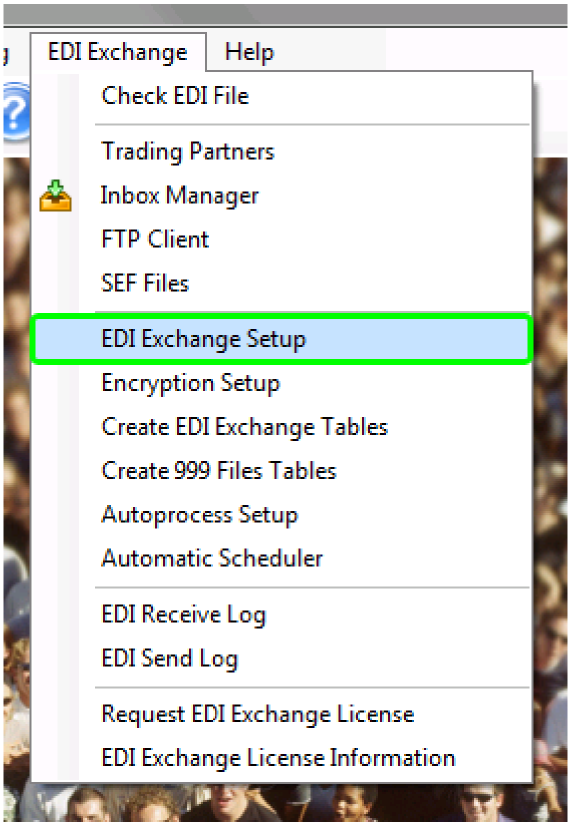
EDI file directory is an obligatory setting you need to set up before starting using the EDI Exchange. In order to keep track of the thousands of EDI files that accumulate over time, EDI Exchange uses a folder structure which we call the "HIPAAsuite Communications Directory" or "HIPAAsuiteCommDir" in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

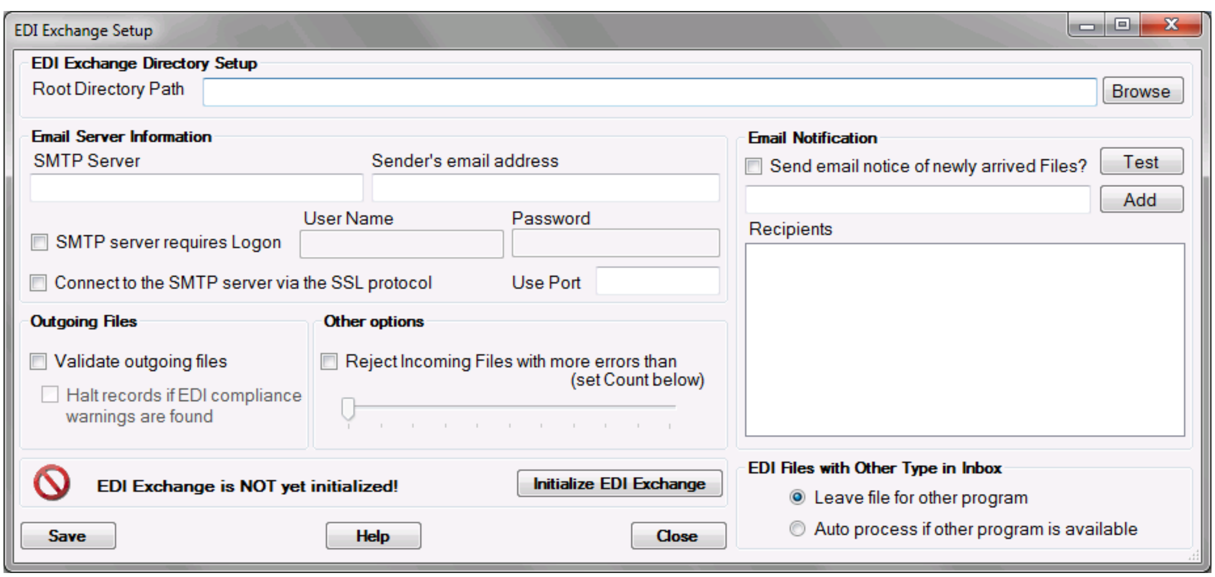
Follow the instructions below to specify EDI communications root directory.

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



The "EDI Exchange Setup" menu item

2. The following window will appear.

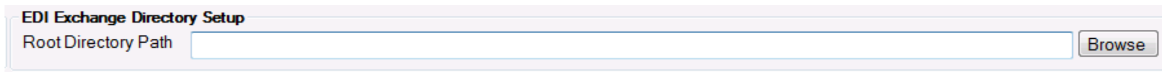


The "EDI Exchange Setup" window

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

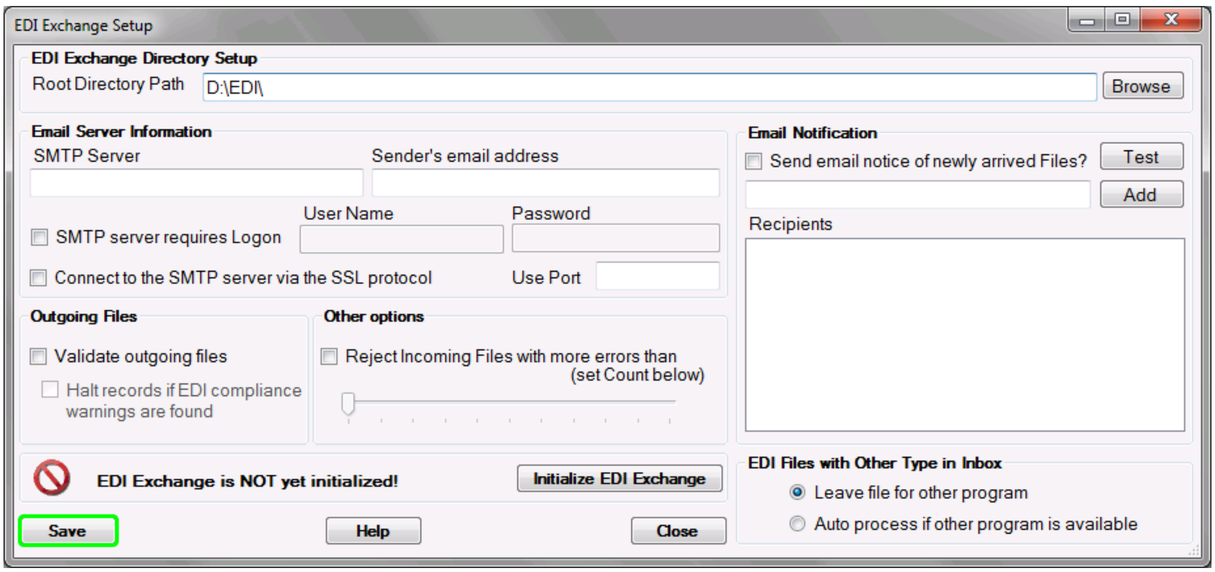
3. Under "EDI Exchange Directory Setup" specify the following setting:

- **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."



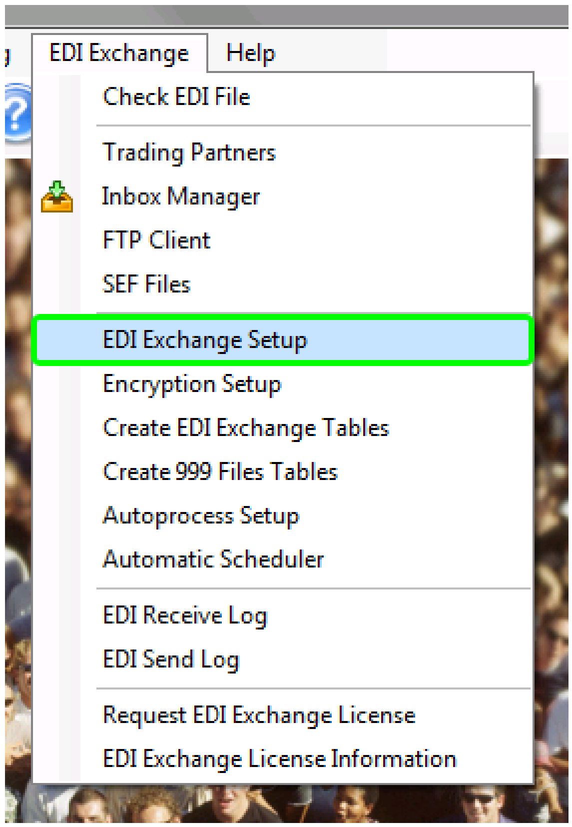
The "Save" button

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

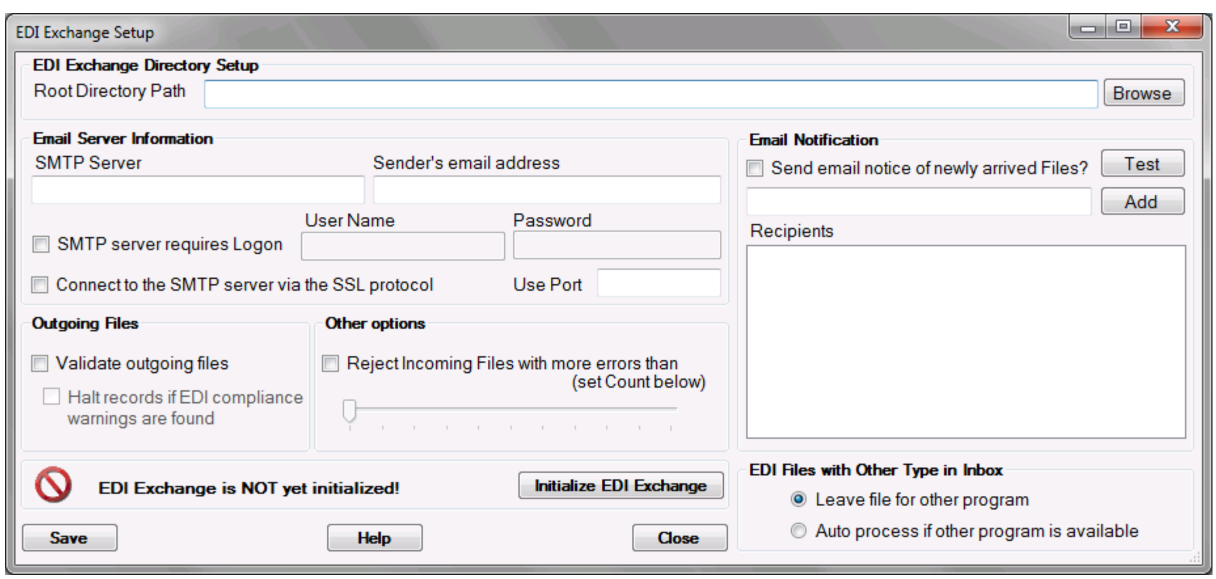
Before you can use EDI Exchange, and after you have configured the obligatory settings, you have to perform the initialization. Follow the instructions below.

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



The "EDI Exchange Setup" menu item

2. The following window will appear.

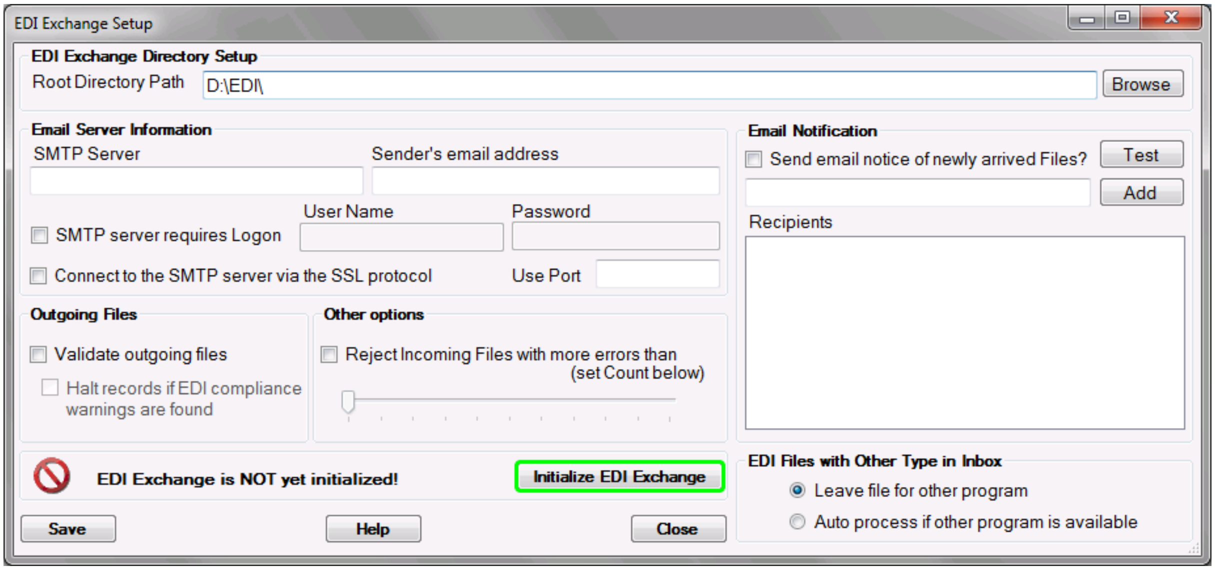


The "EDI Exchange Setup" window

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

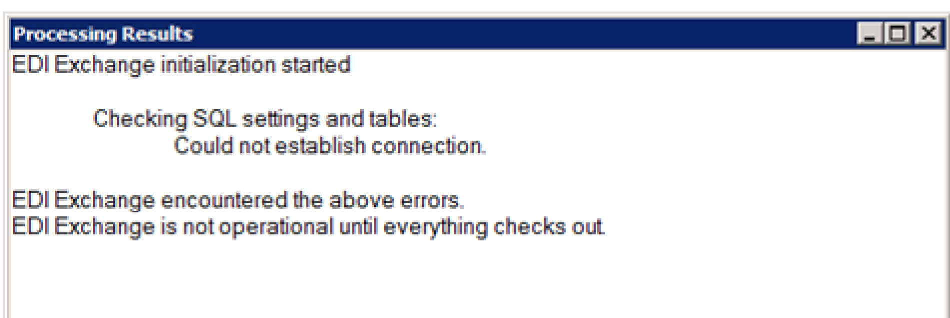
Directory), you can initialize EDI Exchange module. Click the "Initialize EDI Exchange" button to accomplish the process.



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

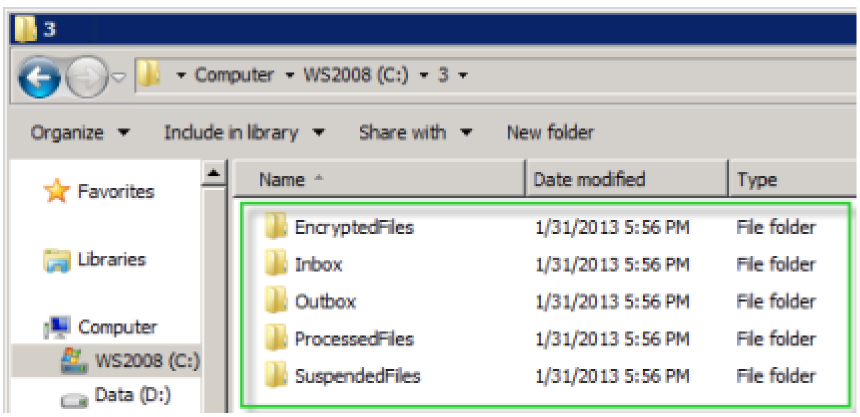
Read more in Setting up Database Connection.

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:

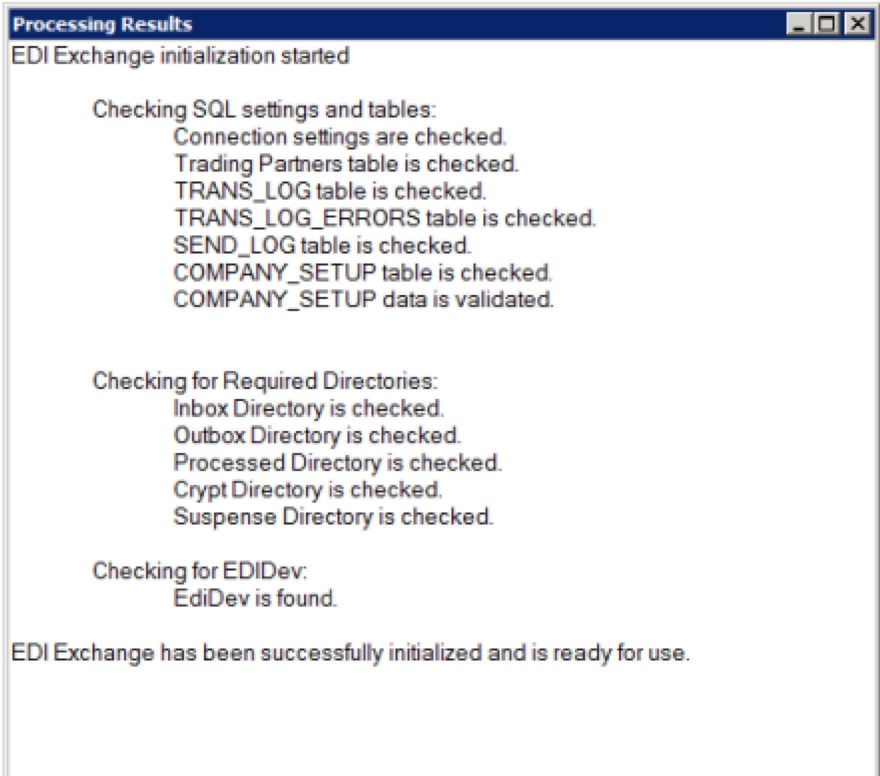


The directory structure of EDI Exchange

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

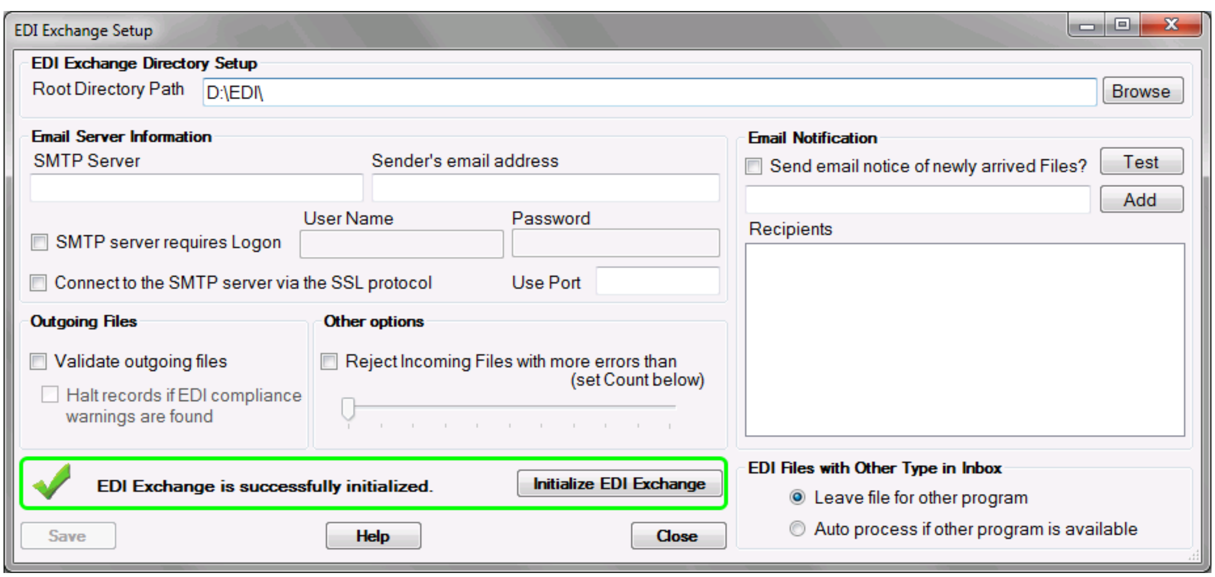
5. The last thing checked by the system is if the Automatic File Processing options have been set up. Read more in Defining Auto-Processing Options. The options are important for the hand over from EDI Exchange to the other HIPAAsuite program that hosts EDI Exchange.

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.



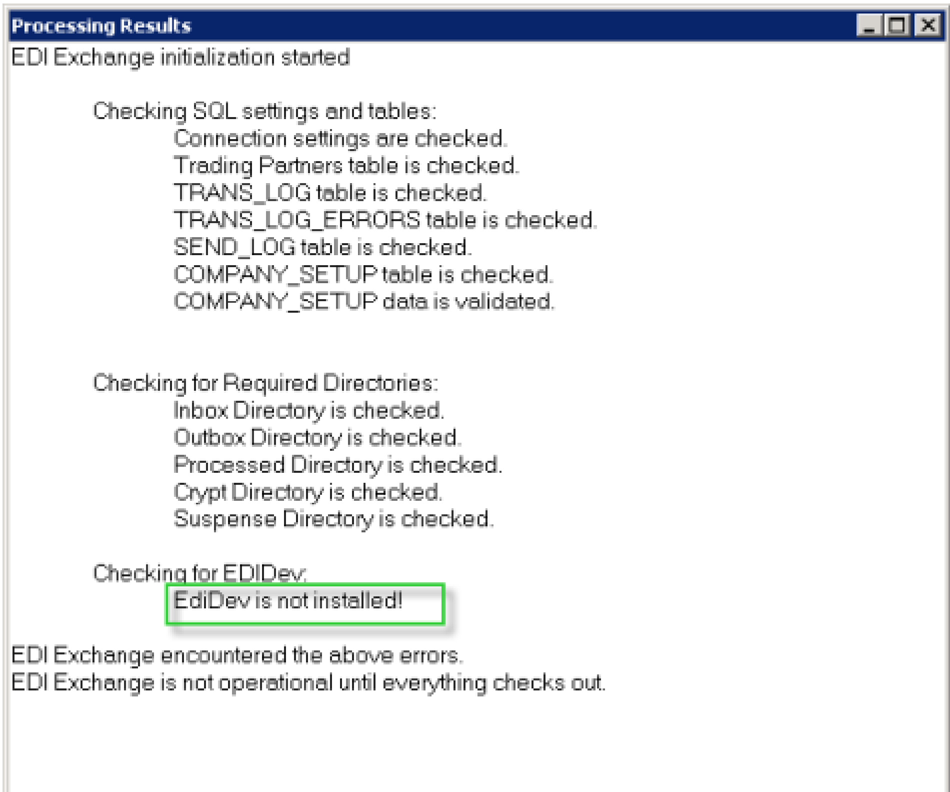
The "EDI Exchange is successfully initialized" message on the bottom of the "EDI Exchange Setup" window

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!
```

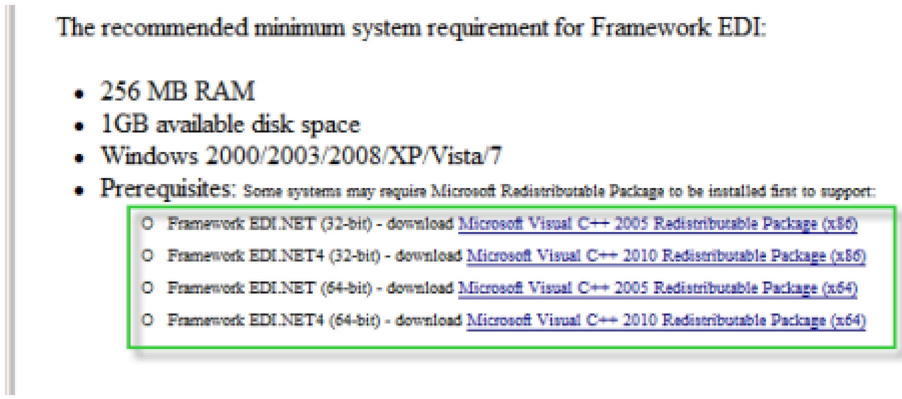


The EdiDev component is not installed

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)

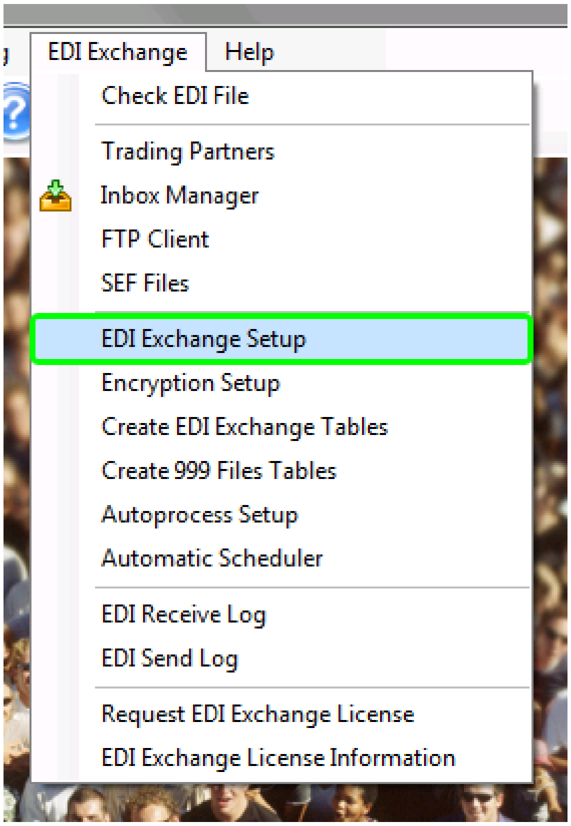
3. Download one of the following components you need according to your OS' bit depth:
   - Framework EDI Enterprise evaluation 32-bit
   - Framework EDI Professional evaluation 64-bit
4. Install downloaded components and start again the EDI Exchange initialization procedure.

7.3 Configuring EDI Exchange (Optional Settings)

7.3.1 Setting up Email Notifications

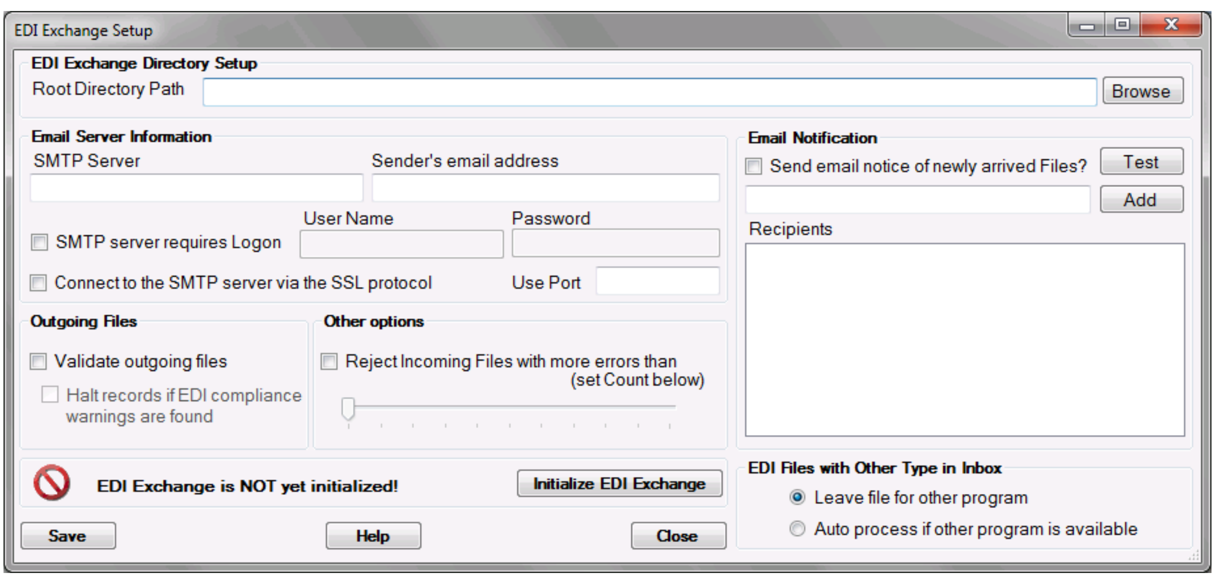
EDI Exchange can send emails to operators and trading partners to notify them about files and processing results. This functionality of EDI Exchange lies beyond the most basic setup that the initialization checks for. For this feature to work properly, you need to set up an email server which EDI Exchange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

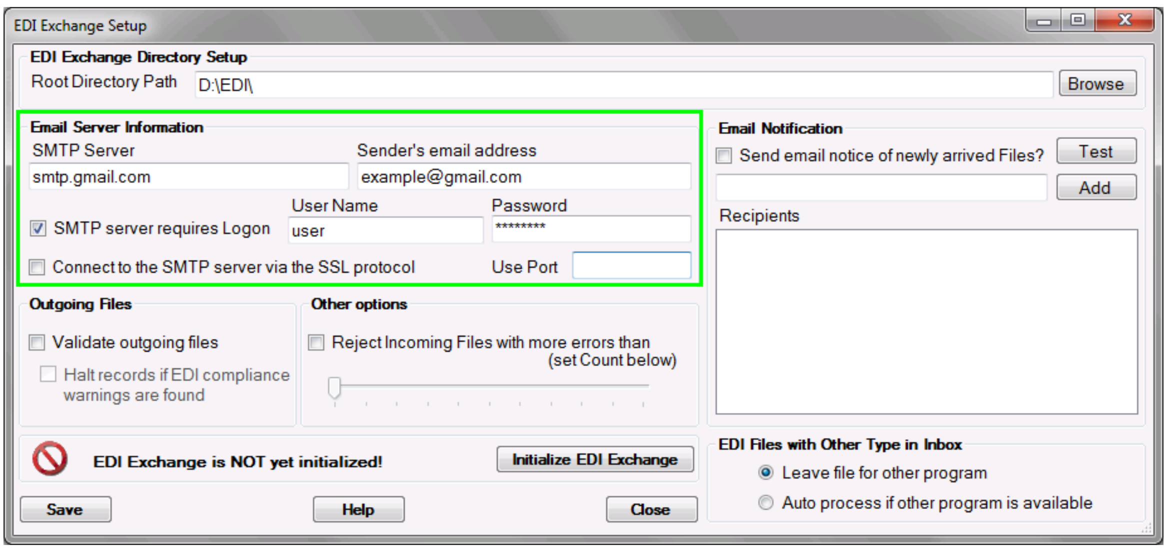


The "EDI Exchange Setup" window

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

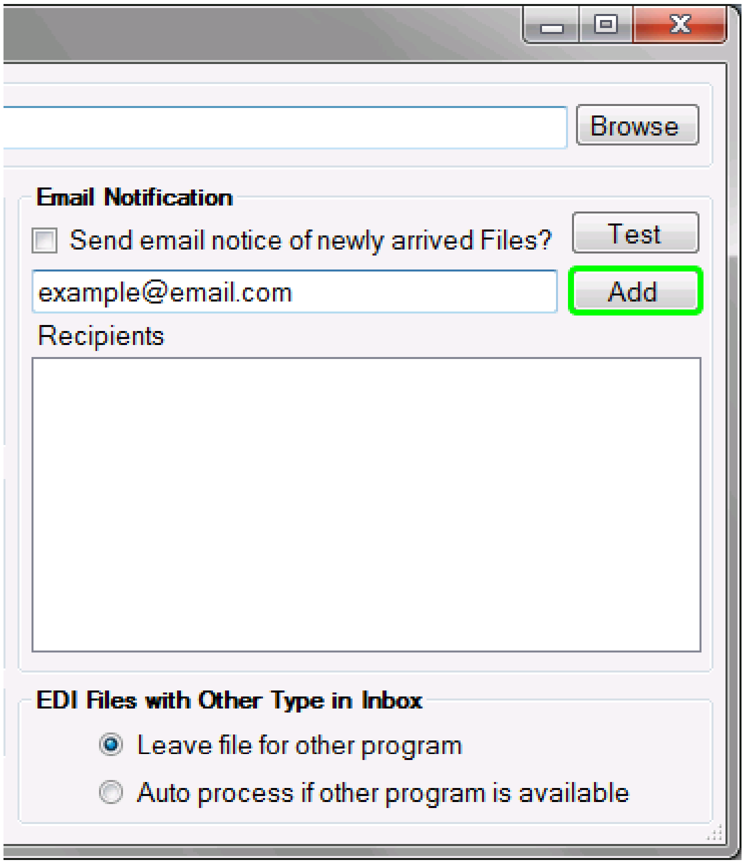
> Note: If you do not have this information, please ask your administrator to set this portion up for you.

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

Email Notification

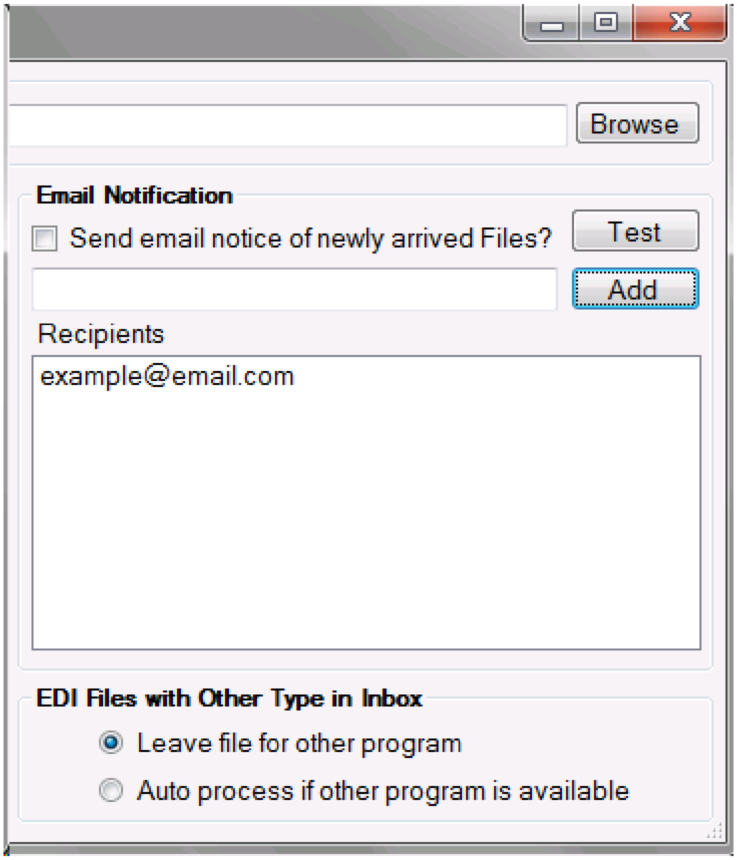
- **Send email notice of newly arrived files?** — Use this checkbox to define if you want to send email notice once new files have arrived.
- **Recipients** — You can add your staff's email(s) and the processing messages will be sent to these emails.

Enter an email address and click "Add."



Setting up the email recipients

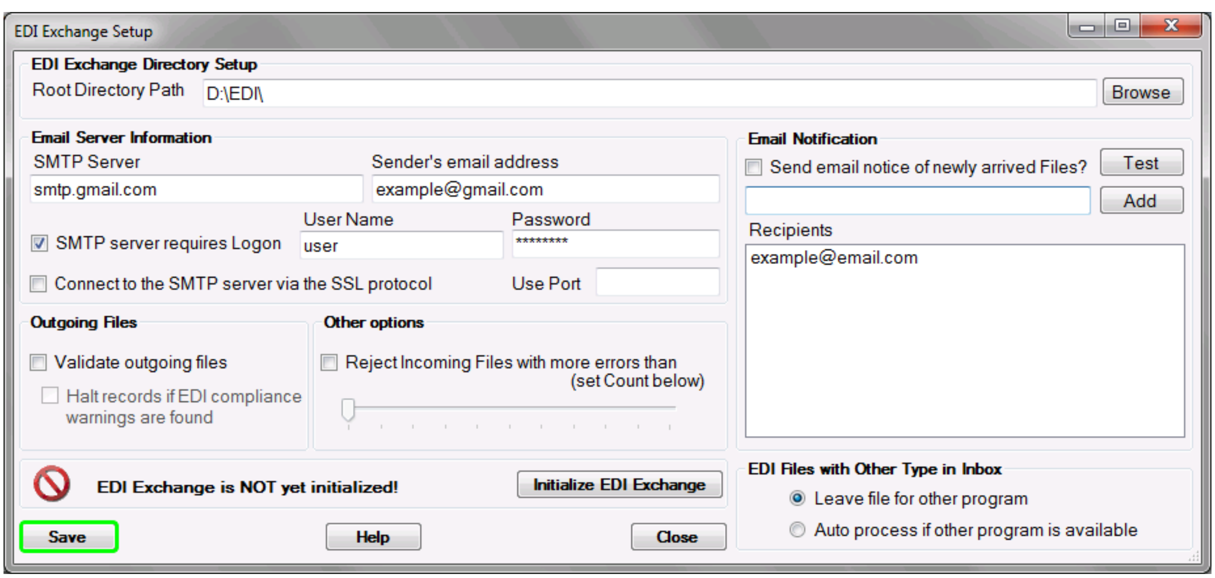
The email address will appear in the list.



Added email recipient

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

6. Click on the "Save" button.

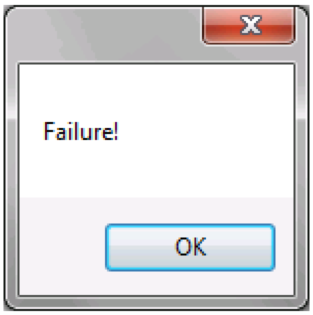


The "Save" button

Troubleshooting Email Settings

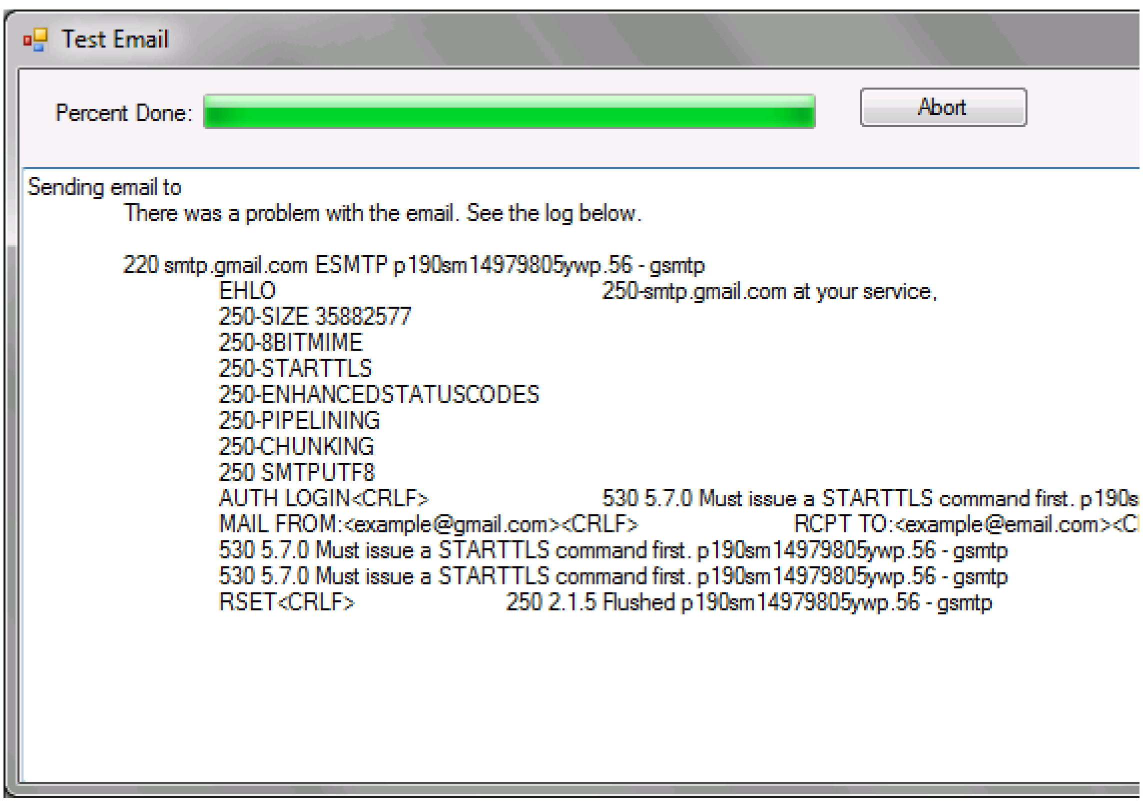
If you have problems with setting up the email server, please contact your administrator. He/ She should know values to specify and how to test the settings.

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.



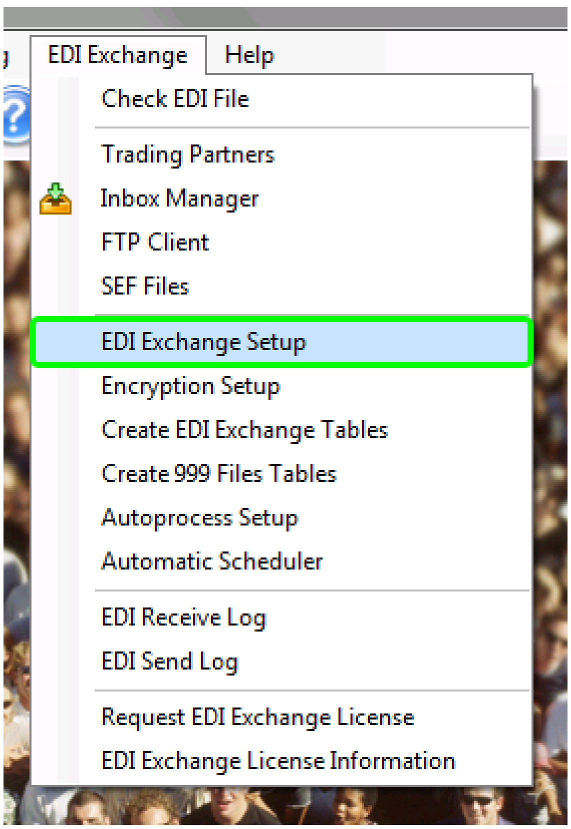
The process result screen with a detailed error message

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.

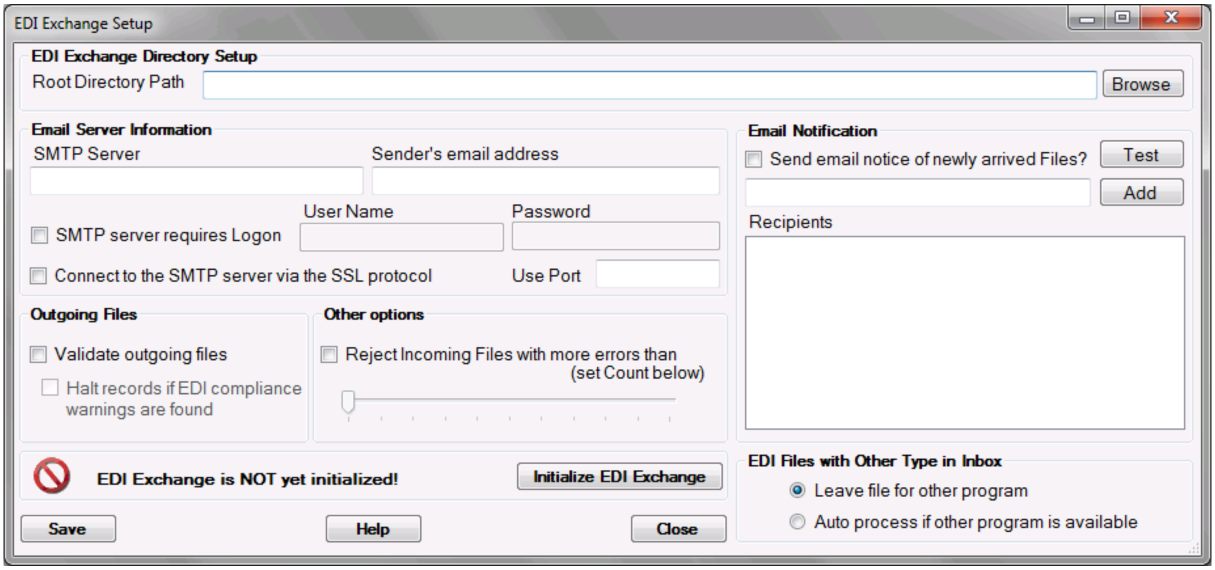
Follow the instructions below.

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



The "EDI Exchange Setup" menu item

2. The following window will appear.

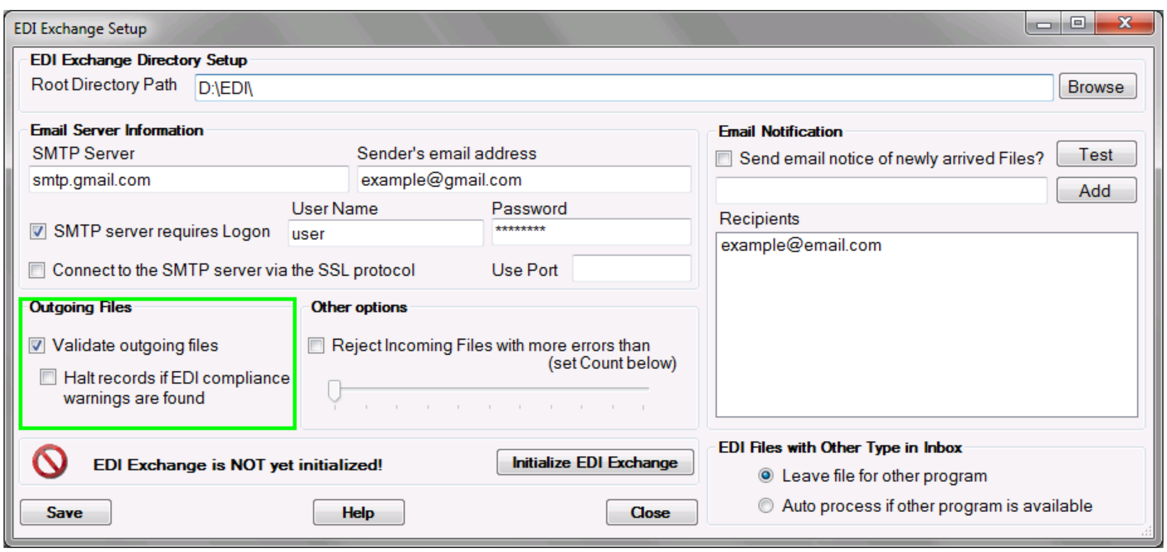


The "EDI Exchange Setup" window

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.

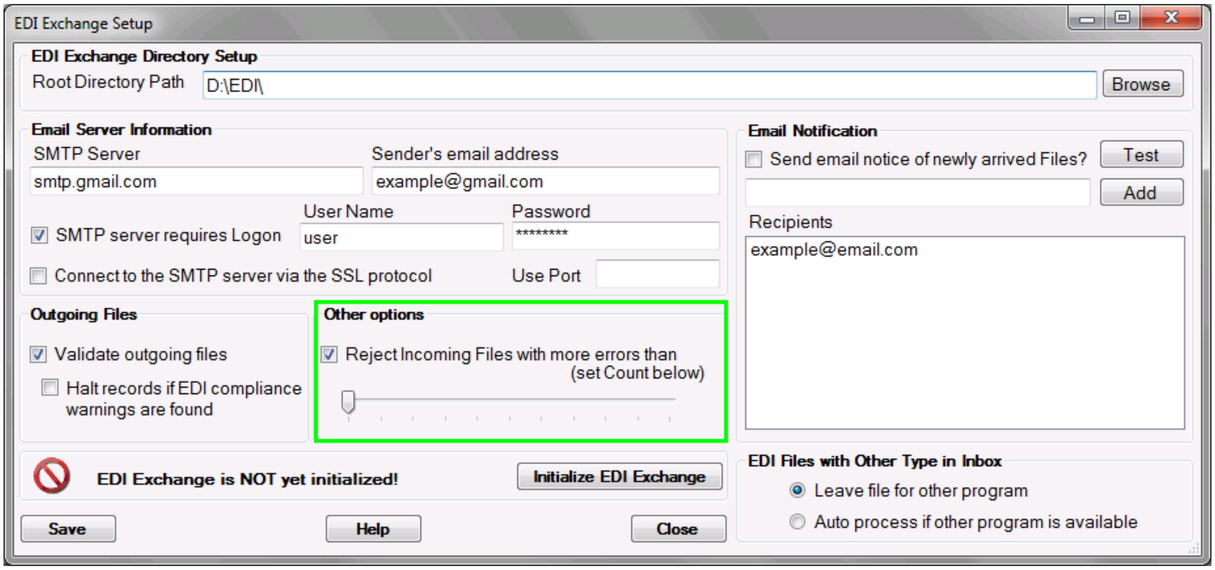


Validating outgoing files

4. Specify the following incoming files options:

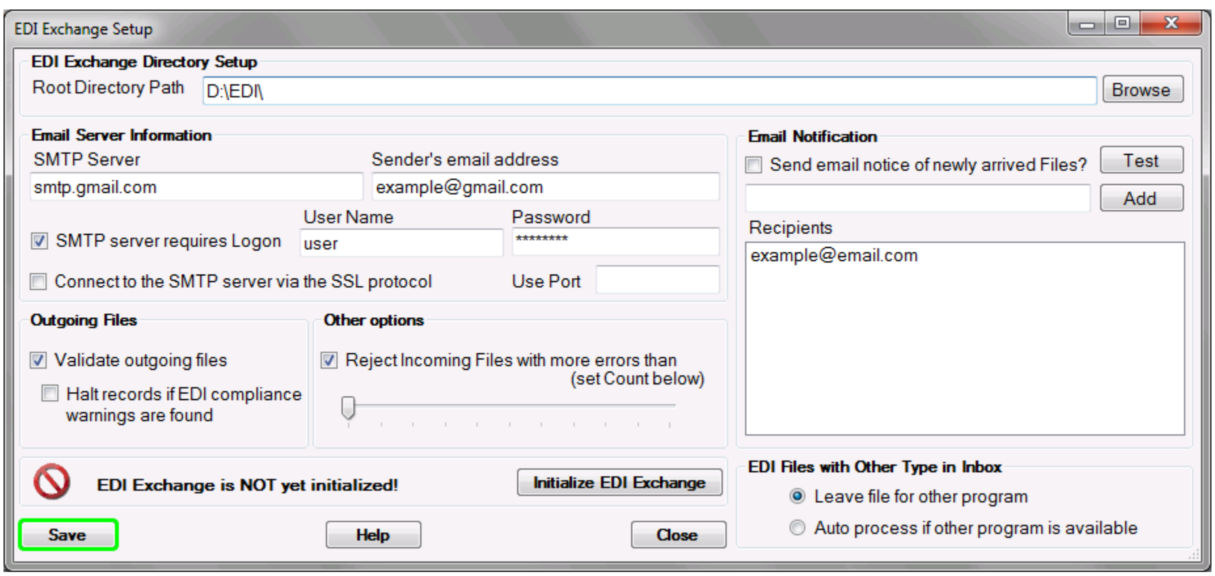
Other Options

- **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."

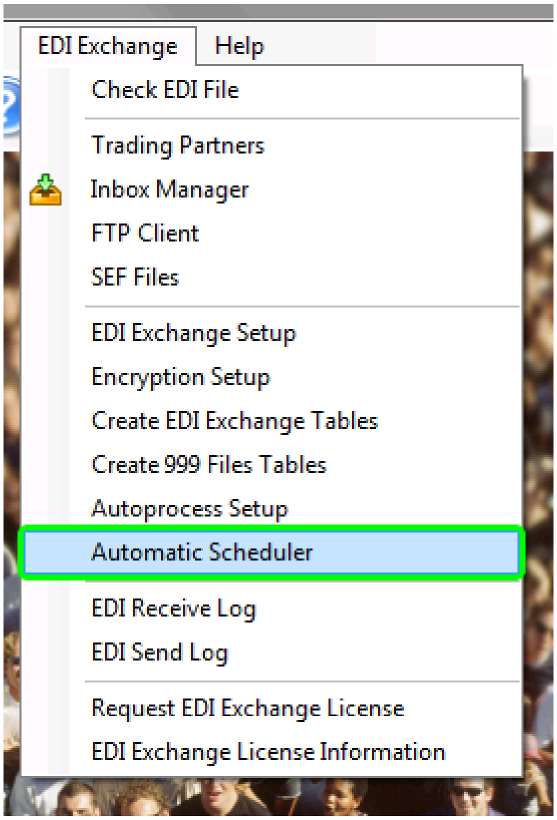


7.3.3 Running the Application via Scheduler

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.

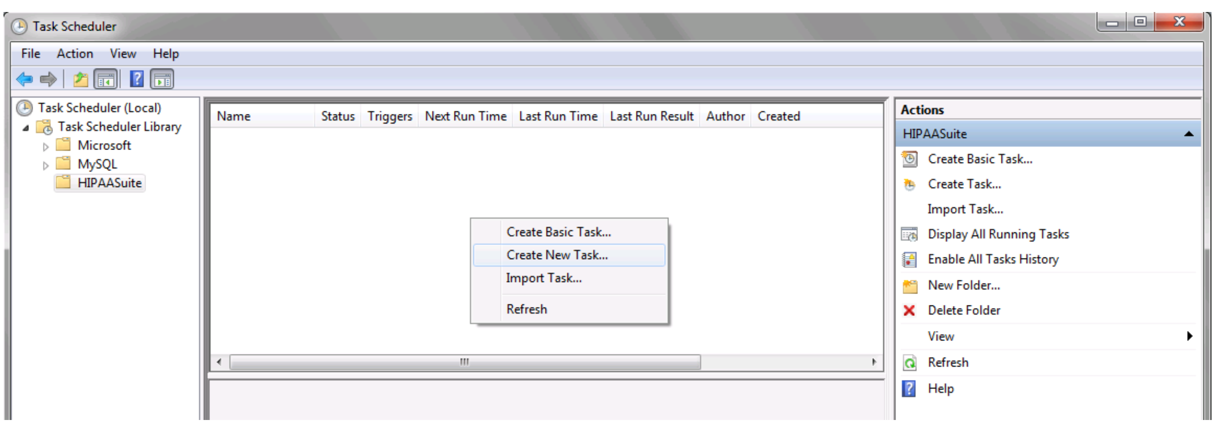
Follow the instructions below to schedule the EDI files exchange process.

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



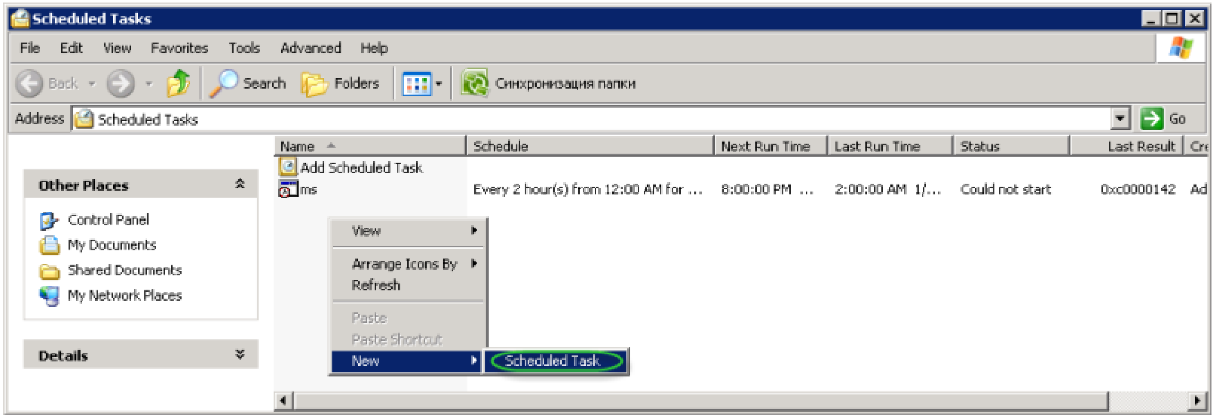
The "Automatic Scheduler" menu item

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.

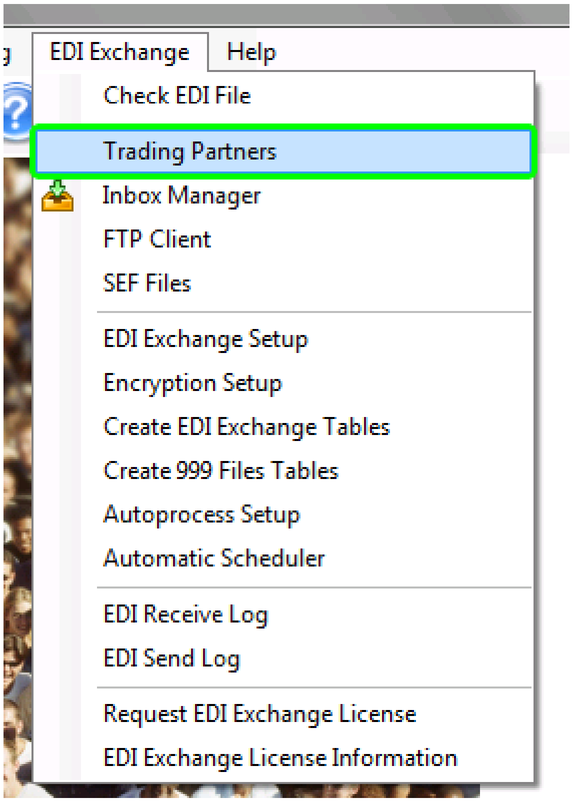
7.4 Working with Trading Partners

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.

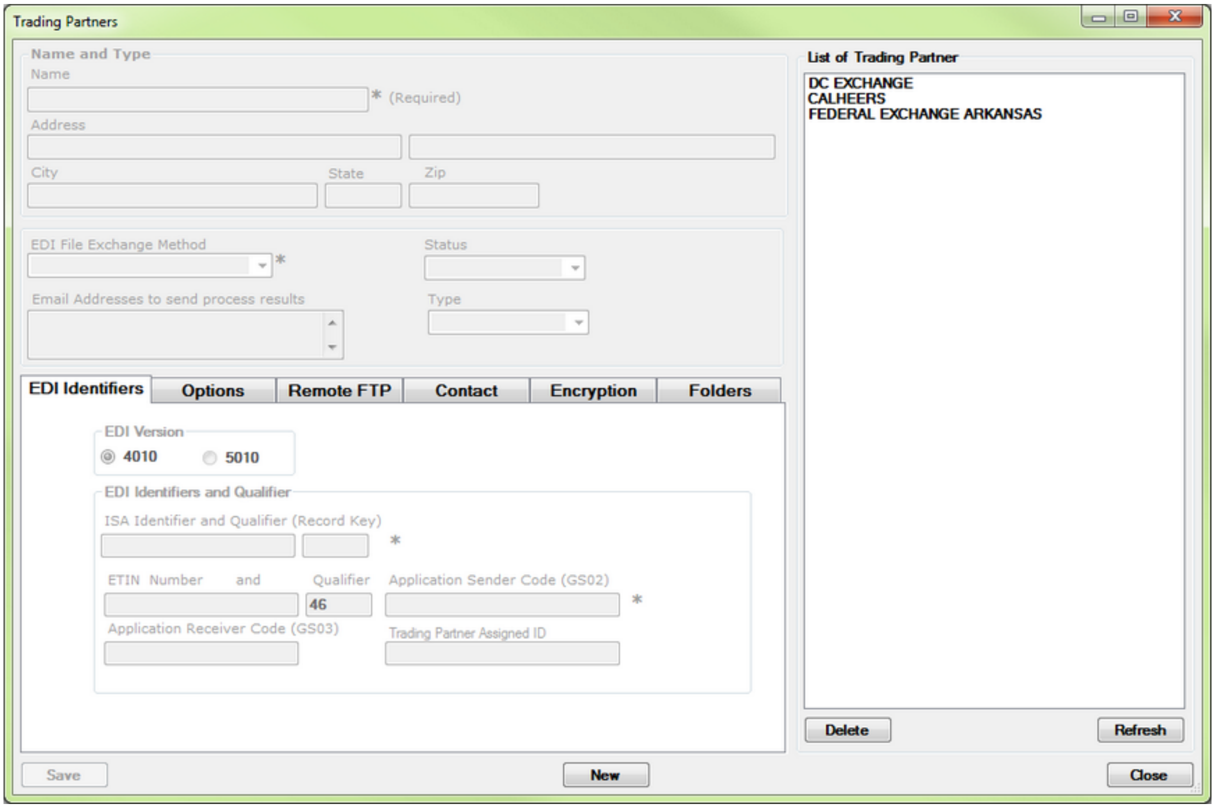
Once you have created the trading partner table (see Creating Database Tables) and initialized EDI Exchange (see Initializing EDI Exchange), you can set up the relationships with your trading partner. Follow the instructions below.

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



The "Trading Partners" menu item

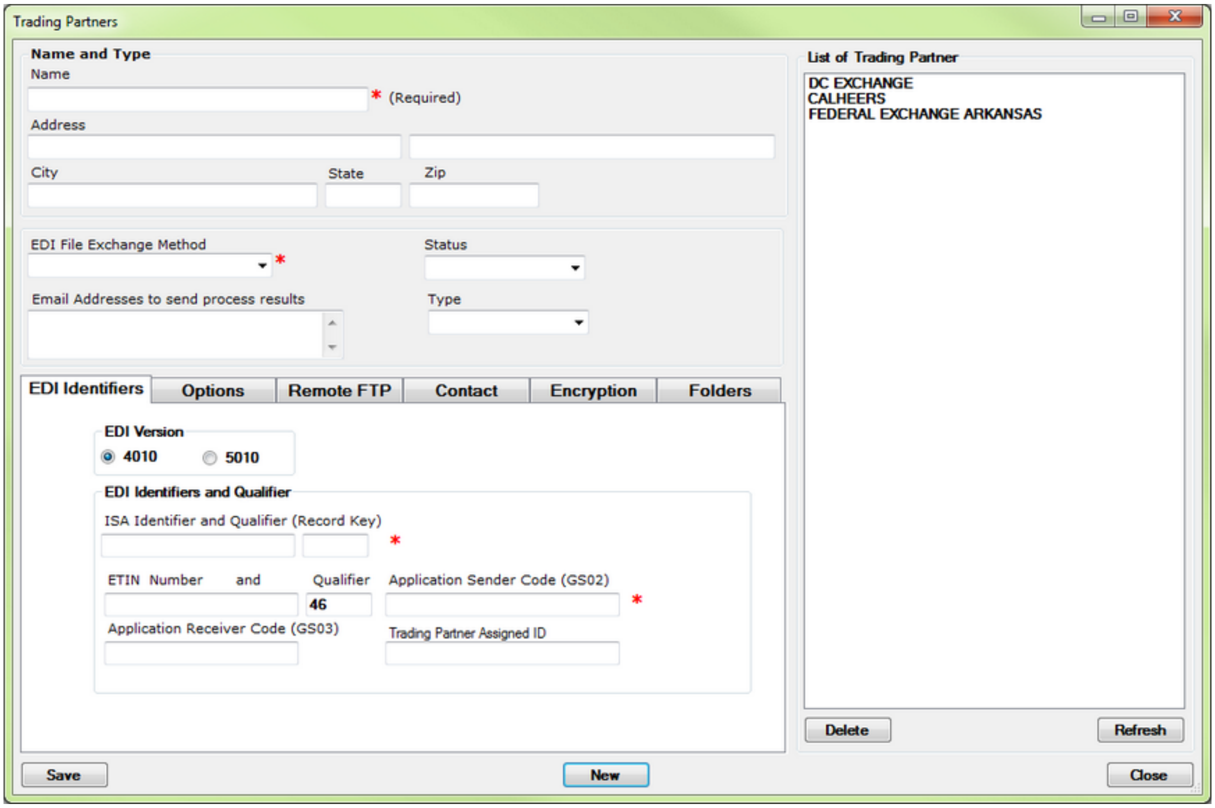
2. The following screen will appear.



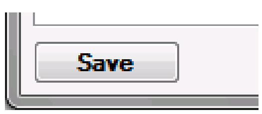
The "Trading Partners" window

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."

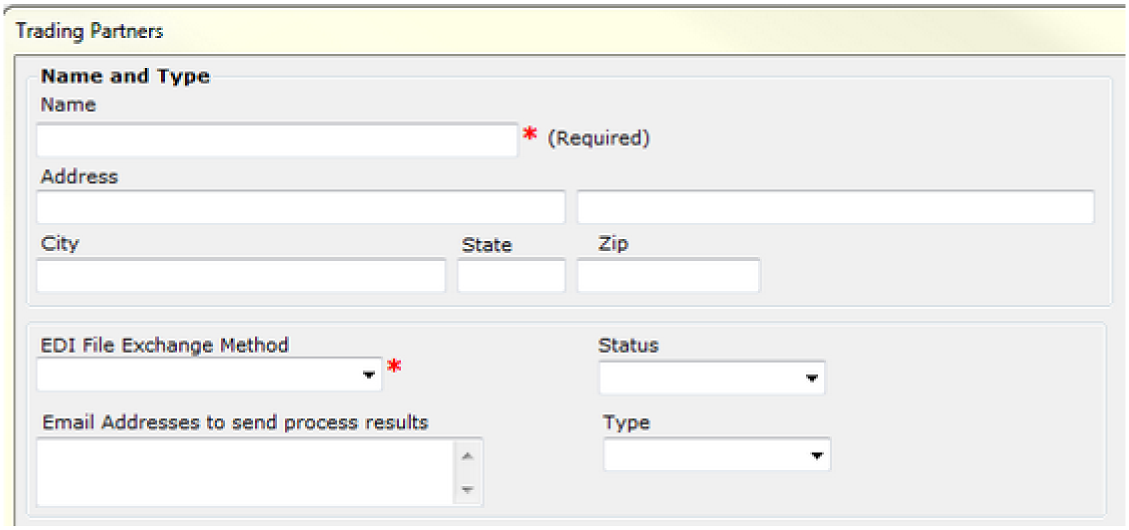


The "Save" button

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.

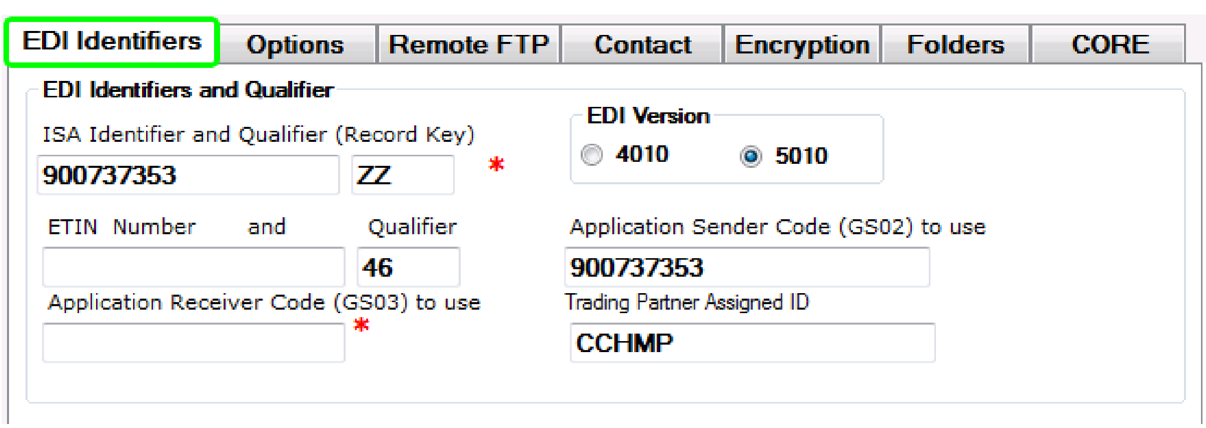
- **Payers** – Entities that pay for health care benefits such as health insurers.

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.
    - **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.

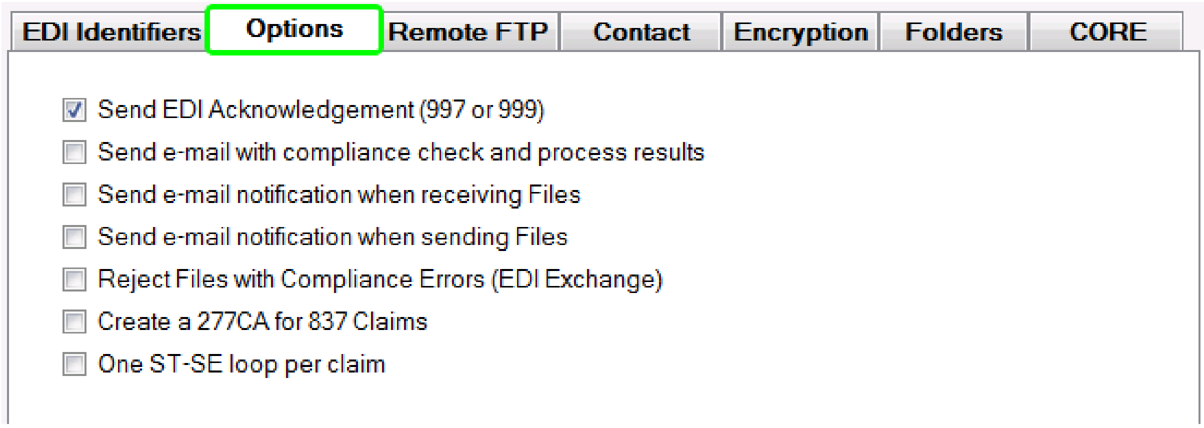


The "EDI Identifiers" tab

- **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



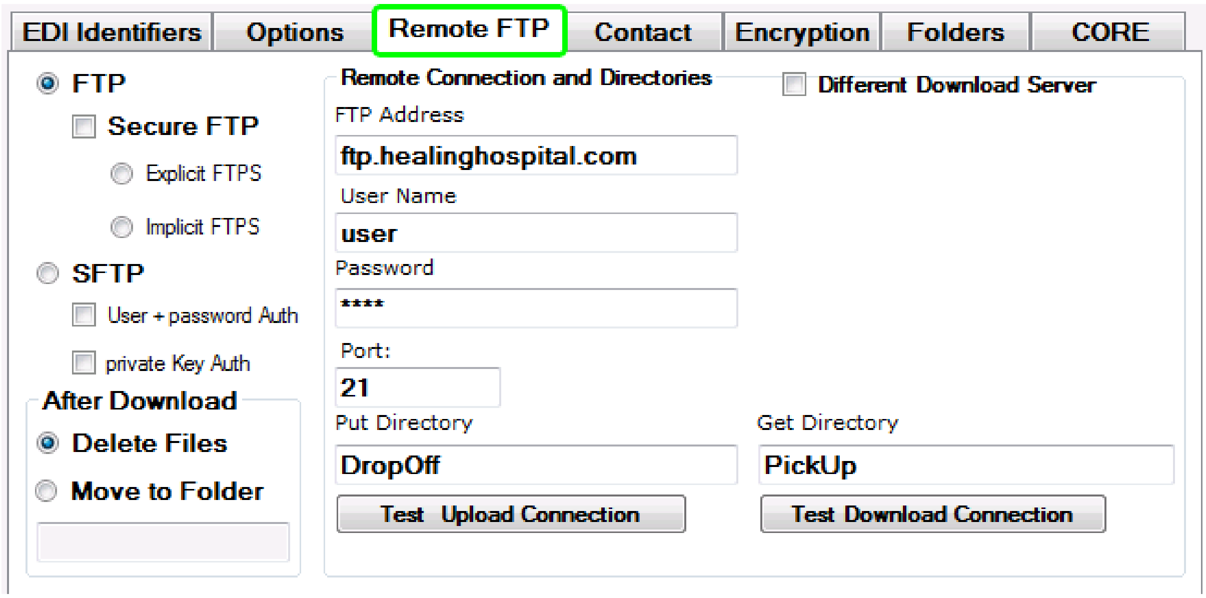
The "Options" Tab

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:

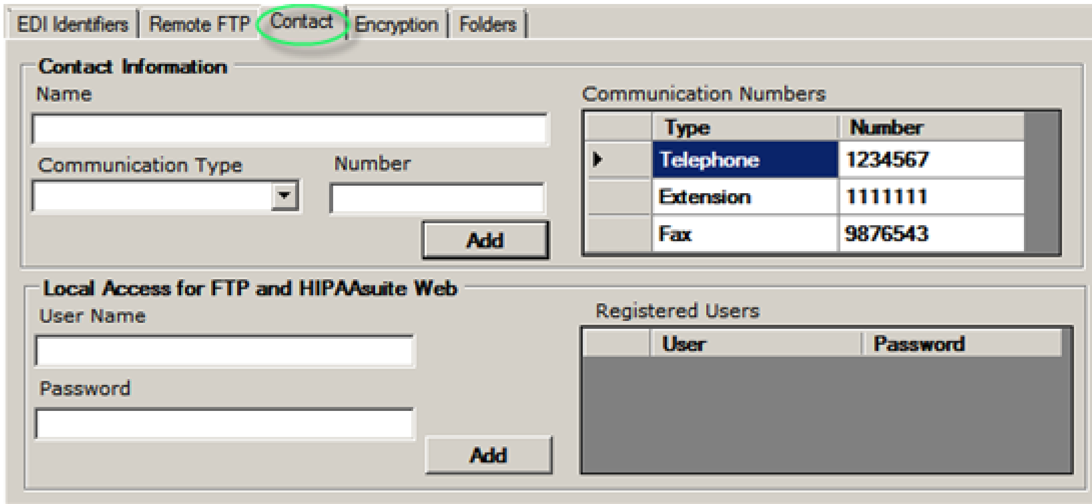
- **FTP Address -** This is usually the IP address of the server
- **User Name**
- **Password**
- **Put Directory -** This is the directory where you drop off files
- **Get Directory -** This is the directory where you download files from

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

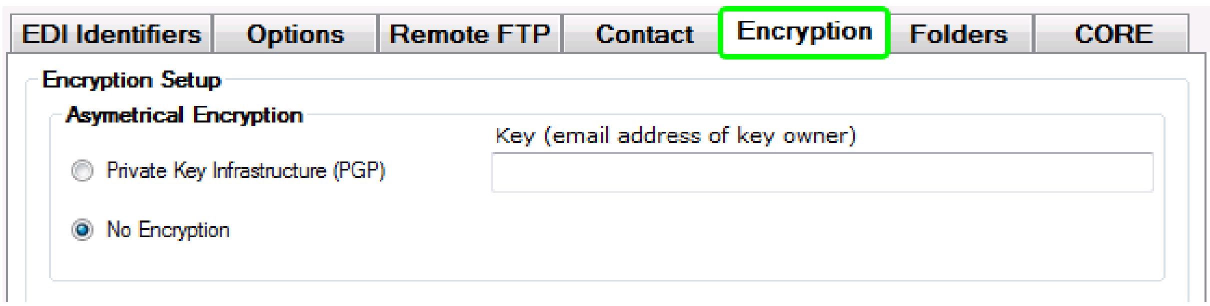
To register a user, enter the user name and the password into the corresponding fields and click the "Add" button. The user will appear in the "Registered Users" table.

- **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

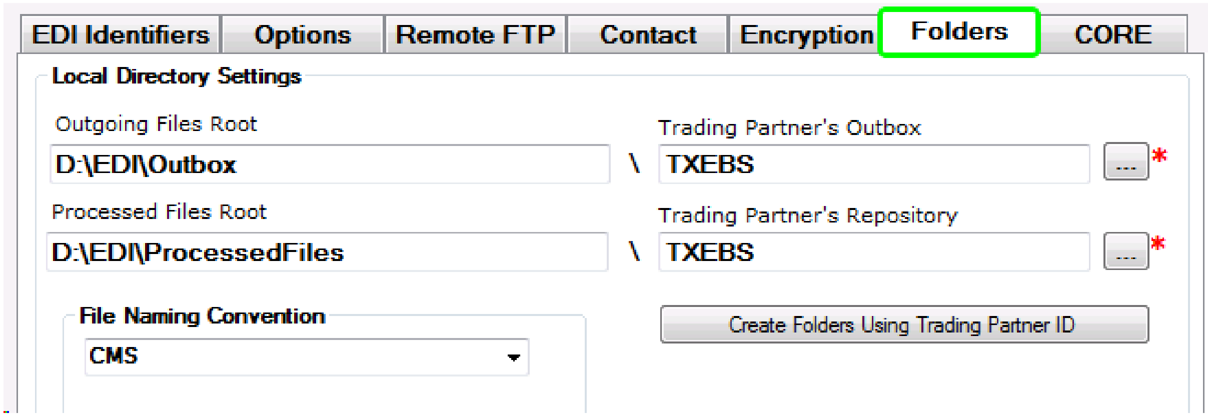
Encryption Setup

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

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

Folders Tab

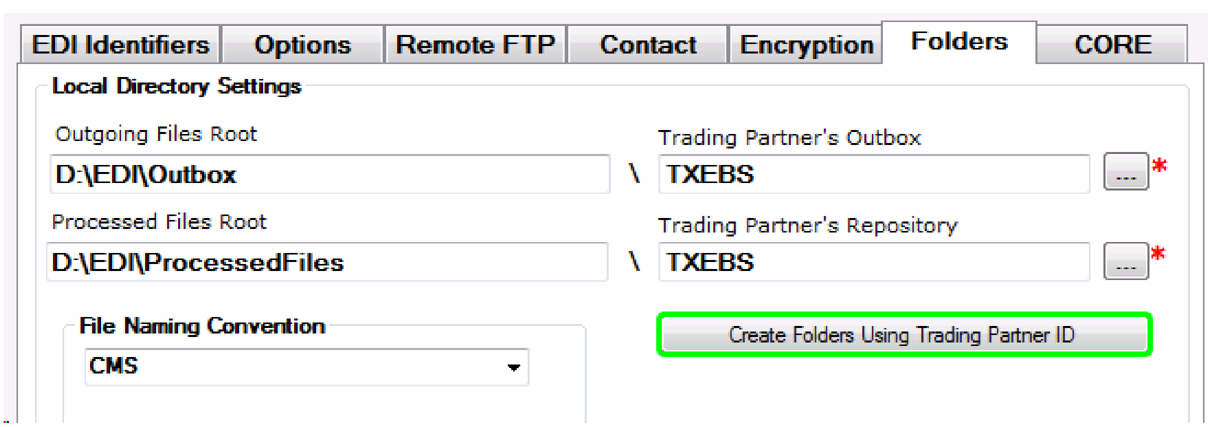
Within the HIPAAsuite Communications Directory, each Trading Partner has his own folder. This keeps files finely separated and in order. Here is where you can set this up. Read more in Defining Communications Directory.



The "Folders" tab

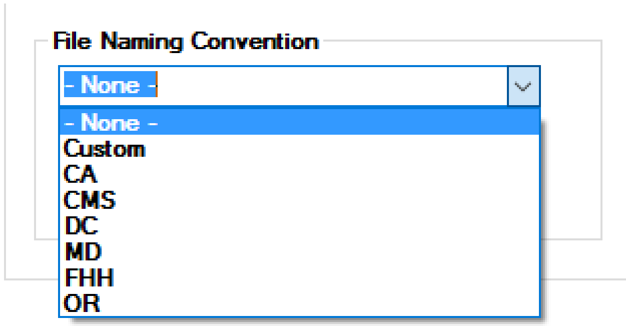
- **Outgoing Files Root** — This field has a pre-generated path. You can change this path by changing the EDI Root Directory.
- **Trading Partner's Outbox** — Mandatory setting. Click on the three-dots button to access the "Select Folder" window. There you choose an existing folder or create a new one.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

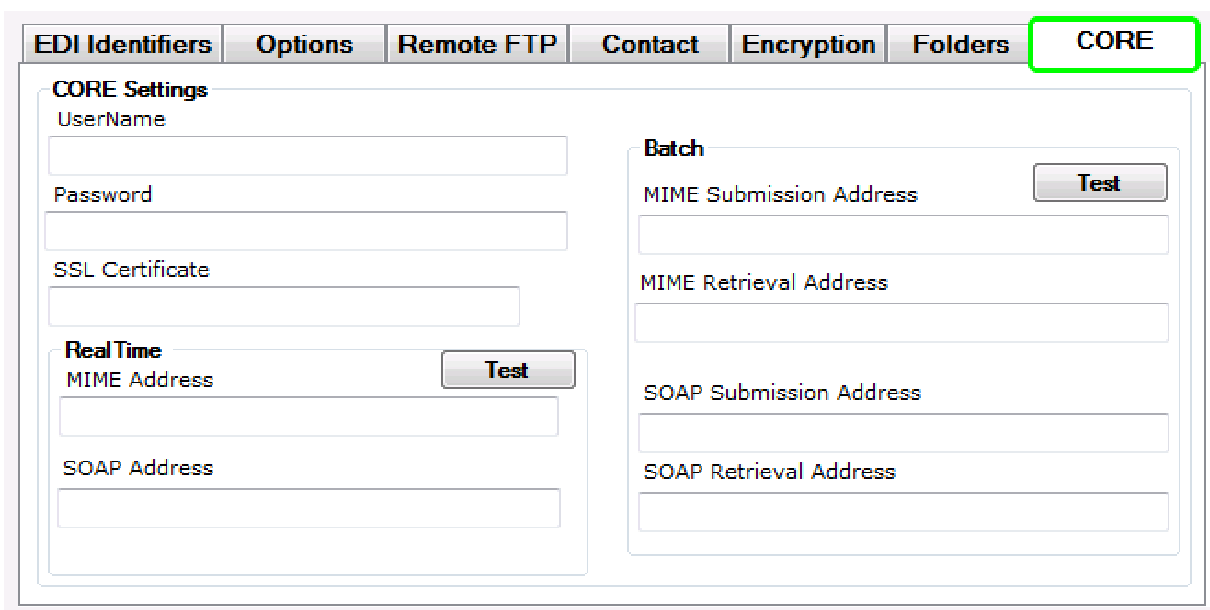


Filenaming dropdown menu options

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.

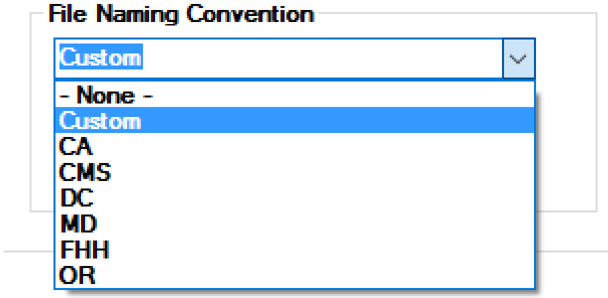


CORE settings tab

- **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.

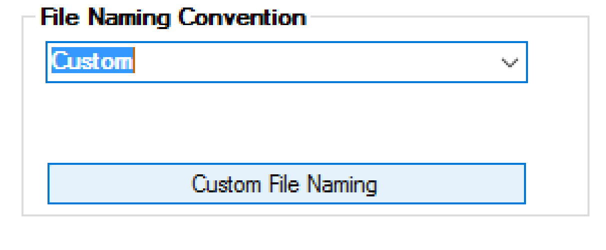
7.4.2 Custom File Naming Conventions

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.



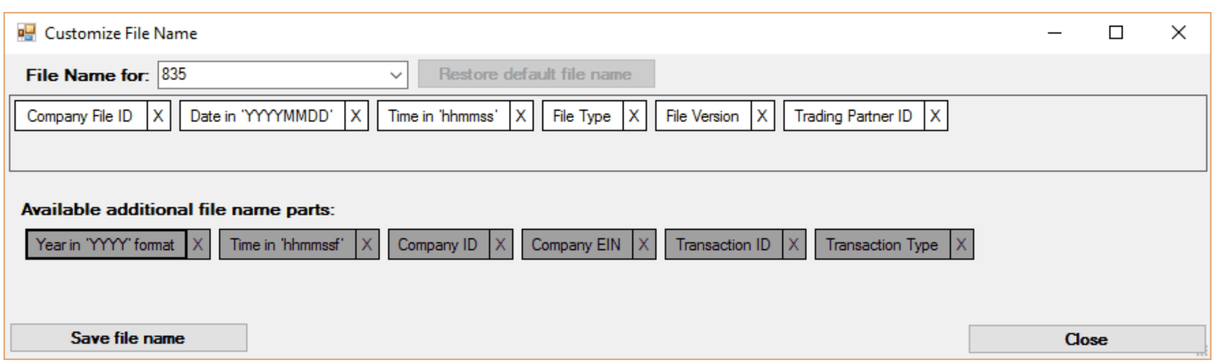
Custom File Naming Convention option highlighted

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

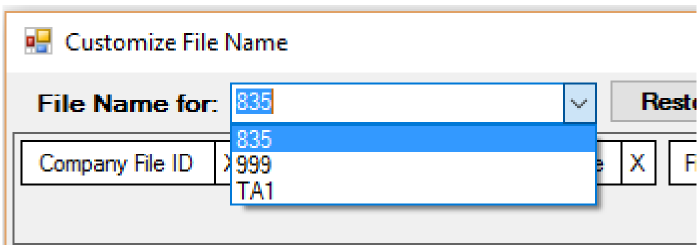
will bring up the screen pictured below. This screen is used to create file naming conventions for a particular trading partner. These examples will use the 835 file type as an example, but all file types the HIPAASuite product represents (as well as TA1s and 999s) can have their own file naming convention 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:



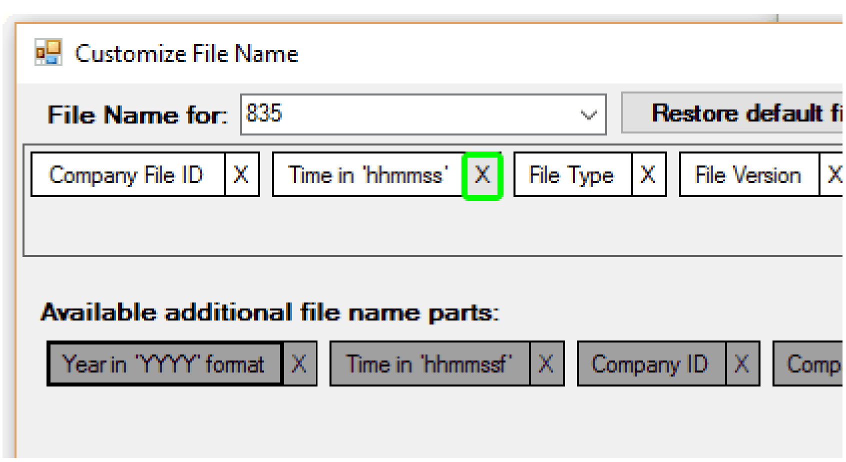
Changing the filetype

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:

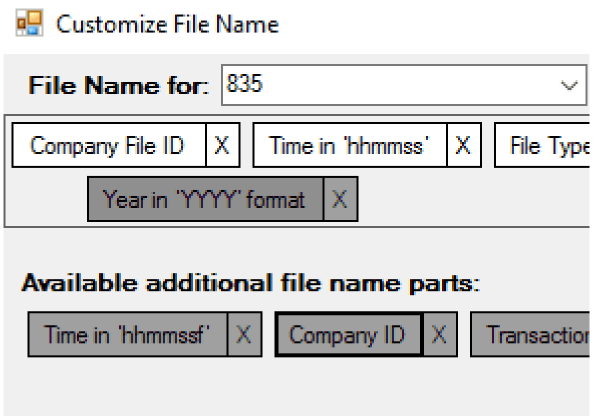
Click-dragging an element into position

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



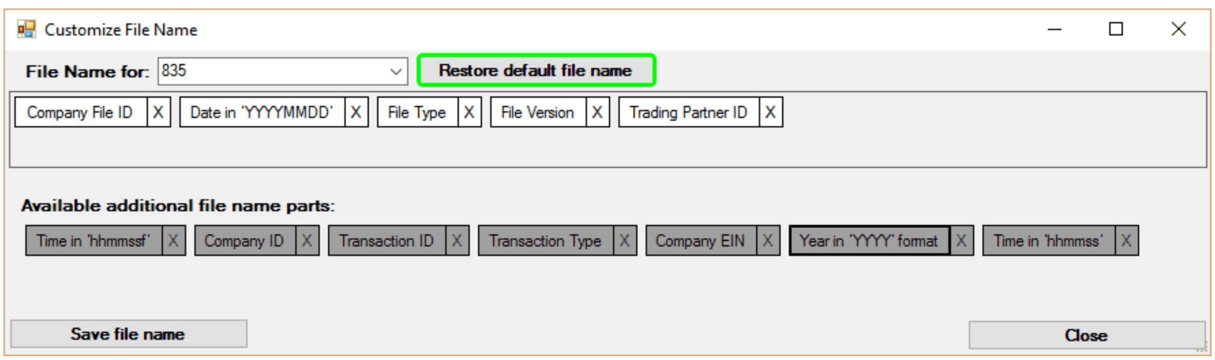
Deleting an element

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

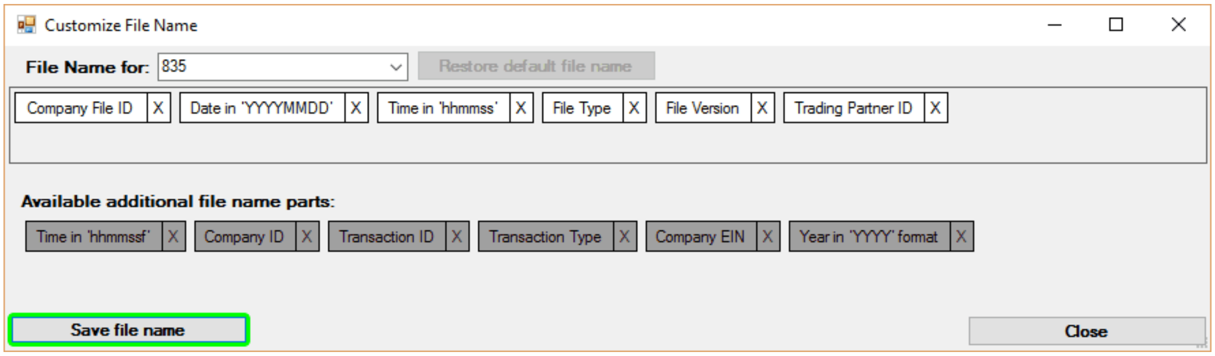
To discard the current changes and start over with the default file naming convention, click the *Restore default file name* button.



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*.



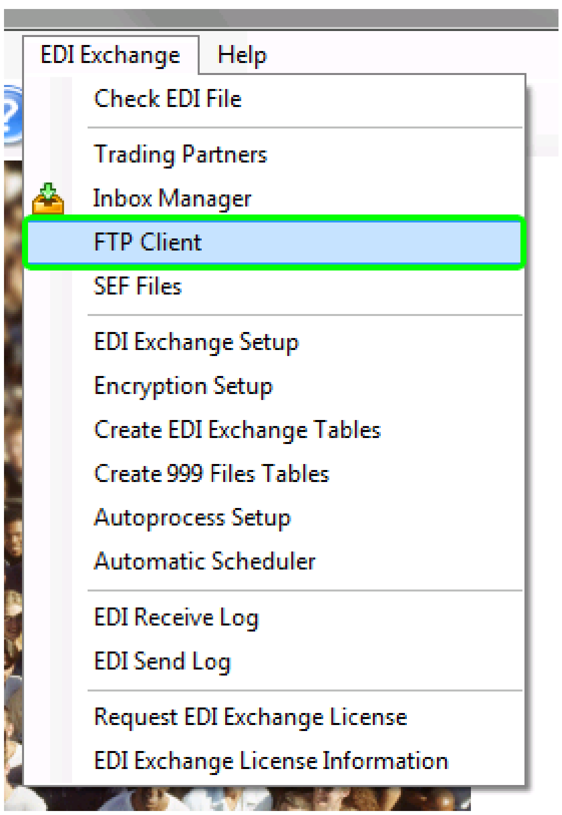
Save button on file name customization screen

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.)

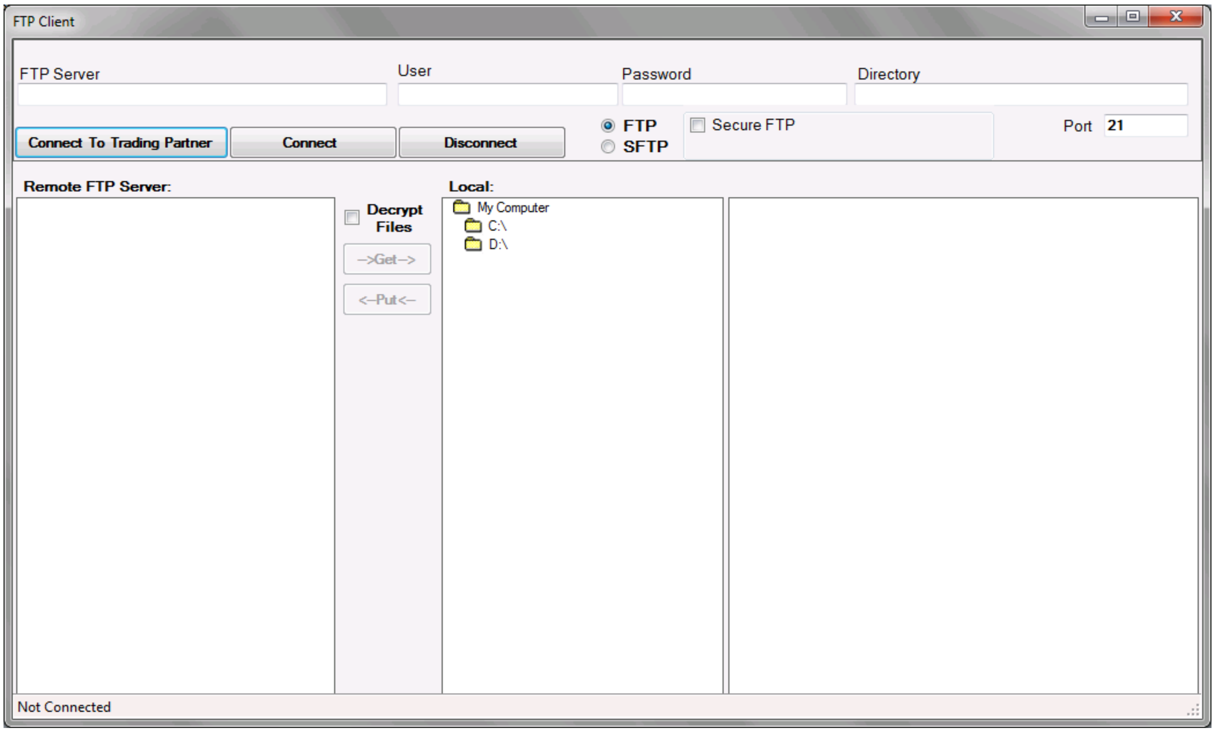
Follow the instructions below to exchange EDI files with your Trading Partner.

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



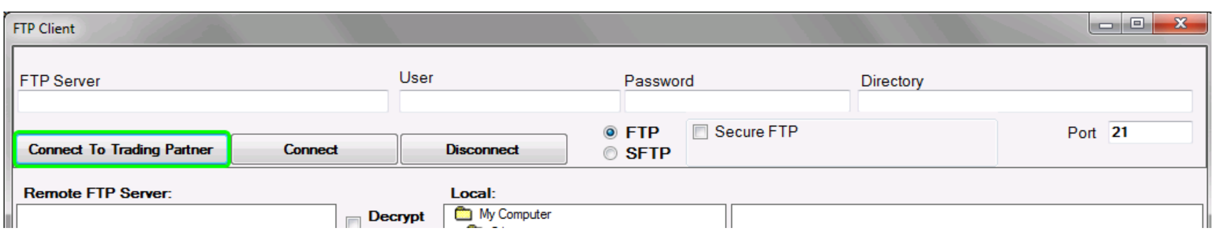
The "FTP Client" menu item

2. The following window will appear.



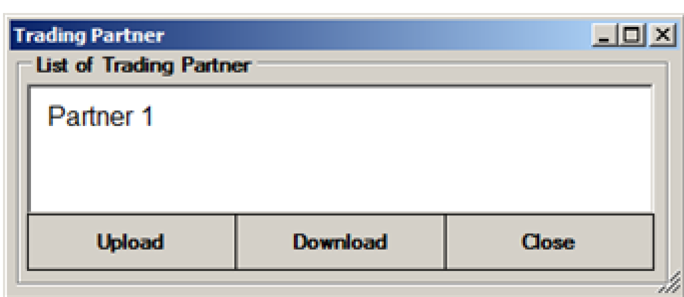
The built-in FTP client

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



The "Connect to Trading Partner" button

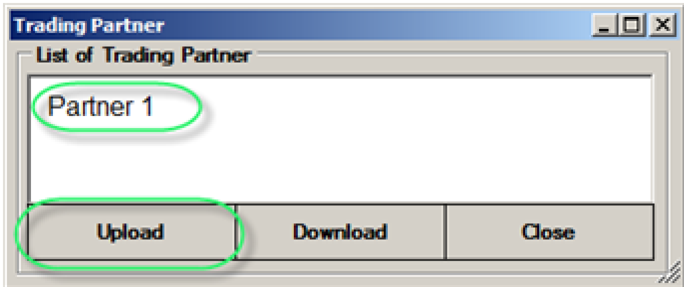
4. The following screen opens.



Selecting a Trading Partner for FTP transfer

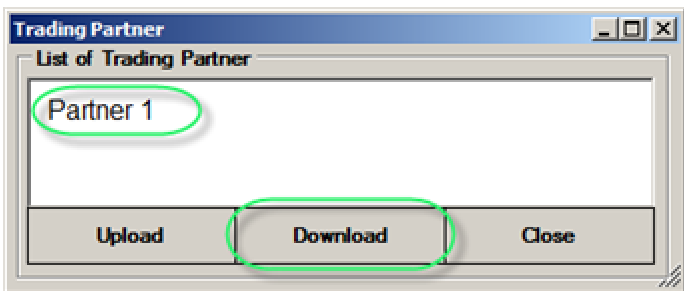
5. Highlight the trading partner that you want to connect to.

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.

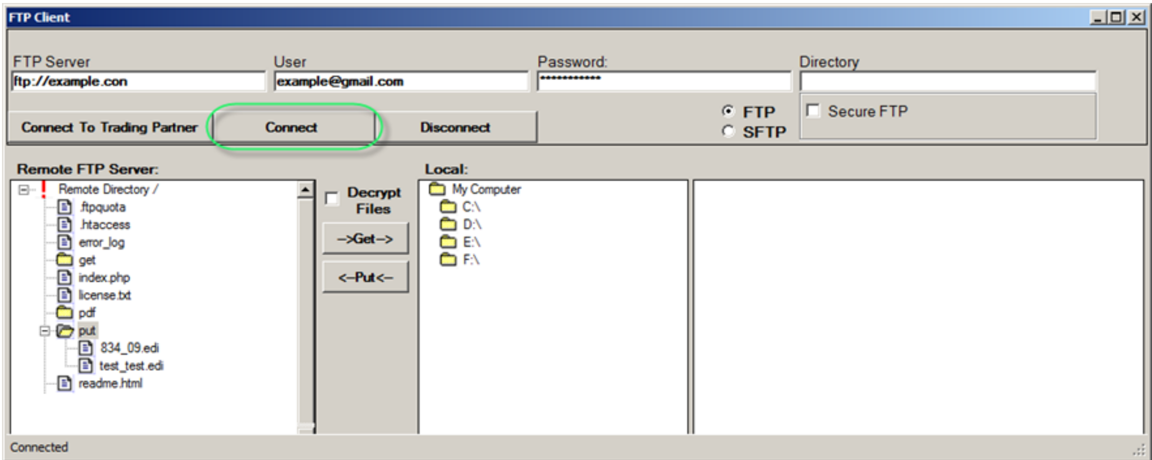


The "Download" button

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.

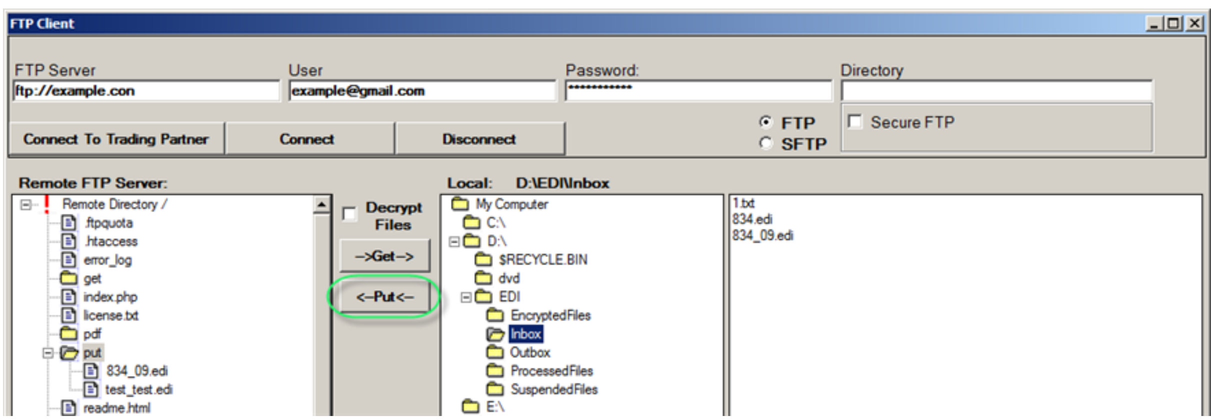
- **FTP server** — IP Address or URL of the FTP server.
- **Username**
- **Password**
- **Directory —** If you leave this value blank, the FTP root directory will be opened.
- **Secure FTP** — If you enable this option, then you can select between implicit and explicit FTPs. See Setting up Trading Partners 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.

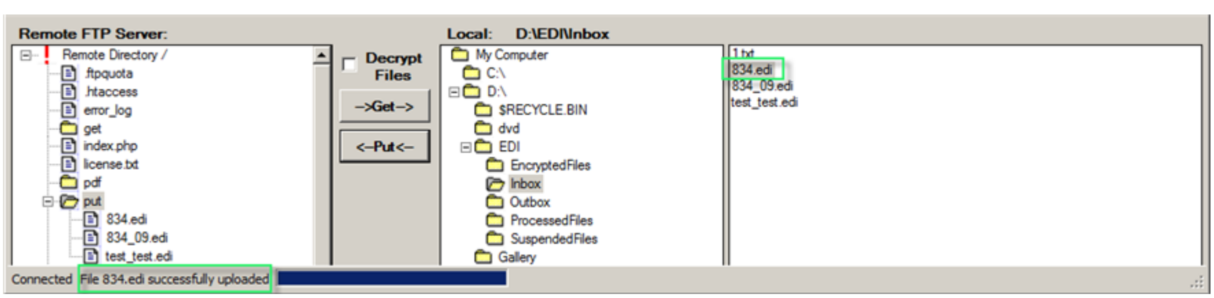


4. Once connected, the content of the folder on the server is displayed. On the right side, you can browse your local PC.

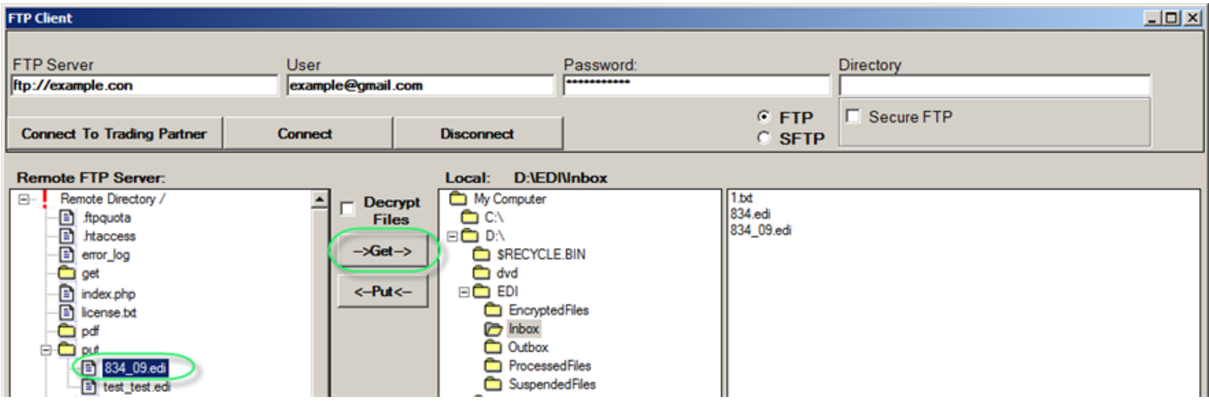
5. To upload a file to the server, select the file on your local PC and click on the "Put" button.



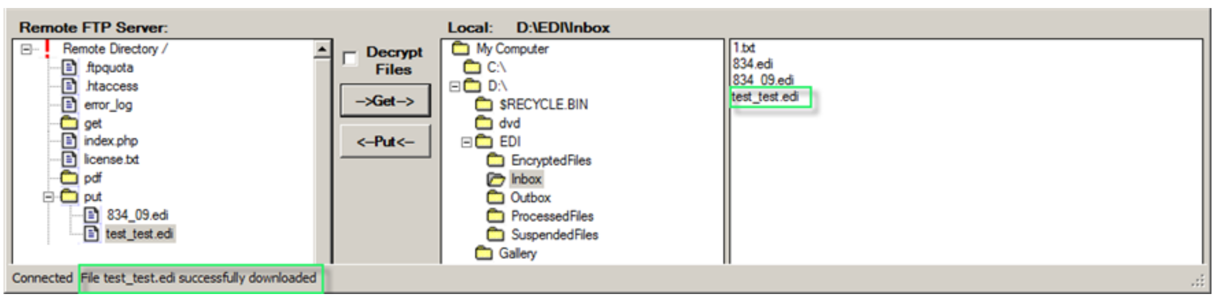
The file will appear in the remote folder. You will receive the "File <filename> successfully uploaded" message on the bottom status bar of the FTP client.



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

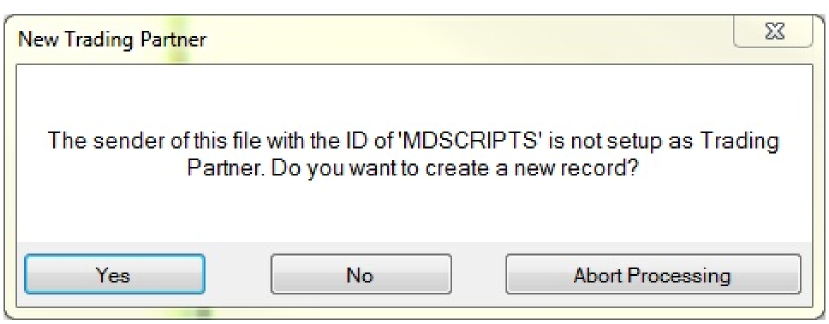


The file will appear in the local folder. You will receive the "File <filename> successfully downloaded" message on the bottom status bar of the FTP client.



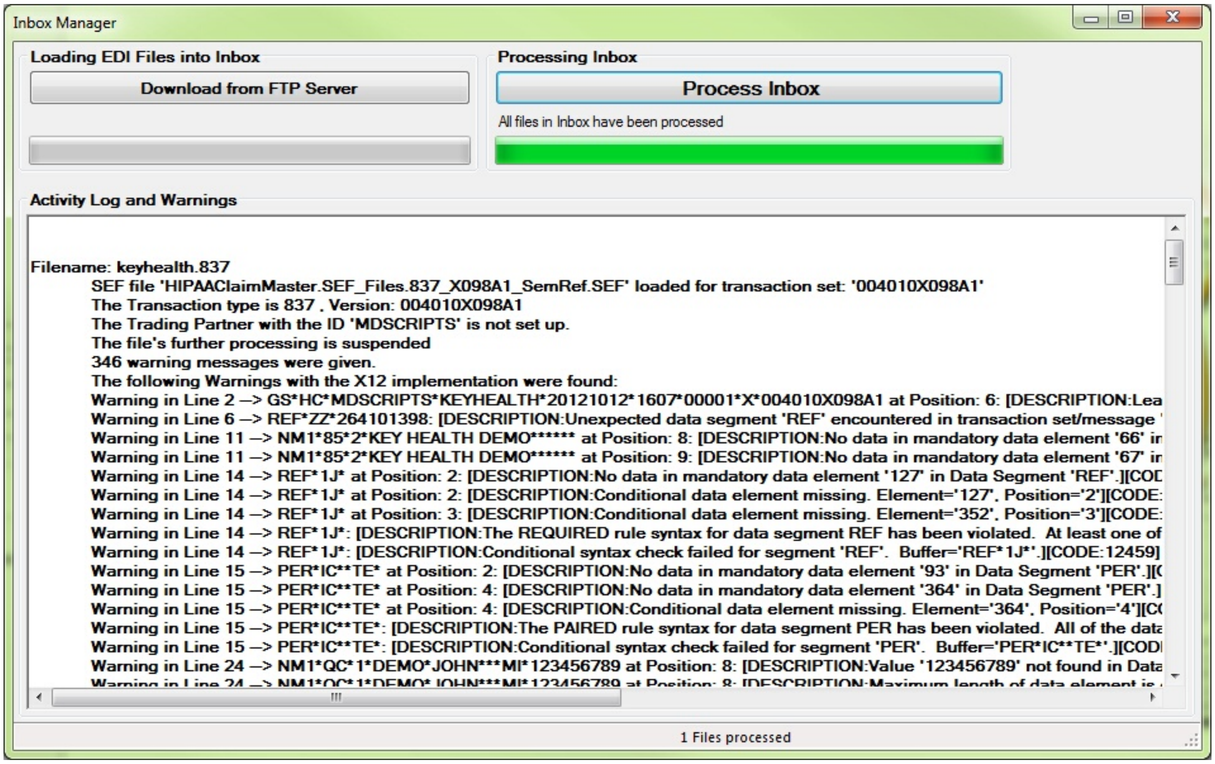
7.4.4 Creating a Trading Partner Automatically

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.



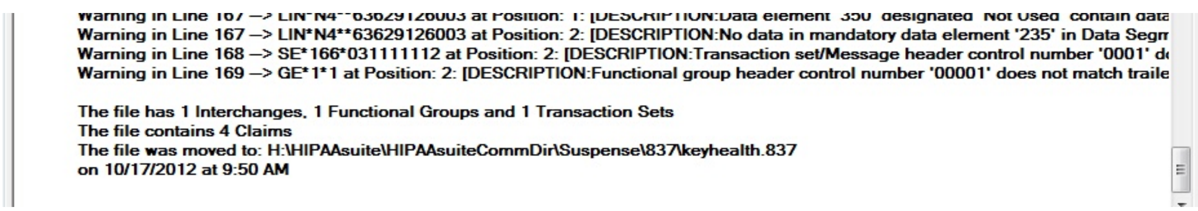
The "New Trading Partner" dialog box

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

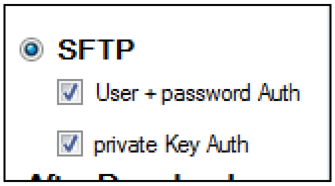
SFTP or FTP over secure shell as it is also known is deemed to be the most secure method of file transport. There are 3 methods of authentication in Sftp.

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.



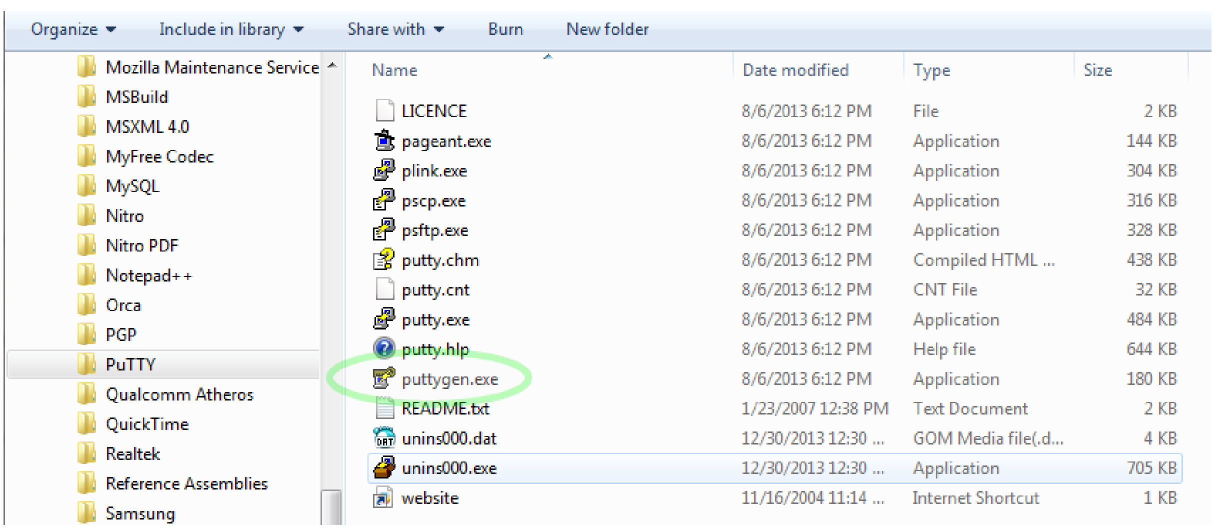
The sub choices when you select SFTP

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.

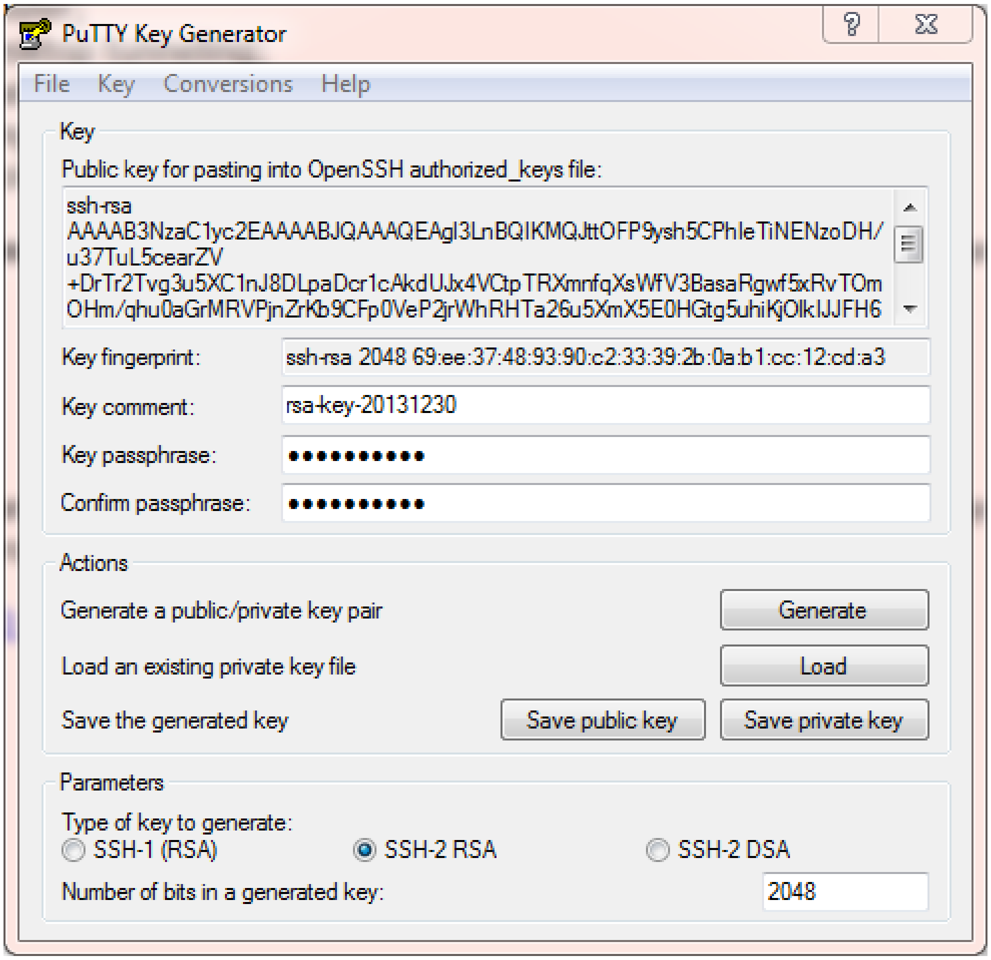
How do you create such a certificate? Here is one way:

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.



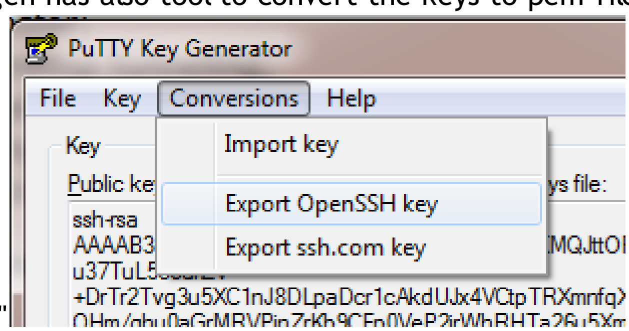
The programs and files that come with putty

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:

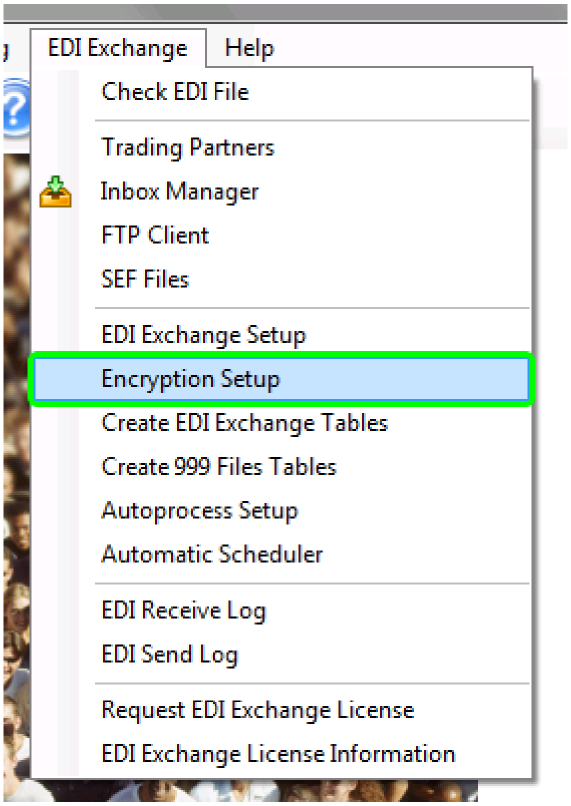
- A certificate authority (CA) that both issues and verifies the digital certificates.
- A registration authority which verifies the identity of users requesting information from the CA.
- A central directory is a secure location to store and index keys.
- A certificate management system.

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

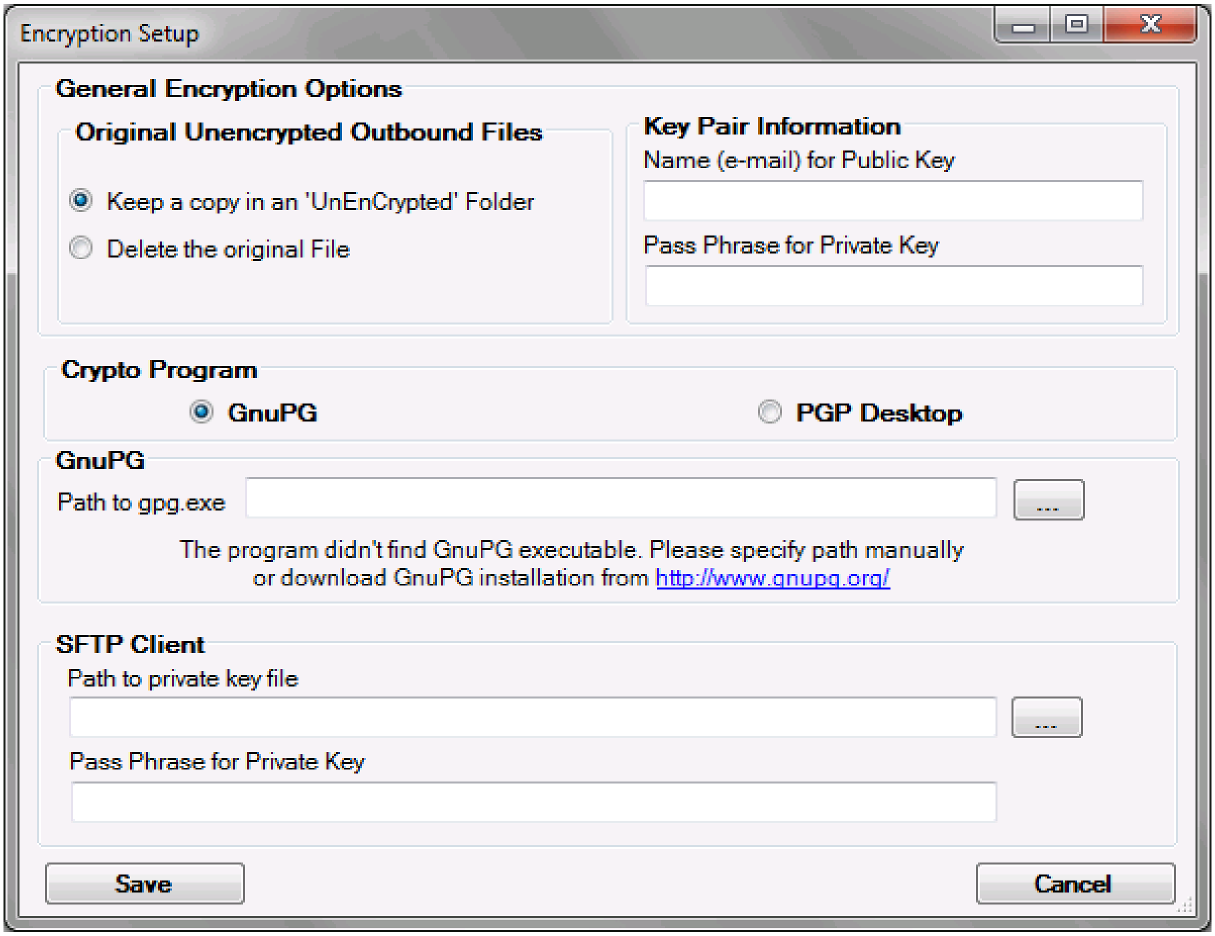
EDI Exchange allows you to set up the encryption for your EDI files. Follow the steps below.

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.

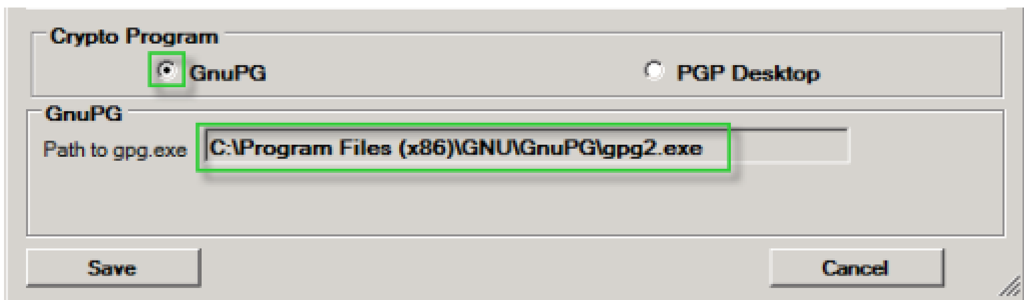
  - **Delete the Original File** — If you do not want to keep the unencrypted copy, select this option.

- **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.

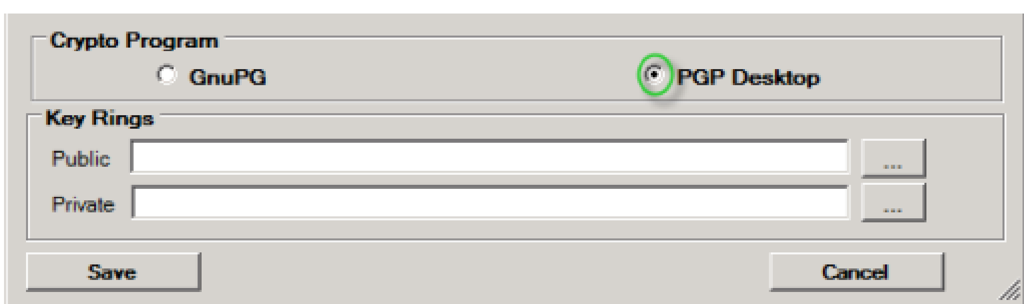
- **Crypto Program**
  - **GnuPG** – Select this option if you have already installed the GnuPG software and want to use it.



The configuration using GnuPG

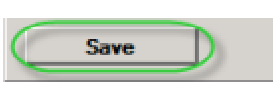
Note: When you select GnuPG, the program checks if the executable `gpg.exe/gpg2.exe` is present on your computer. If it is not found, you will have to specify the path manually or install the program first.

  - **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.

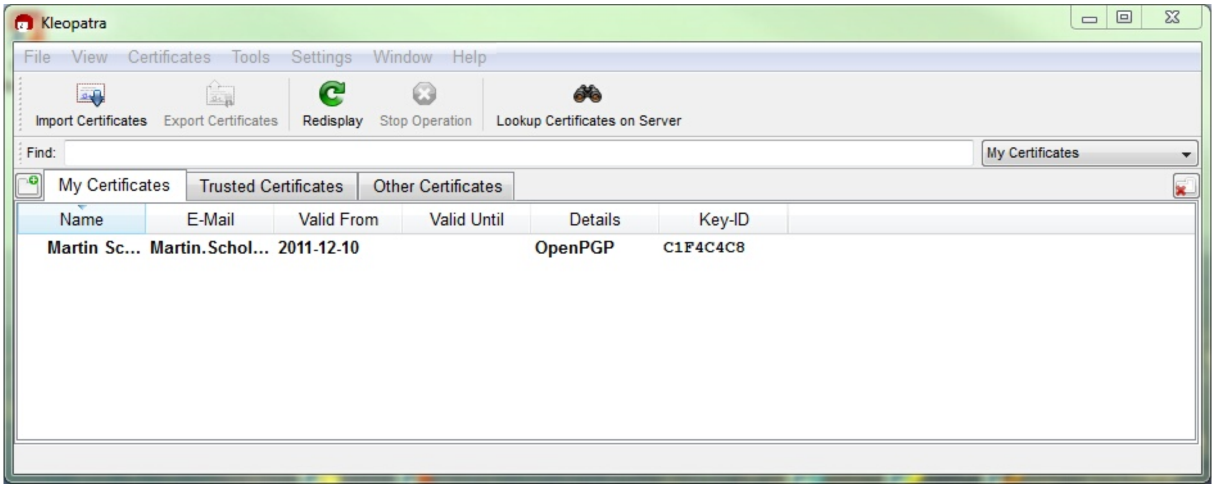
3. Encryption Management Server. See System Requirements.

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.

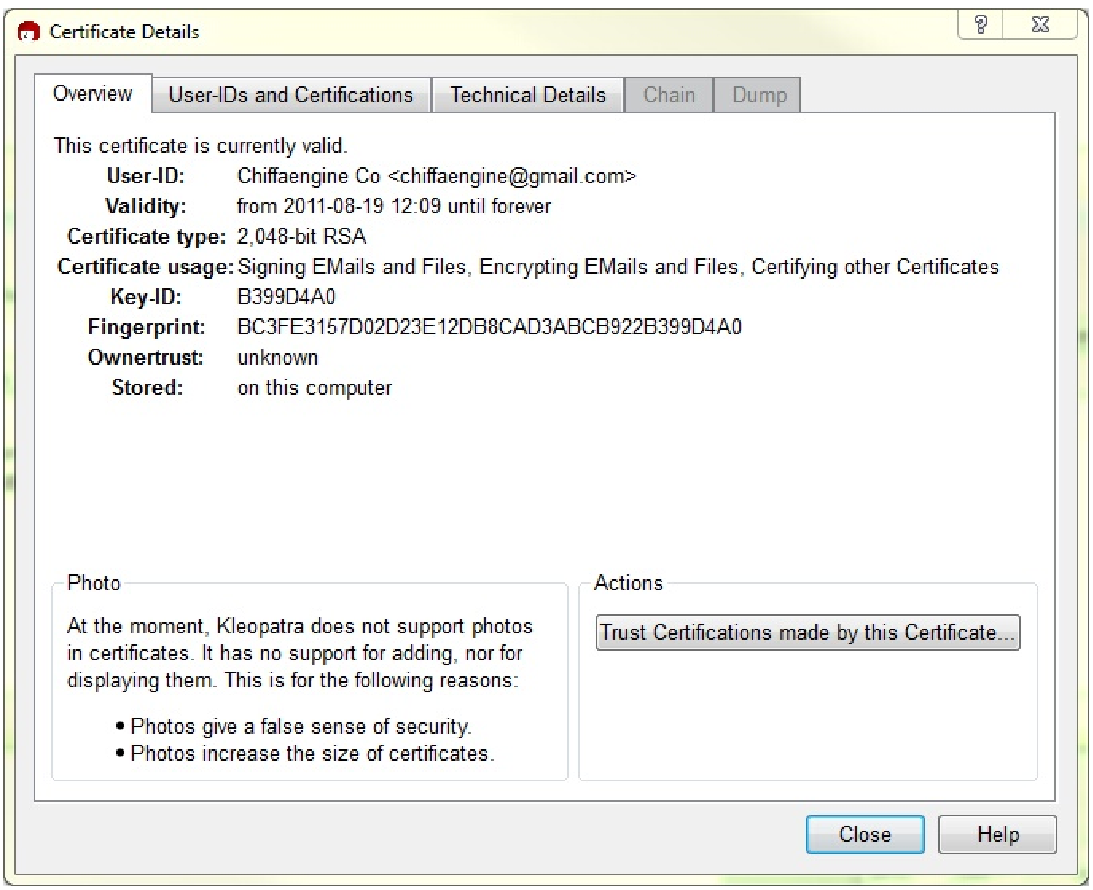
GnuPG is a free software, so it can be freely used, modified and distributed under the terms of the GNU General Public License.

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.



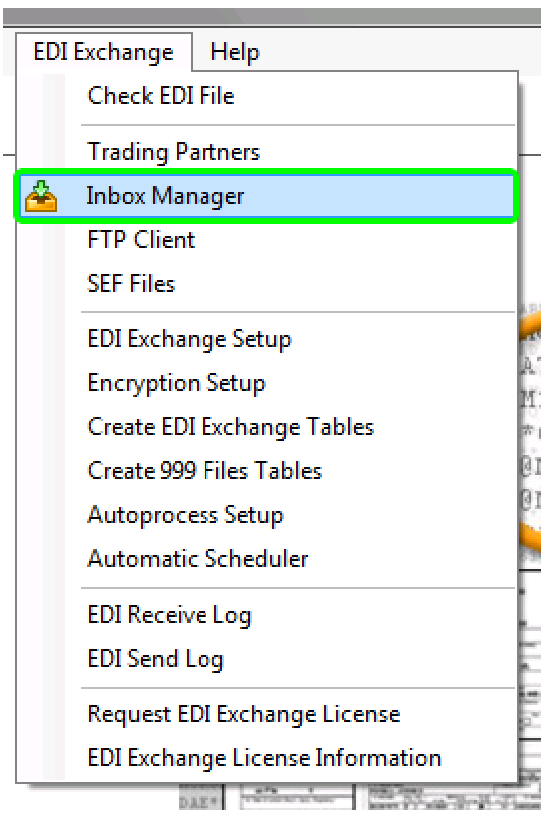
Certificate details with Kleopatra

7.6 Using EDI Exchange Features

7.6.1 Accessing Inbox Manager

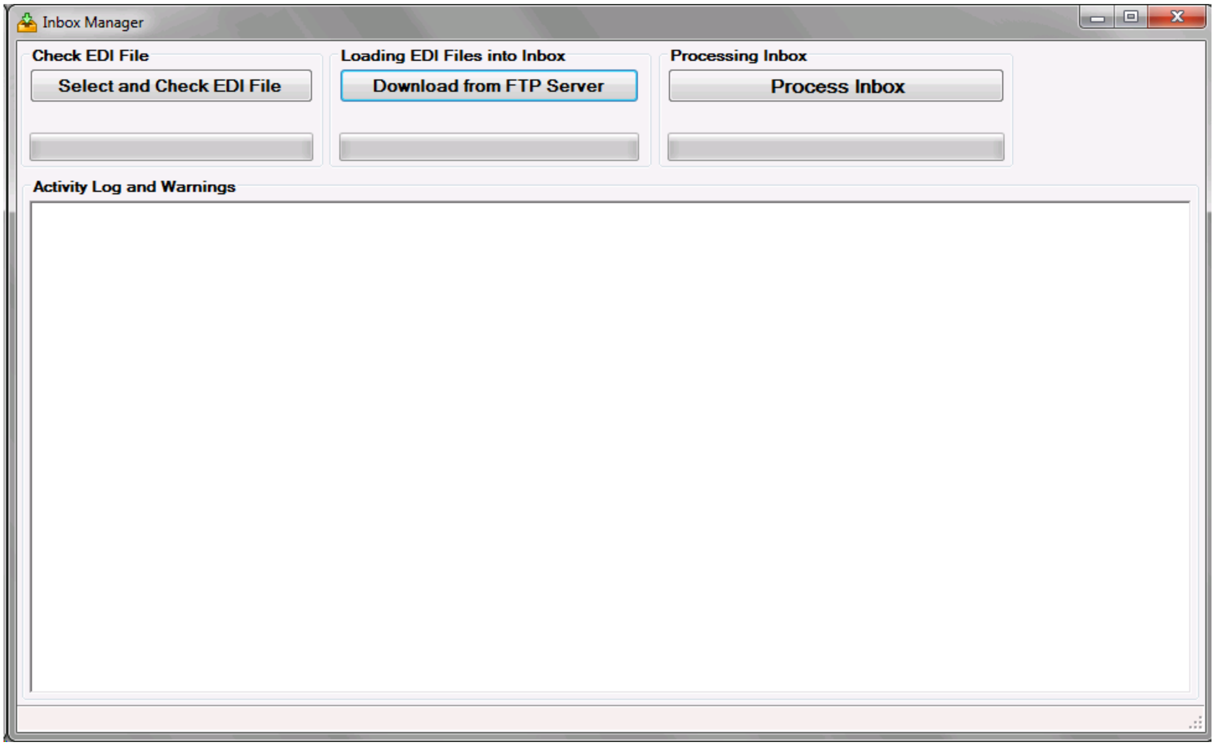
Using the Inbox Manager you can access the most important functions of EDI Exchange. Inbox Manager allows you to download EDI files into the "Inbox" folder and process these files. This screen handles the post-processing of the EDI files, their compliance check and auto-processing options.

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.

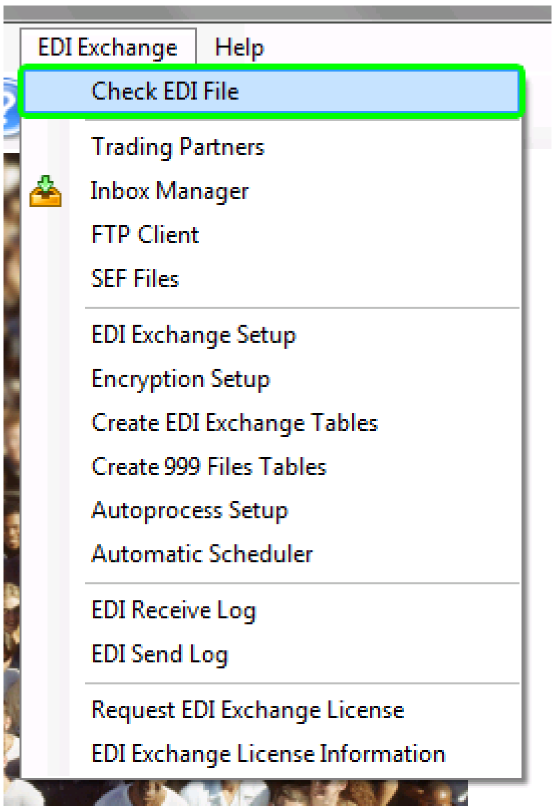
Unfortunately, HIPAA compliance is difficult and the truth is that many HIPAA EDI files are truly bad. Syntax errors, omitted loops, missing elements, wrongly formatted elements — these are the most common EDI errors. Without a true analysis, it is difficult to say what data ends up in your system.

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.

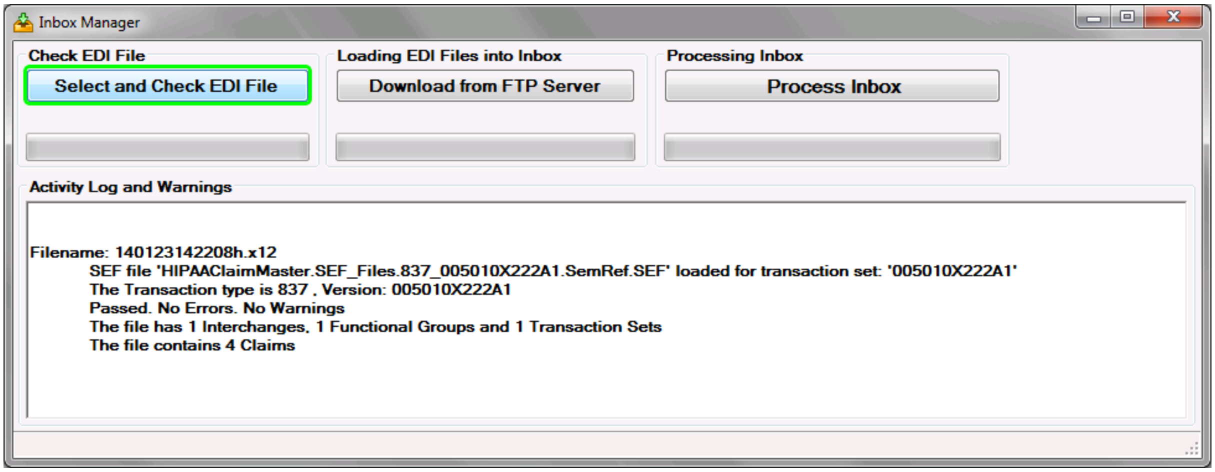
Follow the instructions below to check EDI files for compliance.

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



The "Check EDI File" menu item

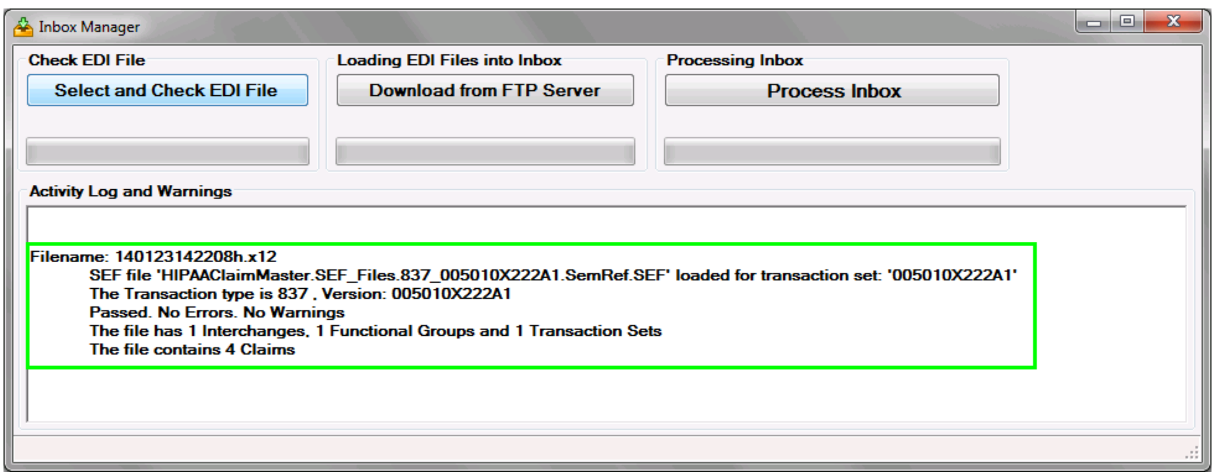
Alternatively, you can click on the "Select and Check EDI File" button in the Inbox Manager window. Read more in Accessing Inbox Manager.



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.



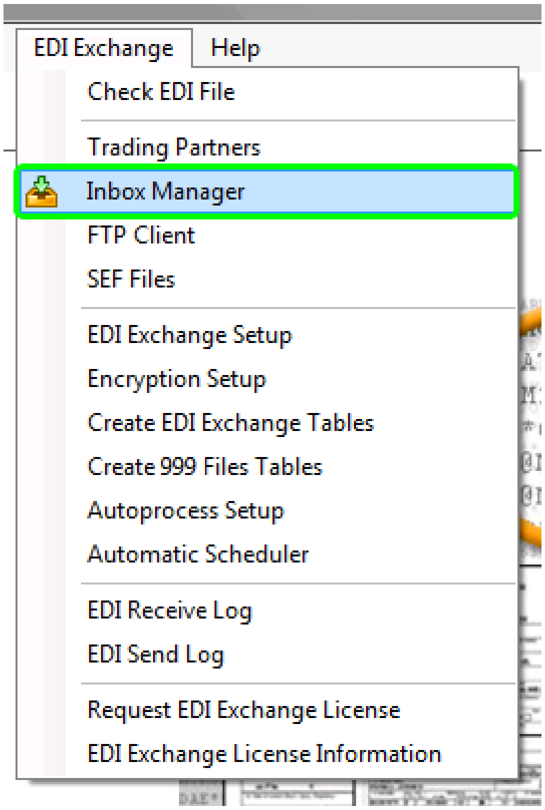
The "Activity Log and Warnings" area displaying log messages

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).

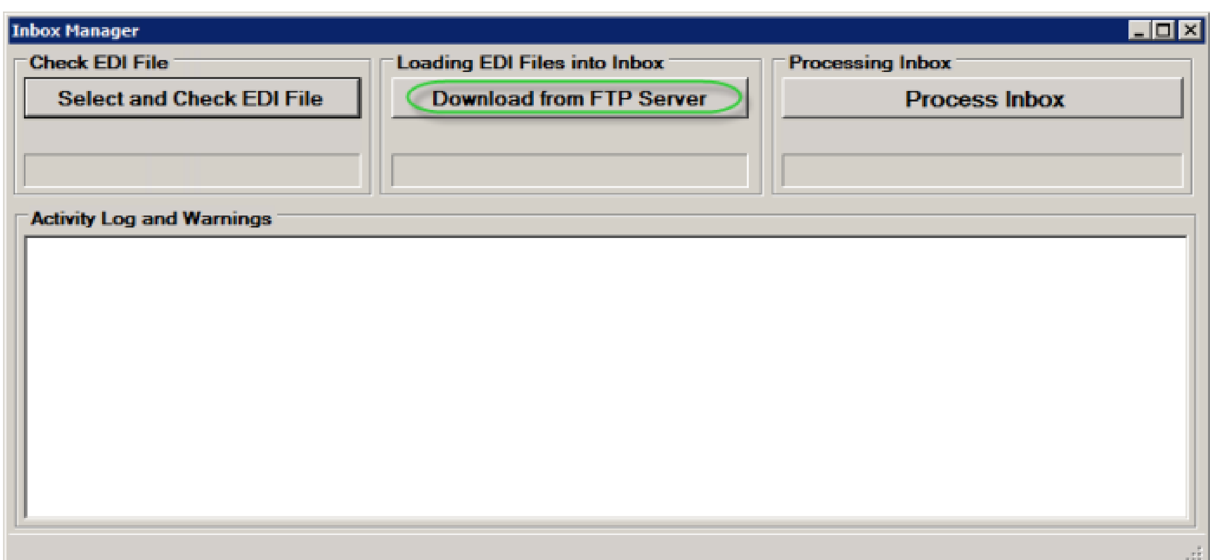
Follow the instructions below to upload EDI files into the "Inbox" folder.

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



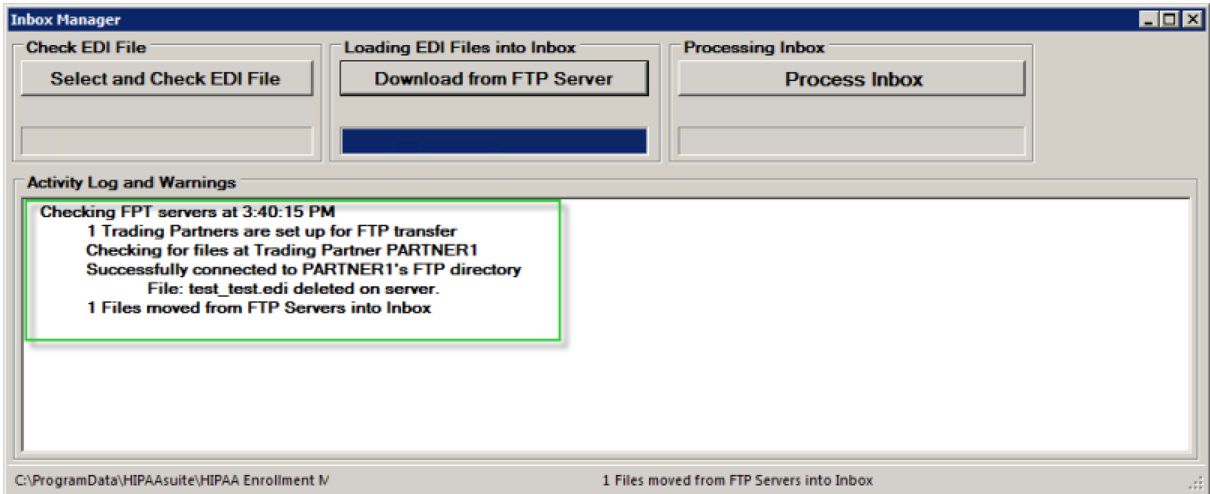
The "Inbox Manager" menu item

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.



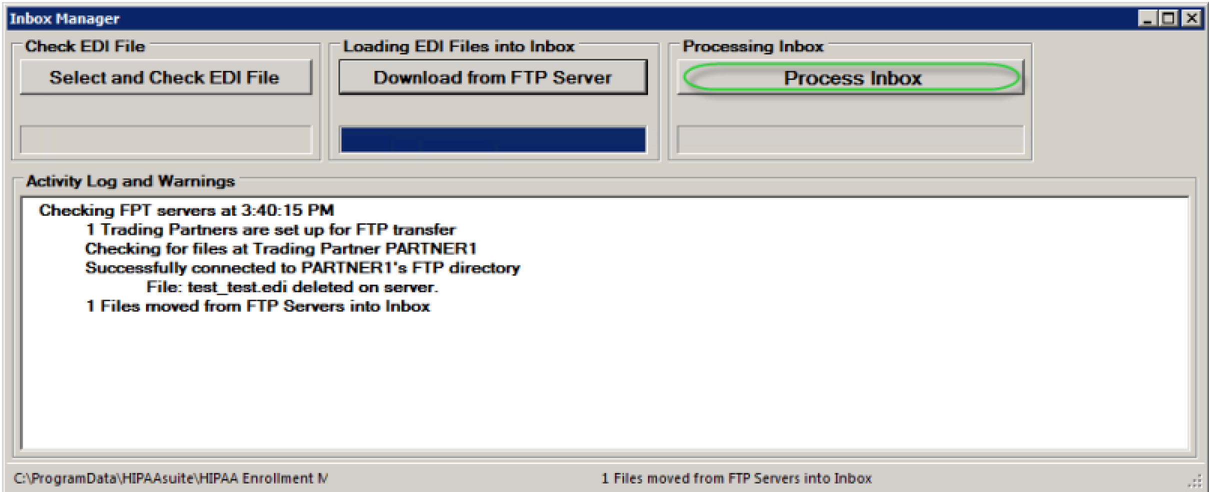
Activity Log and Warnings information

7.6.4 Processing EDI Files

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

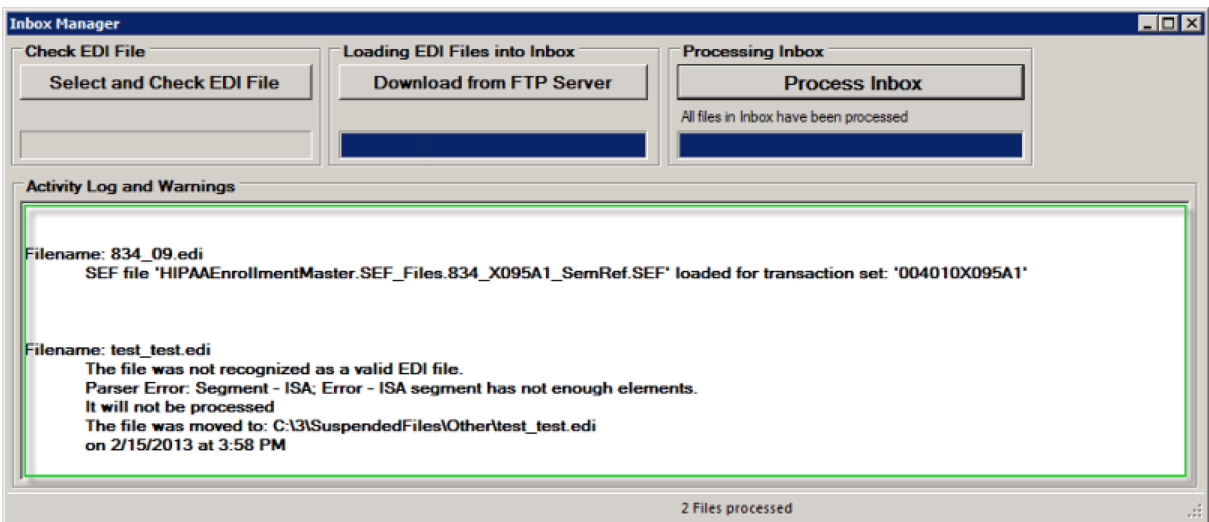
> Note: Once you have saved the auto-processing options (see Defining Auto-Processing Options), the files will not only be analyzed but also processed according to the defined settings. The auto processing enables you to combine and run multiple fulfillment steps together (for example, export, saving,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

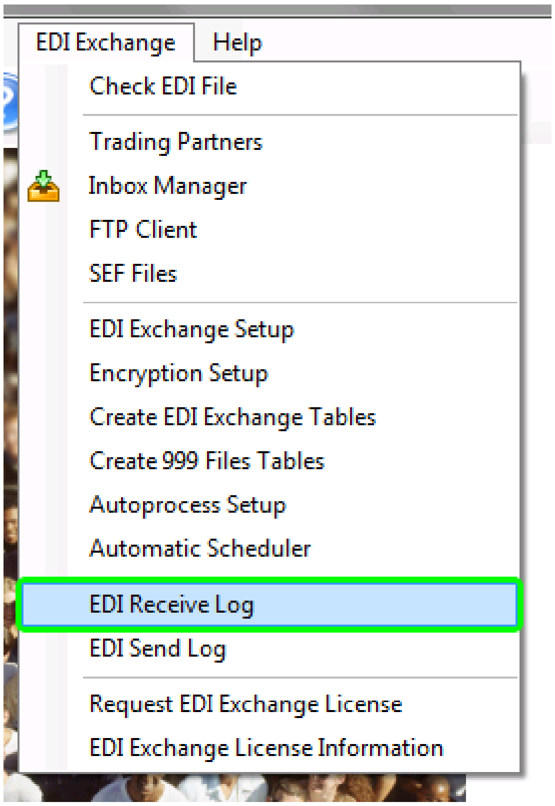


Activity Log and Warnings information

7.6.5 Accessing EDI Receive Log

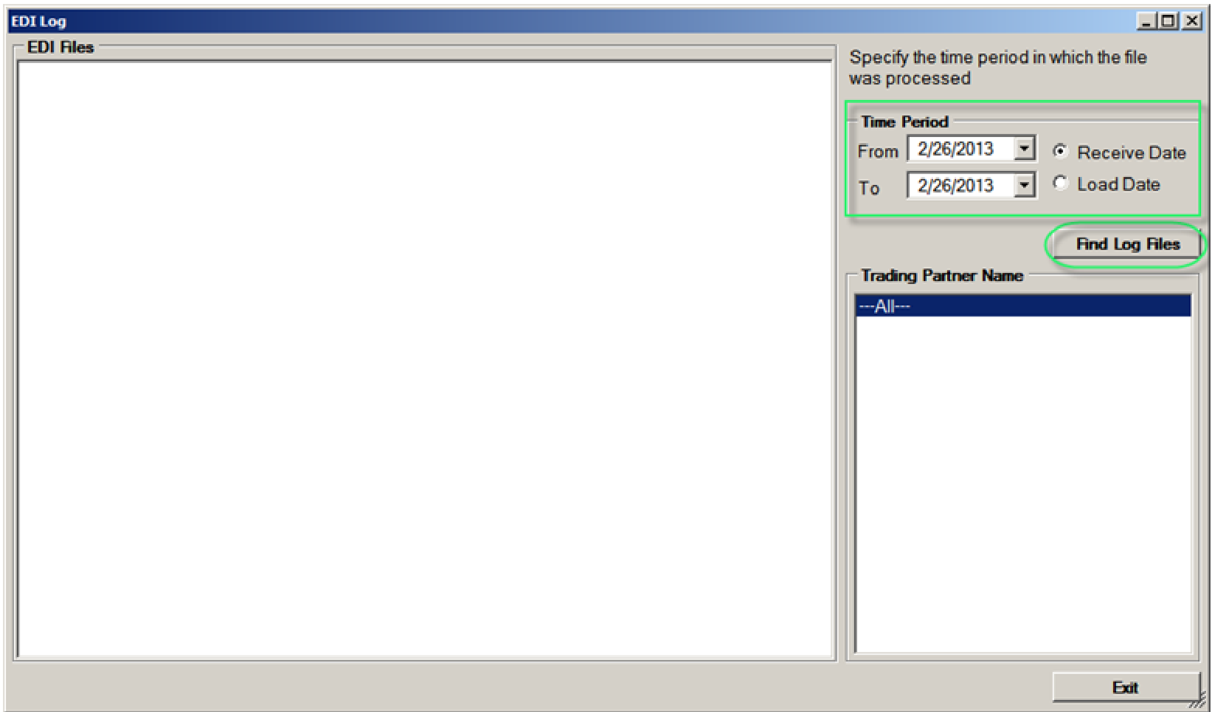
EDI Exchange has a file log. Each processed file creates an entry in the `Trans_Log` table. You can access the "EDI Log" window to query this table and see what files came in and how they were processed. You can access the EDI Receive Log once the application has been initialized. Follow the instructions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

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



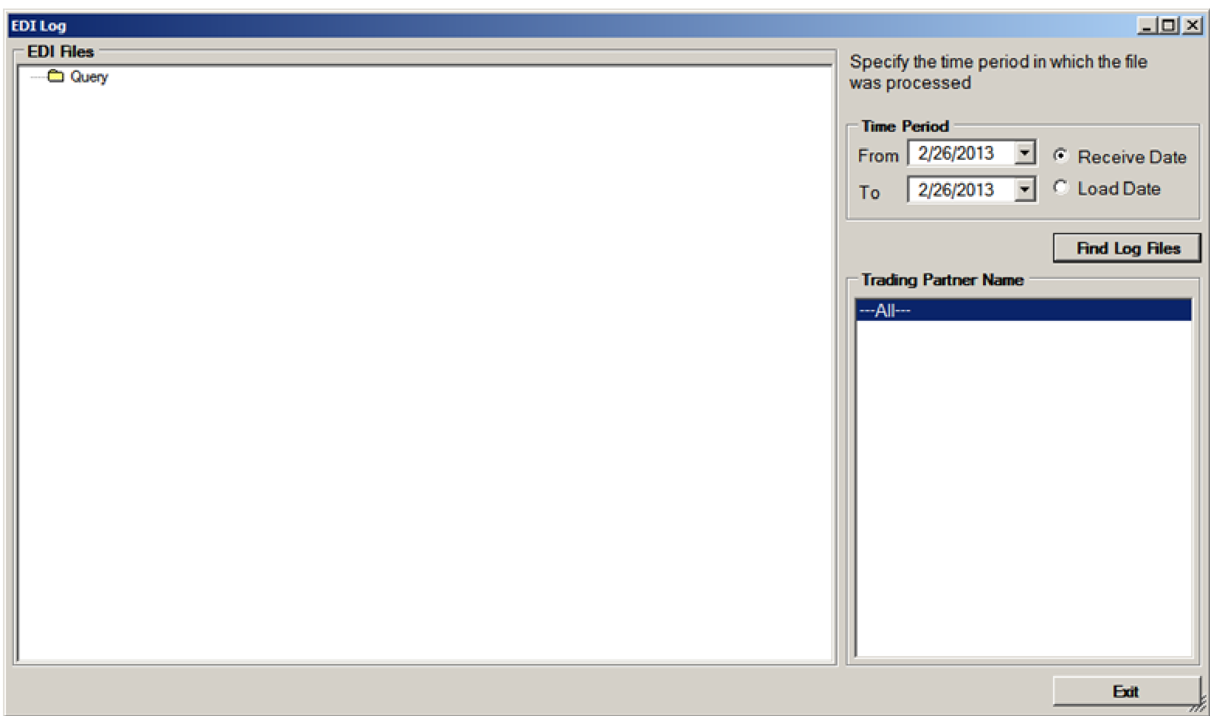
The menu for the EDI Receive Log

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.



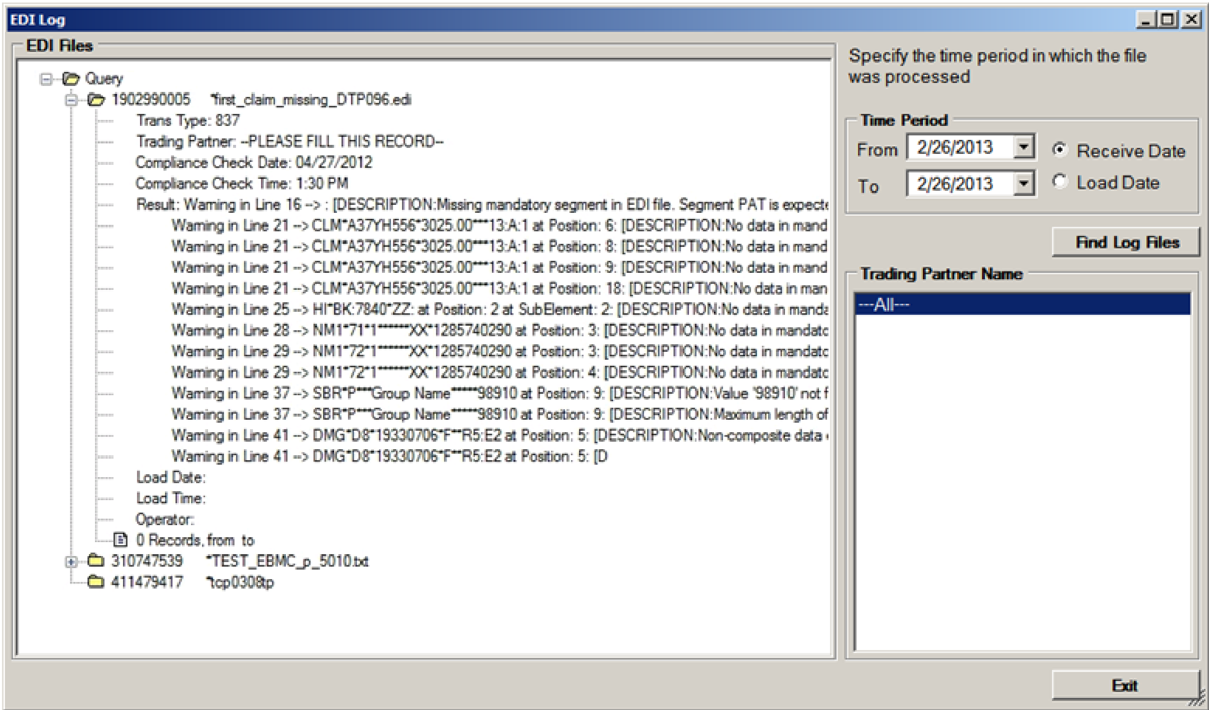
Specifying the time period

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.



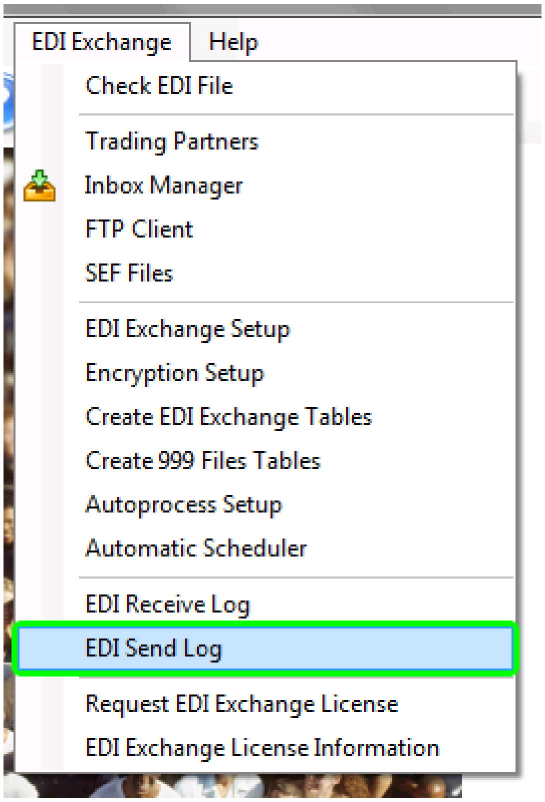
Details of the EDI Receive Log

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

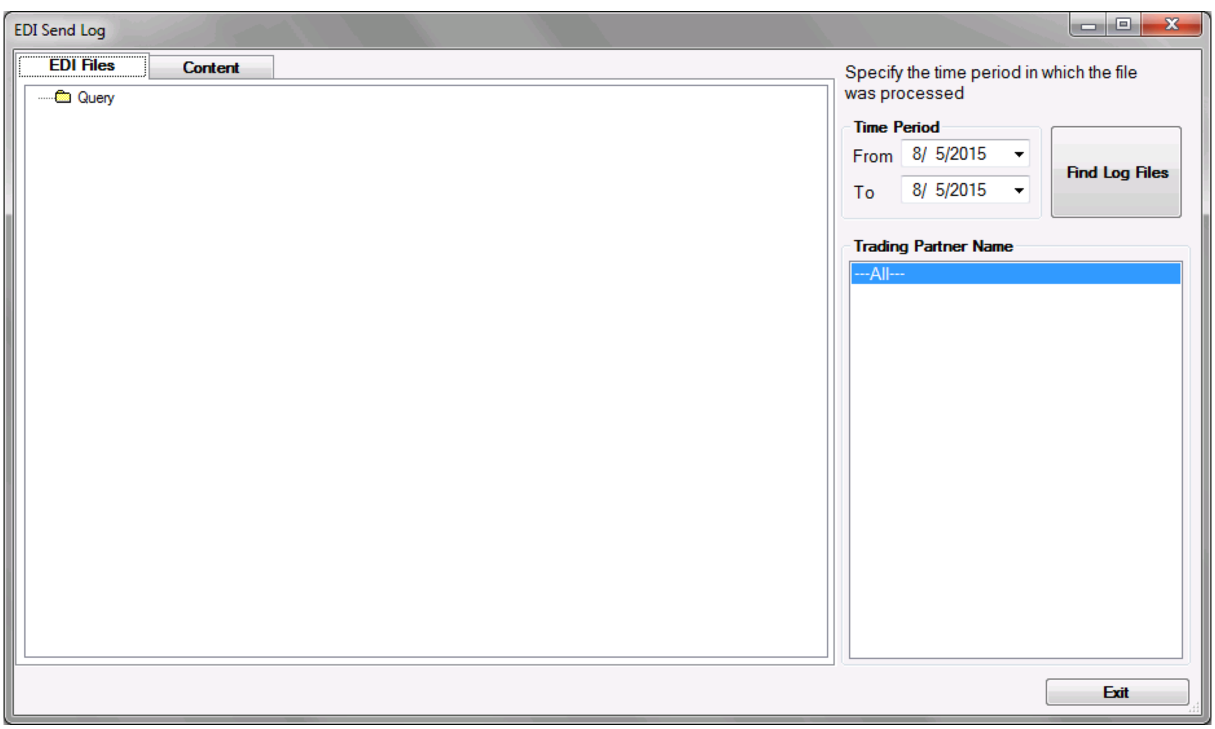
This page contains instructions on how to access the "EDI Send Log" window. It becomes available once EDI Exchange has been initialized.

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**

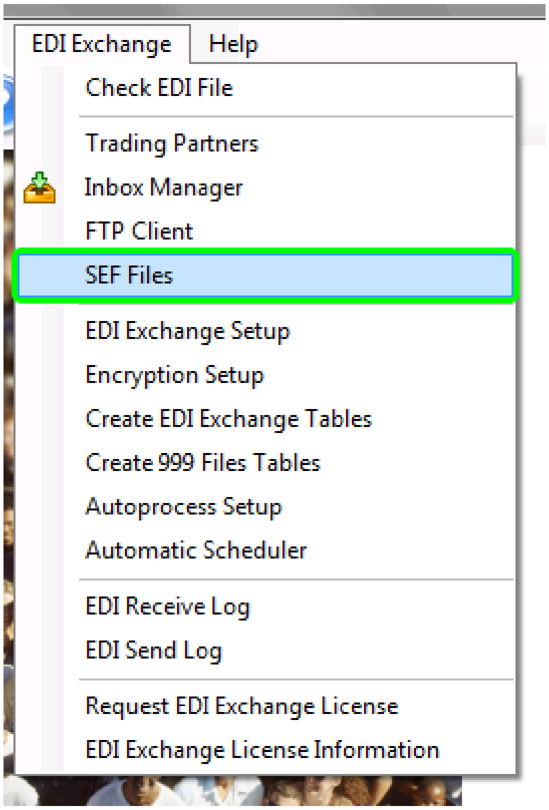
   - **Trading Partner Name** — Select a trading partner in the list. If you select "---All---", all trading partners will be included.

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

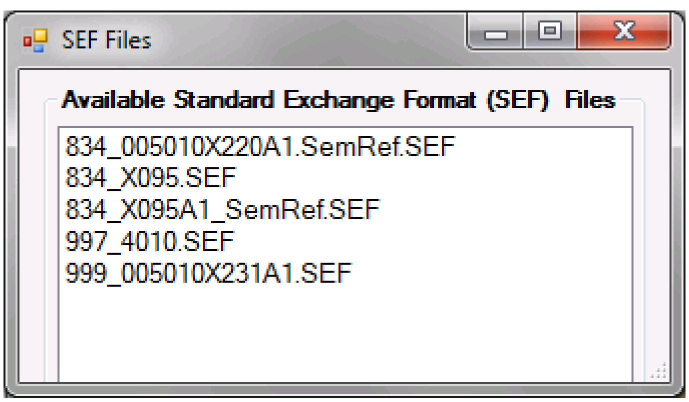
SEF (Standards Exchange Format) files are repositories of standards information that define the format of EDI documents. SEF files are the basis for the compliance check engine that EDI Exchange uses. These files contain all rules of the implementation guide of a transaction. There is a SEF file for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

8.1 Concepts

The **HIPAA RealTime Client** is a communications client designed to interact with SOAP and MIME services. This makes **HIPAA Eligibility Checker** able to request and receive EDI files, in turn enabling providers of health care services to check whether a patient is covered by a health insurance policy electronically. The client will package and send EDI 276 files and receive the 277 claim status transaction files using secure http as a transport medium. The **RealTime Client** is also capable of sending unencrypted test-only messages for use in a testing environment, however in a production environment they will be sent via https. This means every service needs an SSL Certificate signed by a recognized certificate authority and every EDI message sent through https will be sent encrypted and can only be decrypted by its intended recipient.

With the Affordable Care Act's (ACA or Obamacare) adoption of the EDI connectivity rules developed by the Coalition for Affordable Quality Healthcare (CAQH), a consortium of healthcare industry providers and insurers, the need. They devised and prescribed mechanisms to transfer claim status information in real-time between two computers.These new CORE standards will greatly enhance the efficiency of establishing insurance coverage for a patient, reducing the wait time to under a minute. CAQH's CORE standards for administrative data exchange are rolled out in segments referred to as Phases. The HIPAA RealTime Client is CORE Phase II-certified, meeting all connectivity and data content rules specified therein.

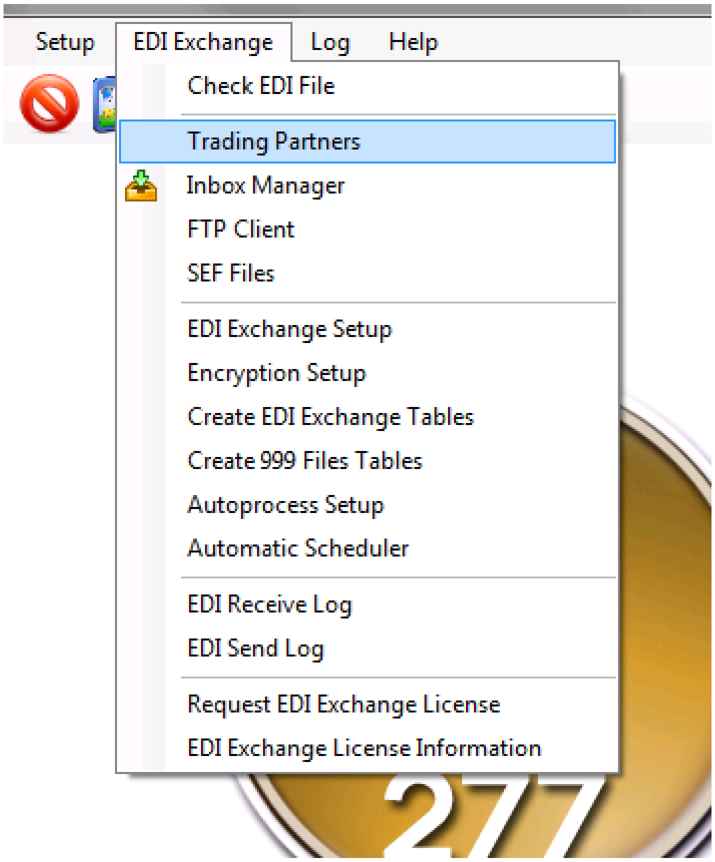
The HIPAA ClaimStatus Checker's RealTime Client requires EDI Exchange. It will allow you to send EDI 270 requests securely to the trading partner of your choice and process the resulting EDI 271 file. Although named RealTime, the client does support batch mode EDI transfers for large or bundled Claim Status requests.

8.2 Trading Partner Setup

The HIPAAsuite RealTime Client can be used to consume a CORE-compliant service hosted by a Trading Partner. In HIPAAsuite ClaimStatus Checker, this means you can verify a patient's medial coverage in real time; RealTime Client also supports batch mode transfers for larger or multiple Claim Status requests packaged in a single EDI file. In order to consume a client's CORE-compliant SOAP or MIME service, the following steps must be taken:

1. You will need your Trading Partner's service's URL address. Some Trading Partners may have separate addresses for SOAP and MIME services (both being specified in the CORE Connectivity Rules), Real Time and Batch services, or Batch request submissions and Batch request pickup.

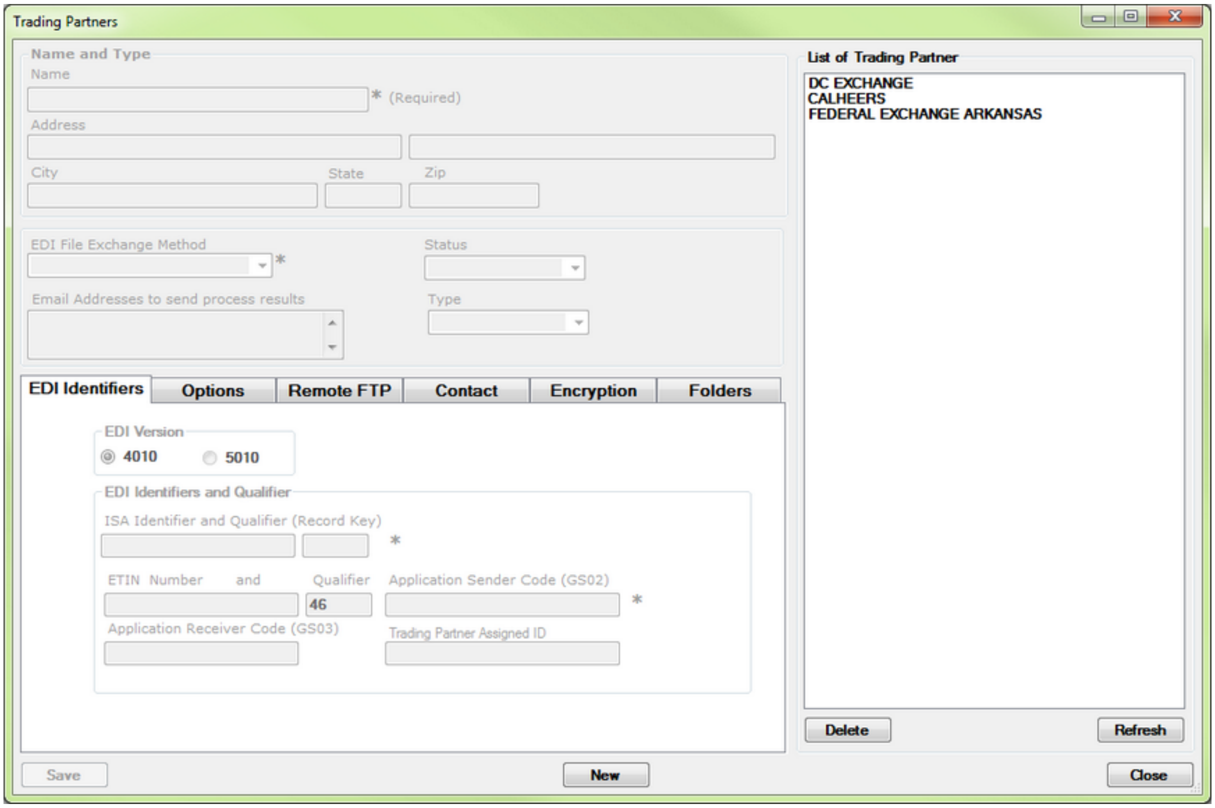
2. Head to your trading partner's configuration settings under the "EDI Exchange" menu:



"Trading Partners" option under "EDI Exchange" menu

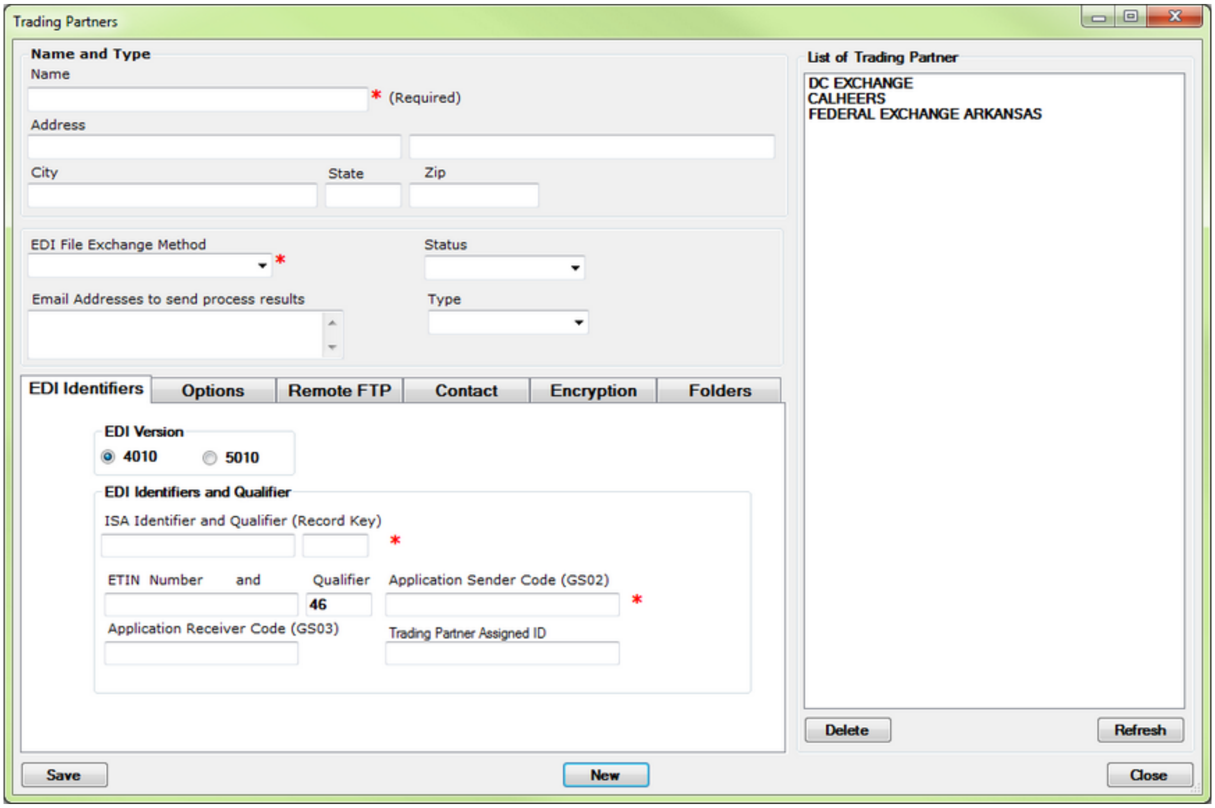
The "Trading Partners" menu item.

3. The "Trading Partners" configuration window will appear. If the Trading Partner for whom you are configuring the RealTime Client is already listed, double click on the Trading Partner and skip to step #5. Otherwise, click the "New" button and continue onto step #4.



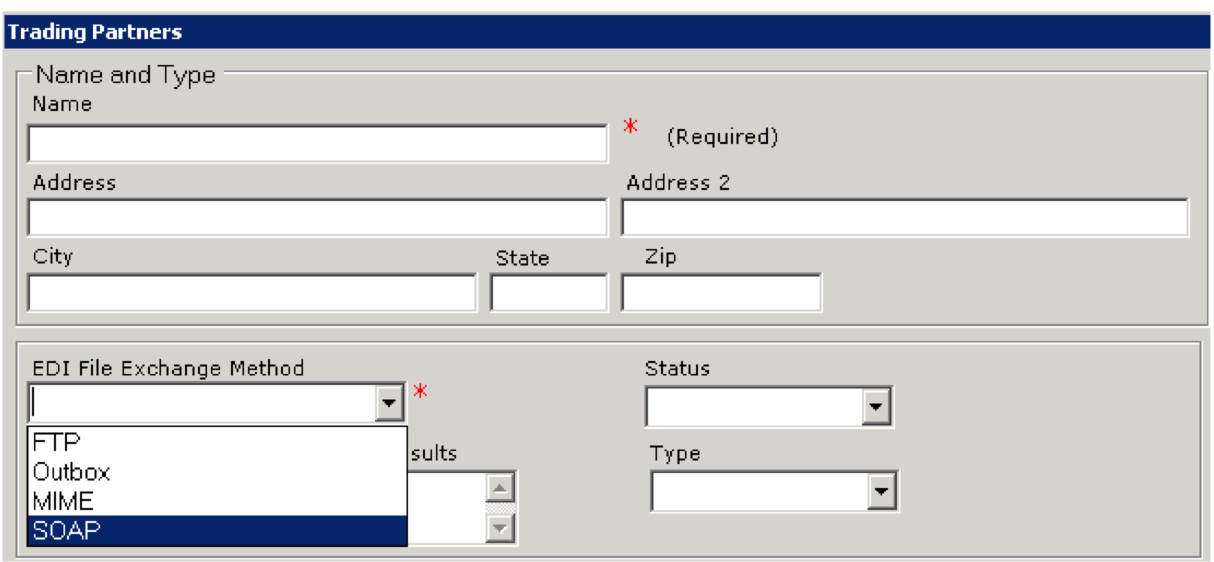
Trading Partner configuration window populated with some Trading Partners.

4. The left side of the Trading Partner configuration window will become available to you for editing. Fill in at least the Trading Partner's name, ISA identifier and qualifier, the Trading Partner's application code, and finally, under the "Folders" tab, the outbox and repository folders to be used for this Trading Partner. The "Create... " button underneath these last two fields will automatically fill in the text for you using the Trading Partner's name.



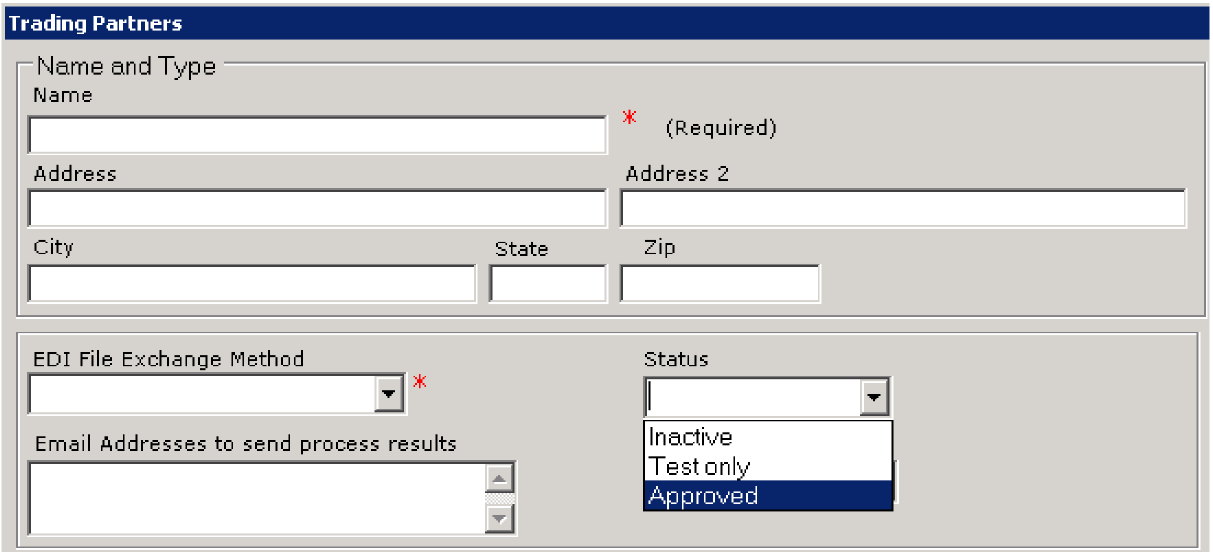
A blank Trading Partner.

5. The fields specific to the RealTime Client are the "EDI File Exchange Method" dropdown selection in the main configuration window and the "CORE" tab on the bottom of the same window. You can select either CORE or MIME from the "EDI File Exchange Method" to send messages to your trading partner using the RealTime Client.



Selecting MIME or SOAP will use the RealTime Client to send EDI requests to this trading partner.

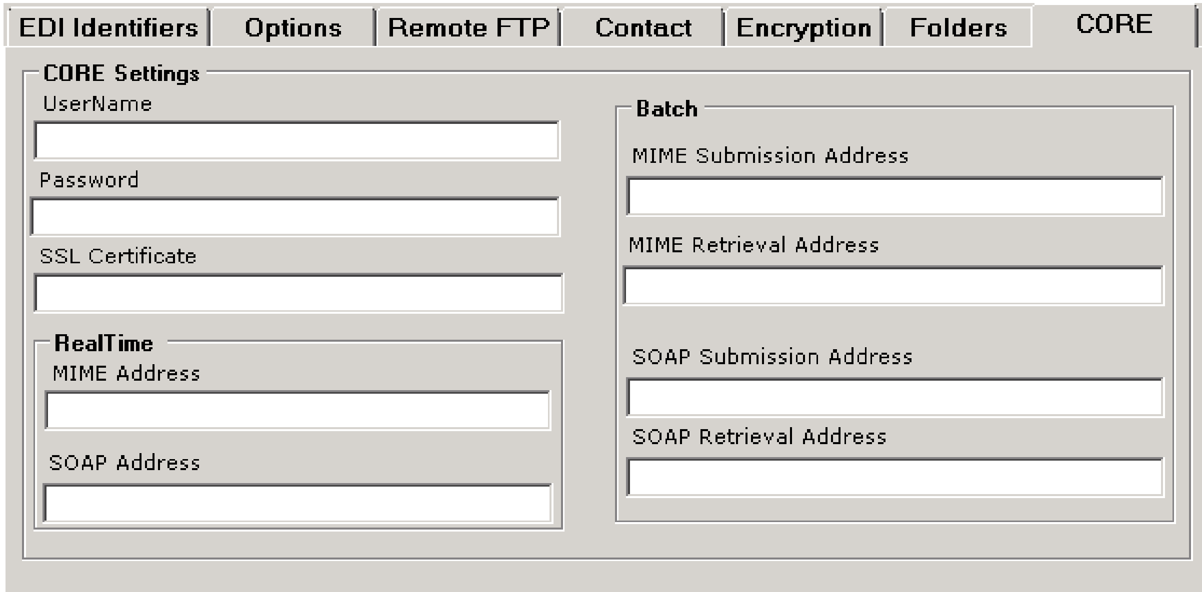
6. To flag the trading partner as OK for EDI transfers, the Status field must be set to Active or Test Only. "Test Only" is only for testing and will enable you to use unsecure http:// addresses to contact your Trading Partner. The "Approved" option flags enables secure transfers to this trading partner.



"Approved" will let ClaimStatus Checker know this is a trusted Trading Partner.

7. Lastly, the "CORE" settings tab. Settings dealing with addressing and user credentials are stored here. Type in the addresses for this Trading Partner's SOAP or MIME servers. Some Trading Partners listen on different addresses for RealTime and Batch transfers, and some even have distinct addresses for Batch Mode request submissions and Batch Mode results retrieval. Spaces for all of these are provided. If this Trading Partner doesn't have a different service address for Batch Mode result retrieval, the address is the same as for Batch Mode request submission; likewise if this Trading Partner does not have a different address to distinguish RealTime from Batch mode, they are the same address.

Currently only username tokens are supported. Fill in the username and password textboxes with the credentials your Trading Partner has provided you for use of their CORE-compliant service. These will identify you to this Trading Partner when requesting a patient's Claim Status information.



User credentials and CORE-compliant service addresses. Both are required for successful communication.

8.3 Sending Requests and Receiving Responses

View

Sending 276 Requests

Receiving 276 Responses

Back Cover