Iowa Immunization Registry Information System (IRIS)

PHINMS 2.8.00 Data Exchange Setup

Version 1.0

Last Updated: February 12, 2013

Table of Contents

Preparation for PHINMS 2.8 Installation

SSL Certificate Creation

The Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of a message transmission on the Internet. SSL client and server certificates are used as an added security feature for transmitting data for IRIS PHINMS transactions. IRIS requires both the client and server install certificates generated by the Hewlett Packard Enterprise Services (HP) Immunization Services personnel. To accomplish this, first create a private key for each machine that will be accessing the IRIS PHINMS machine. This private key is then used to create a Certificate Signing Request (CSR) which will be sent to HP. HP will create the SSL certificate for installation on the client machine ("client" in this instance will most likely be the server that communicates with the IRIS Web services servers).

Generating a Key and Certificate Signing Request (CSR)

To generate a CSR, a key pair must be created for the server. These two items are a digital certificate key pair and cannot be separated. If the public/private key file is lost or changed before the SSL certificate is installed, the SSL certificate will need to be re-issued. The private key, CSR, and certificate must all match in order for the installation to be successful. The following sequence of commands will generate a 2048 bit key using the OpenSSL software. Below are instructions for creating the CSR in a Windows environment. It is recommended to use the domain name or IP address that will be used for the certificate as the prefix of the filenames. Also make sure that any existing keys and CSRs are NOT overwritten.

Generating a Private Key and CSR using OpenSSL

Step 1: Generate Private Key

Type the following command at the prompt:

```
openssl genrsa –out my.server.com.key 2048
```

This command generates a 2048 bit RSA private key and stores it in the file, ***my.server.com***.key

Note: For all SSL certificates, the CSR key bit length must be 2048. The text in italic bold (i.e., my.server.com) is only an example. Replace it with a name that is meaningful to you. It does not have to be a website but MUST have the ".key" extension.

Step 2: Generate the CSR

Type the following command at the prompt:

```
Openssl.exe req –new –key my.server.com.key –out my.server.com.csr
```

This command will prompt for the following attributes of the certificate:

Field	**Required / Optional**	**Description**
Country Name	R	Use the two-letter code without punctuation for country. Example: US or CA
State or Province	R	Spell out the state completely; do not abbreviate the state or province name. Example: Iowa
Locality or City	R	The Locality field is the city or town name; do not abbreviate. Example: Mount Pleasant , not Mt. Pleasant

Company	R	If the company or department has an &, @, or any other symbol using the shift key in its name, the symbol must be spelled out or omitted. Example: XY & Z Corporation would be XYZ Corporation or XY and Z Corporation.
Organizational Unit	O	Can be used to help identify certificates registered to an organization. The Organizational Unit (OU) field is the name of the department or organization unit making the request. To skip the OU field, press Enter on the keyboard.
Common Name	R	The Common Name is the Host + Domain Name. It looks like "my.server.com".
Email Address	NA	Do **not** enter anything in this field.
Challenge Password	NA	Do **not** enter anything in this field.
Optional Company Name	NA	Do **not** enter anything in this field.

The certificate is used to secure the transaction between provider EHR and IRIS. Each certificate is required to have a unique common name. Combining your host and domain names will ensure your common name is unique.

A public/private key pair has now been created.

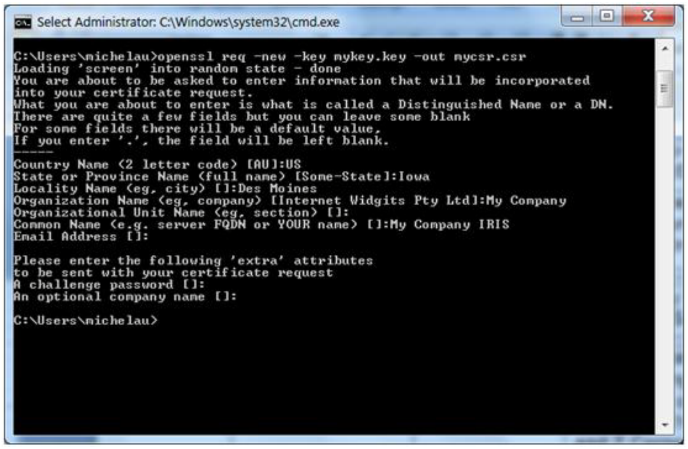
Private Key:

- File Name example: my.server.com.key
- Stored locally on the server machine
- Used for decryption (IMPORTANT – Maintain in a safe place).

Public Key

- File Name example: my.server.com.csr
- In the form of a Certificate Signing Request (CSR)
- Used for certificate enrollment

Screenshot of the screen showing the attributes of the certificate:



```
C:\Users\michelau>openssl req -new -key mykey.key -out mycsr.csr
Loading 'screen' into random state - done
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:Iowa
Locality Name (eg, city) []:Des Moines
Organization Name (eg, company) [Internet Widgits Pty Ltd]:My Company
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:My Company IRIS
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

C:\Users\michelau>
```

Step 3: Send CSR and request for Username and Password to HP and the Iowa Department of Public Health

The CSR is an ASCII text file that can be attached to an email and should be sent to David Thrall at david.thrall@hp.com and copy Kim Tichy at Kimberly.Tichy@idph.iowa.gov.

Step 4: Backup the private key

It is recommended to back-up the *.key* file. An acceptable option is to create a copy of this file onto a flash drive or other removable media. While backing up the private key is not required, having one will be helpful in the instance of server failure.

Step 5: Receiving Your Signed Certificate

Once HP is done processing your CSR, you will receive the signed certificates as an email attachment. These files must be installed in the Trusted Store of the computer for which it was generated. They must be unzipped and placed in the same folder as your request. The files are:

1. The CA certificate, ca.crt. This is common to all Immunization Information System (IIS) users and establishes HP's server as a valid Certificate Authority, which tells your server to trust Certificates issued by HP.
2. The specific server certificate, such as csr-site-request.crt. This is unique to the server it was generated from.

The instructions for this will vary depending on your environment. Two common trusted stores are Public-Key Cryptography Standards #12 (PKCS#12 or PFX) and Java Key Store (JKS). A good source of reference for this information is Google (search for: importing trusted root certificates).

Join your private key with the signed certificate and certificate authority files e-mailed by HP, so the browser and OS can use it.

Here is an example of creating a .pfx file using openssl.

```
Openssl pkcs12 –export –out www.example.com.pfx –inkey www.example.com.key –
in www.example.com.crt –certfile cacert.crt
```

Here are what the example file names represent:

www.example.com.pfx = this will be the output file – which you'll install into Windows 7 so IE can use it

www.example.com.key = this is the key that was generated by step 1

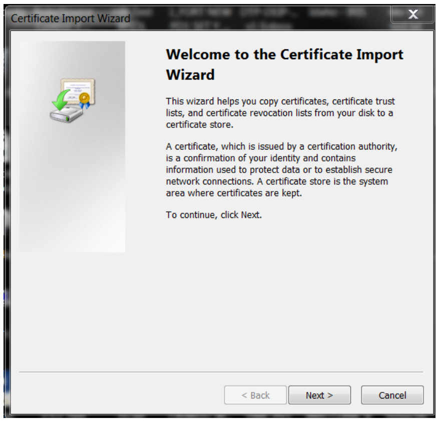
www.example.com.crt = this is the signed certificate provided in response to the CSR

cacert.crt = this is the CA (Certificate Authority) file which was provided. This is needed by openssl to verify the first file was signed.

Refer to the following steps if you are using a .pfx file. Otherwise, skip this section.

1. Go the file where the "www.example.com.pfx" file has been created.
2. Right click on the file.
3. Select Install PFX.

4. Click on Next.



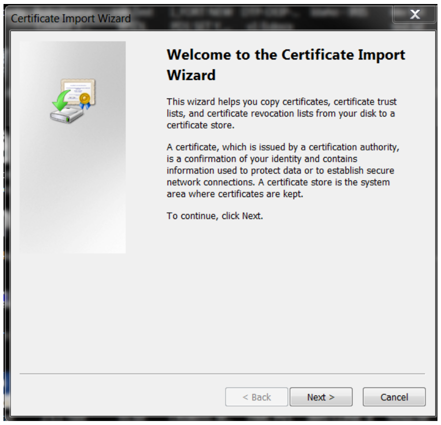
Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

5. Click on Next.



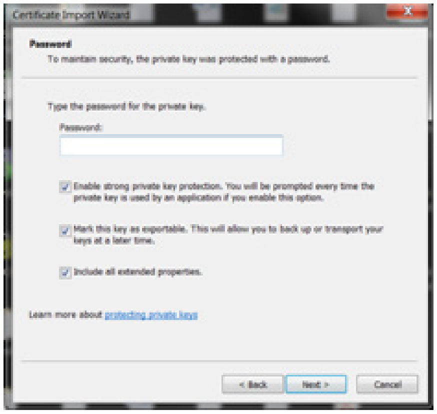
Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

6. No password is required. Ensure that all three check boxes are selected. Click on Next.



Password

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

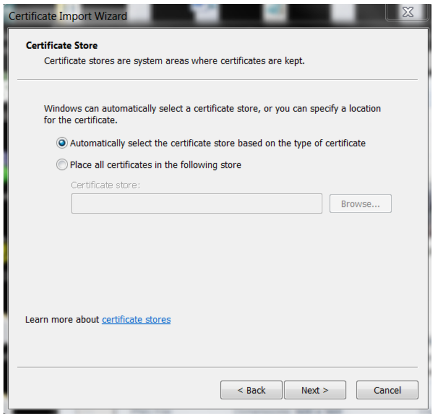
☑ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

☑ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

☑ Include all extended properties.

Learn more about protecting private keys

8. Click on Next.



Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

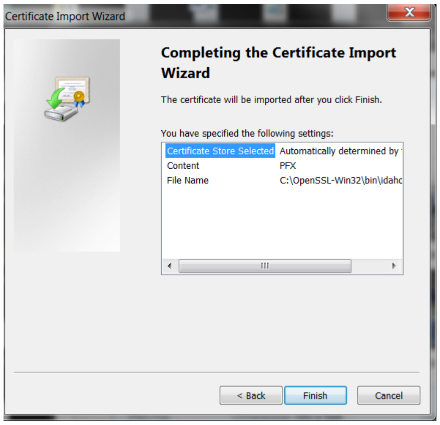
● Automatically select the certificate store based on the type of certificate

○ Place all certificates in the following store

Certificate store:

Learn more about certificate stores

9. Click on Finish.



Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected	Automatically determined by
Content	PFX
File Name	C:\OpenSSL-Win32\bin\idahc

Generating a Private Key and CSR using Microsoft Windows

Step 1: Creating the Private Key and CSR

1. Open the **Microsoft Management Console** (MMC). On the Start menu, click Run, type MMC, and then click OK. MMC opens with an empty console.
2. Right-click the default Web site, click **New**, and then click **Site**. Create a new site and give it a temporary name.
3. Right-click the new site, click **Properties**, click the **Directory Security** tab, and then click **Server certificate**.
4. Select **Create new certificate** and follow the wizard to create a new CSR. Use the information from the OpenSSL instructions above in Step 2, when filling out the request. When prompted, select **Prepare the request now but send it later**.
5. Use the CSR that you just created to request a new certificate from HP.
6. See the OpenSSL instructions Steps 3, 4, and 5, above, to finish the process.

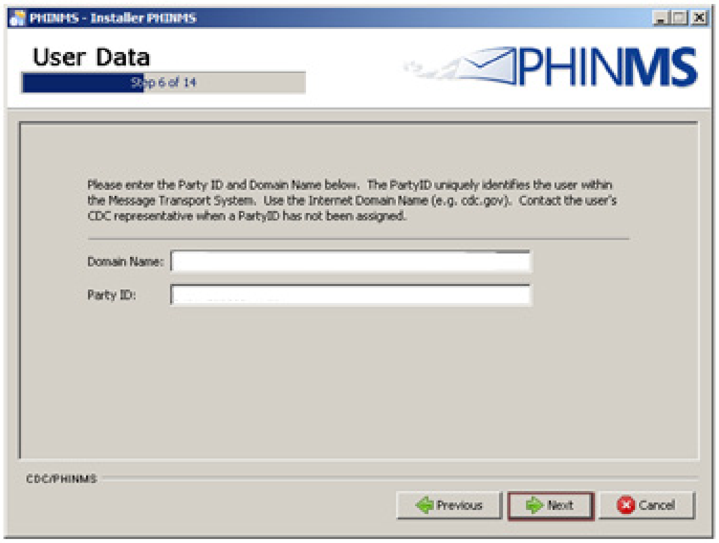
Installing PHINMS

Before installing PHINMS client, verify you have received the following from HP:

1. Your organization's specific Party ID
2. Your organization's CPA file
3. SSL Certificate

Once you have the necessary information, you may install the PHINMS console.

During the installation process, you will be required to enter a Domain name and Party ID.



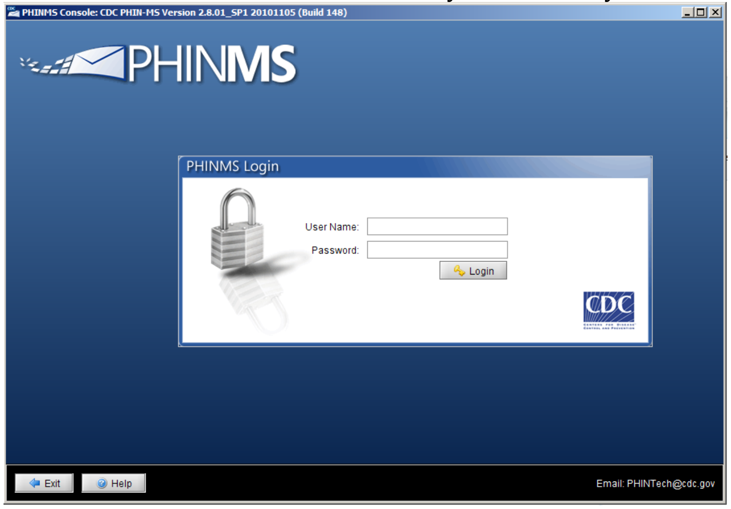
Please enter the Party ID and Domain Name below. The PartyID uniquely identifies the user within the Message Transport System. Use the Internet Domain Name (e.g. cdc.gov). Contact the user's CDC representative when a PartyID has not been assigned.

Domain Name:

Party ID:

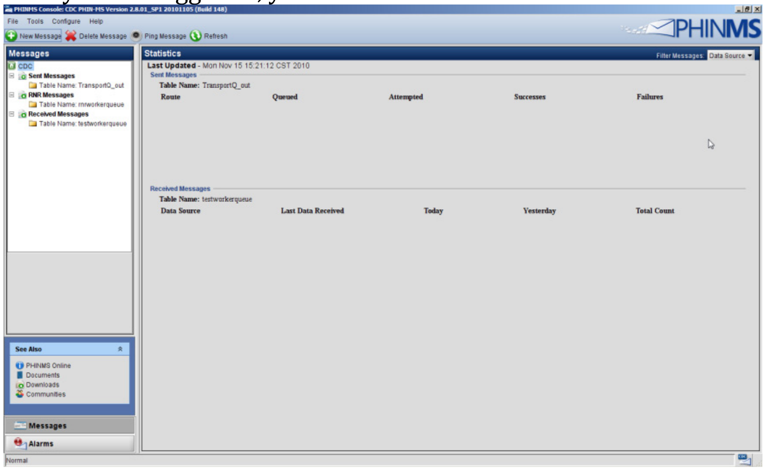
Please enter the following information:
Domain Name: https://64.73.41.133/IRISUATJ/portalInfoManager.do
Party ID: The unique Party ID assigned by HP

Once the PHINMS console is successfully installed on your client, log in using the following credentials:



Username: system
Password: Phinms123

Once you are logged in, you will see the main console screen:



PHINMS Console: CDC PHIN-MS Version 2.8.01_SP1 20101105 (Build 148)

Last Updated - Mon Nov 15 15:21:12 CST 2010

Sent Messages

Table Name: TransportQ_out

Route	Queued	Attempted	Successes	Failures

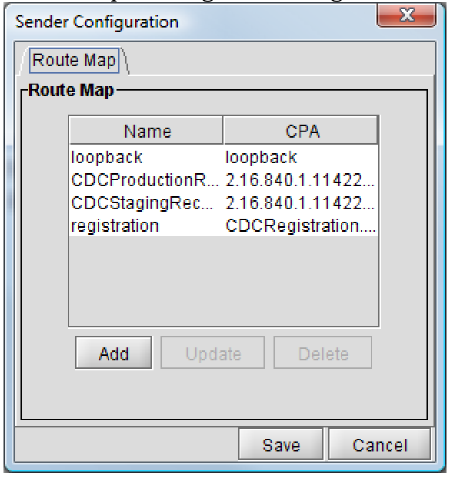
Received Messages

Table Name: testworkerqueue

Data Source	Last Data Received	Today	Yesterday	Total Count

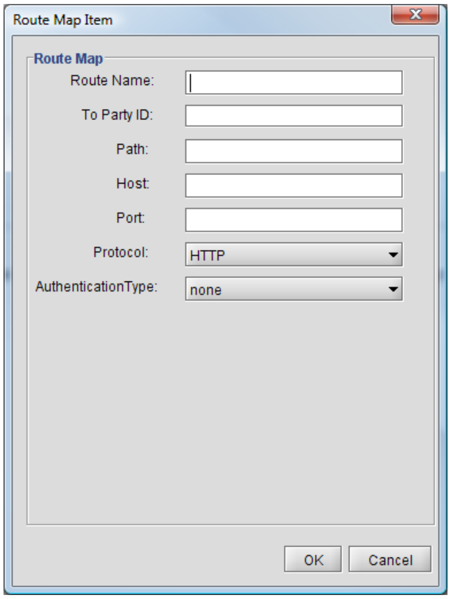
Setting up the Route Map

1. From here, you will begin setting up the correct configurations.
2. On the Top Menu go to: Configure -> Sender -> Route Map



Name	CPA
loopback	loopback
CDCProductionR...	2.16.840.1.11422...
CDCStagingRec...	2.16.840.1.11422...
registration	CDCRegistration....

3. Click the Add button.



Protocol: HTTP

AuthenticationType: none

4. Enter the following and click OK:

	IRIS UAT PHINMS Server
Route Name	IRIS_UAT
To Party ID	IRIS_UAT
Path	phinms-uat/receivefile
Host	64.73.41.133
Port	443
Protocol	**HTTPS**
Authentication Type	none

Note: Some of the values above will be different in production and will be provided when testing is completed.

5. Click Save in the Route Map screen.
6. On the Top Menu go to: Configure -> Restart PHINMS

Setting up Folder Based Polling

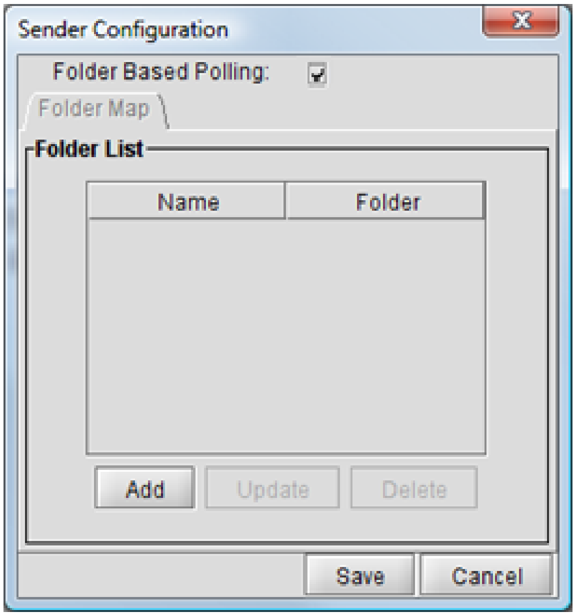
Paths to Folders: You will need to create three folders in a location where your PHINMS installation can be used:

i. Outgoing: Will be used to drop off the HL7 files that you want PHINMS to pick up and send. Recommend naming the folder in a way that identifies its functionality (i.e., IRIS environment to send the file to: "UAT")

ii. Processed: A second folder called "Processed" will be used by PHINMS to place the processed/sent files. Recommend creating this folder within the main folder.

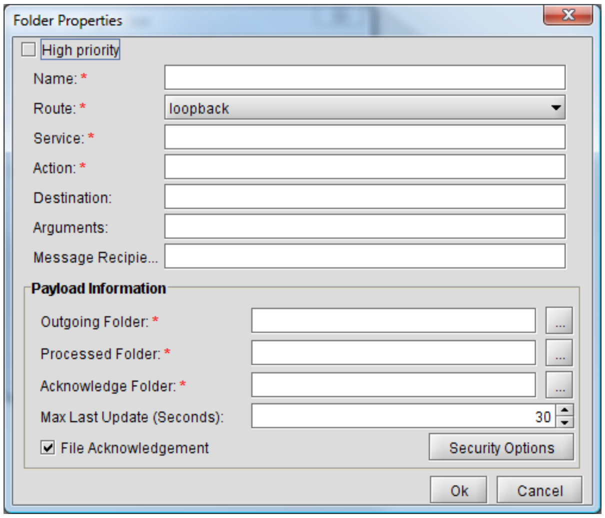
iii. Acknowledgement: A third folder called "Acknowledgement" will receive the Ack message from the PHINMS server describing whether the transmission was successful or not. Recommend creating this folder within the main folder.

1. On the Top Menu go to: Configure -> Sender -> Folder Pooling



Folder Based Polling: ☑

2. Check the Folder Based Pooling check box.
3. Click the Add button.



□ High priority

Route: * loopback

Max Last Update (Seconds): 30

☑ File Acknowledgement

Enter the following and click OK:

	IRIS UAT
Name:	IRISUAT
Route:	IRISPHINMS*
Service:	irisTransfer
Action:	realtime
Destination:	{leave blank}
Arguments:	{leave blank}
Message Recipient:	{leave blank}
Outgoing Folder:	Path to “Folder Pooling”**

Processed Folder:	Path to "Processed"**
Acknowledge Folder:	Path to "Acknowledgement"**
Max Last Update:	30
File Acknowledgement:	{leave checked}

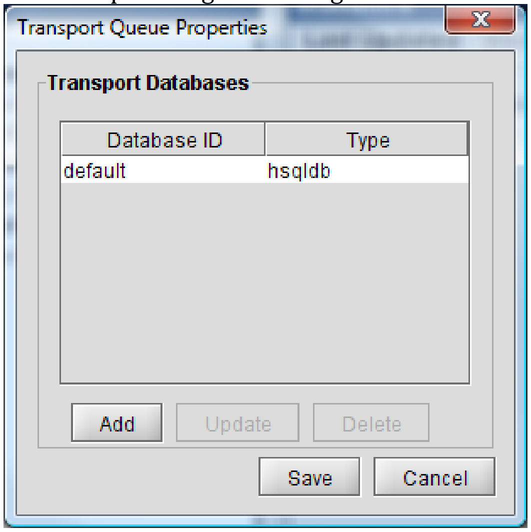
NOTE: * Name from Route Map created on 1.1
** As defined in "**A. Paths to Folders**" on this section.

4. Click Save in the Folder Based Pooling screen.
5. On the Top Menu go to: Configure -> Restart PHINMS

Setting up File Response

In order to receive the Response File from IRIS into the default location "senderincoming", located at: "PHINMS_Installation_Directory/shared/senderincoming":

1. On the Top Menu go to: Configure -> Sender -> Transport Queues

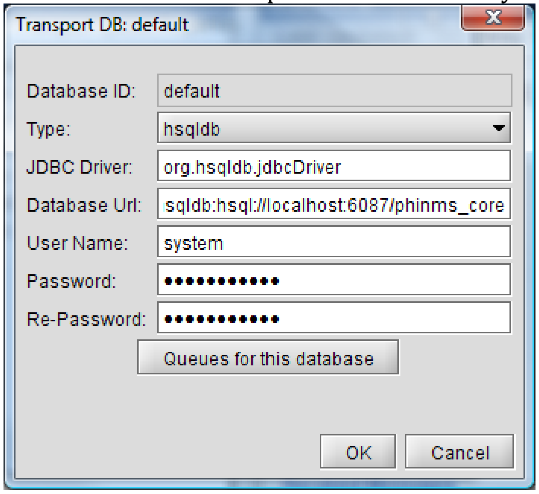


Transport Queue Properties

Transport Databases

Database ID	Type
default	hsqldb

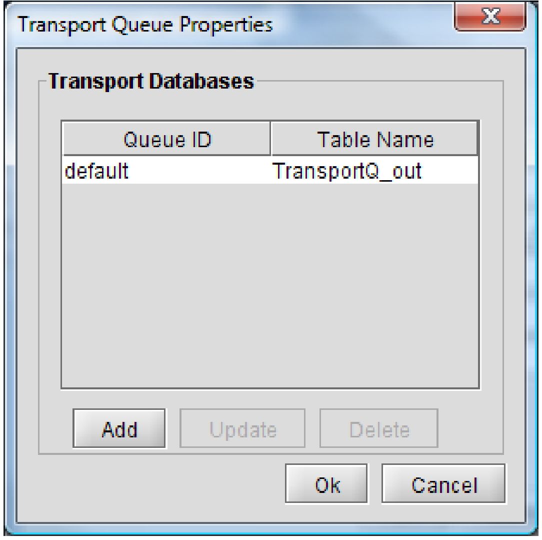
2. Select the default transport database already there and click Update:



Transport DB: default

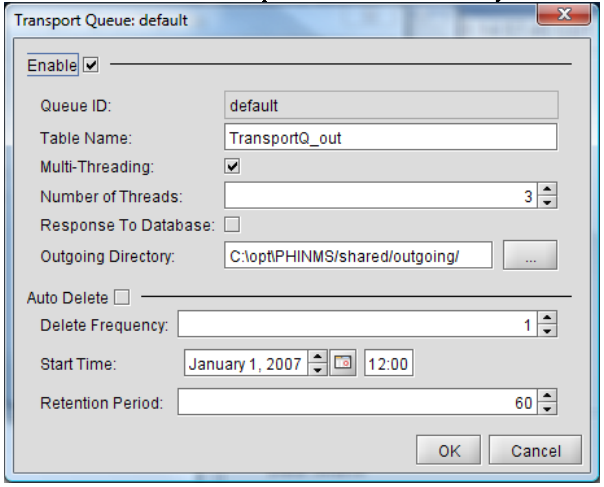
Database ID: default
Type: hsqldb
JDBC Driver: org.hsqldb.jdbcDriver
Database Url: sqldb:hsql://localhost:6087/phinms_core
User Name: system
Password: ●●●●●●●●●●●●
Re-Password: ●●●●●●●●●●●●

3. Click Queue for this database:



Queue ID	Table Name
default	TransportQ_out

4. Select the default transport database already there and click Update:



Enable ☑

Queue ID:	default
Table Name:	TransportQ_out
Multi-Threading:	☑
Number of Threads:	3
Response To Database:	□
Outgoing Directory:	C:\opt\PHINMS/shared/outgoing/

Auto Delete □

Delete Frequency:	1
Start Time:	January 1, 2007 12:00
Retention Period:	60

5. Uncheck the Response To Database option.
6. Click OK an all screens and Save on last one. Restart PHINMS.

Importing Certificates

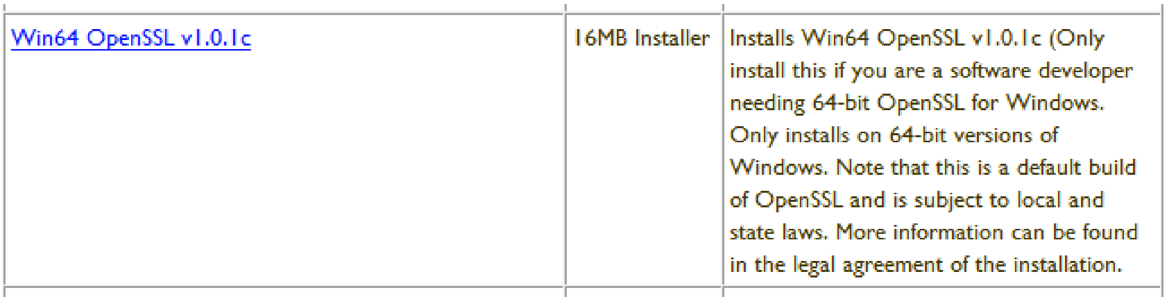
You will need to import both the SSL Trusted Certificate and the CPA file into your PHINMS client.

1. On the top menu go to: Tools -> Import Trusted Cert
    a. Locate the SSL Certificate sent by HP and open the file
    b. Select Ok
    c. Restart the PHINMS console
2. On the top menu go to: Tools -> Import CPA Files
    a. Locate the CPA file sent by HP and open the file
    b. Select Ok
    c. Restart the PHINMS console

Appendix A: URL for OpenSSL

OpenSSL can be downloaded from:
http://slproweb.com/products/Win32OpenSSL.html

The version that is downloaded must the version the technical team is using.



Win64 OpenSSL v1.0.1c	16MB Installer	Installs Win64 OpenSSL v1.0.1c (Only install this if you are a software developer needing 64-bit OpenSSL for Windows. Only installs on 64-bit versions of Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.