Implementation Guide

Public Health Information Network Messaging System (PHINMS)

Version 1.0

Prepared by:
Centers for Disease Control and Prevention

October 31, 2023

EXECUTIVE SUMMARY

Many organizations work together to protect and advance public health. These organizations use the internet to securely exchange sensitive data between various public health information systems. The exchange of data, also known as messaging, is enabled through electronic messages created by using special file formats and a standard vocabulary. The exchange uses a common approach to data security, data encryption, methods for dealing with various firewalls, and internet protection schemes. The Centers for Disease Control and Prevention (CDC) Public Health Information Network Messaging System (PHINMS) is the software that facilitates this secure messaging. PHINMS provides a standard way for addressing and routing content and a standard and consistent way for information systems to confirm an exchange. It securely sends sensitive data to and receives sensitive data from public health information systems through the internet.

The PHINMS Implementation Guide provides instructions for installation and basic configuration of the PHINMS software; advance configuration procedures are in the PHINMS Technical Guide.

REVISION HISTORY

VERSION #	IMPLEMENTER	DATE	EXPLANATION
1.0	Joseph Mai	11-30-2023	Update
1.0	Anu Gattu	12-28-2023	Update
1.0	Jannie Williams	04-11-2024	Review

TABLE OF CONTENTS

ACRONYM LIST

CDC	Centers for Disease Control and Prevention
CPA	Collaboration Protocol Agreement
CPS	Certification Practice Statement
ebXML	Electronic Business Extensible Markup Language
FAQs	Frequently Asked Questions
FTP	File Transfer Protocol
HF3	Hot Fix 3 (installs with 32 and 64 bit versions of java)
JDBC	Java Database Connectivity
LDAP	Lightweight Directory Access Protocol
PC	Personal Computer
PartyID	Party Identifier
PHINMS	Public Health Information Network Messaging System
PHINMSG	Public Health Information Network Messaging
RDBMS	Relational Database Management System
SDN	Secure Data Network
SP1	Service Pack 1
SQL	Structured Query Language
SSL	Secure Socket Layer
TLS	Transport Layer Security
TransportQ	Transport Queue
URL	Uniform Resource Locator
WorkerQ	Worker Queue

1.0 INTRODUCTION

The Public Health Information Network Messaging System (PHINMS) Implementation Guide assists users with the installation, configuration, and upgrade of the PHINMS product. It also provides instructions to install and configure PHINMS to send and receive messages from the Centers for Disease Control and Prevention (CDC) and CDC partners.

PHINMS is updated periodically; refer to the PHINMS website at www.cdc.gov/phin/php/phinms for the most current release of PHINMS software. Information available on the website includes:

- **Overview:** The overview summarizes the purpose of PHINMS and announces new PHINMS features and processes.
- **Installation:** This section of the website provides documentation pertinent to the installation and configuration of the PHINMS software.
- **Quick Tips for Getting Started:** PHINMS Quick Tips provide an overview of the information needed most often. Quick steps are documented for Release 3.3. Suggestions for additional questions can be sent to the PHINMS point of contact by using the support tab.
- **FAQs:** The list of frequently asked questions (FAQs) is stored in this section. The list contains answers to many questions users have previously submitted. The PHINMS team welcomes questions, suggestions, and/or comments.
- **Support:** The support section provides contact information for contacting the PHINMS Help Desk and accessing online help.

2.0 INSTALLATION REQUIREMENTS

2.1 PHINMS 3.3 Tests

PHINMS 3.3 has been tested on the following platforms:

- o Operating systems (64-bit only):
    - Windows Server 2019.
    - Windows 10.
- o Databases:
    - Default Databases: HSQL DB 1.8.0.4
    - Microsoft SQL Server 2019.
- o Application Servers:
    - Tomcat 9
- o Receiver Side Proxy Servers:
    - IIS 10
- o JDBC drivers.

DB SERVER	VERSION	JDBC DRIVER NAME	VERSION	DATE
MS SQL	2016	mssql-jdbc-11.2.1. jre8, mssql-jdbc-11.2.1.jre11, mssql-jdbc-11.2.1.jre17, mssql-jdbc-11.2.1.jre18	11.2.1	09/13/2022

Table 1. JDBC Drivers

Note: Java Database Connectivity (JDBC) drivers listed in this table were successfully tested for connectivity. However, CDC does not support potential defects of JDBC drivers. It is up to PHINMS users to decide which JDBC driver is appropriate to use. This table is provided for reference purposes only.

2.2 System Requirements

The installation of PHINMS 3.3 system requirements are as follow:

- Local administrator for Windows
- Minimum disk space: 6 GB
- Minimum memory: 8 GB
- TLS 1.2
- Java Open JDK or Oracle JDK from version 8 to 17.

Ensure that all the correct ports—which may be 5088 (default local host port), 443 (Hyper Text Transfer Protocol over Secure Sockets Layer [HTTPS])—are open on the firewall.

Once the requirements above have been met, proceed to Section 2.3, which can be performed simultaneously with Section 2.4.

2.3 Apply for a Digital Certificate

PHINMS users who send data to CDC are required to have a digital certificate. To obtain a certificate, contact PHIN Help Desk at PHINtech@cdc.gov. Information about digital certificates is available in the PHINMS Digital Certificate Policy | CDC section on the PHINMS website.

2.4 Software and PartyID Request

To obtain the PHINMS software, email PHIN Help Desk at PHINTech@cdc.gov. Information will need to be provided about the organization(s) that will use the software. This information will be reviewed and confirmed by the PHINMS support team, and the software download link will be emailed to the requestor.

A unique PartyID is required for every organization who uses PHINMS to send data to the CDC, contact PHIN Help Desk at PHINTech@cdc.gov to request a PartyID. The PartyID uniquely

identifies a PHINMS installation, also called an instance. The PartyID is included with every message, which informs the recipient of the originator/sender.

The PartyID is required during installation and becomes a permanent, identifying part of the application. The PHINMS application will need to be reinstalled if the PartyID needs to be changed.

Note: If there is a need to install PHINMS at more than one site or to install more than one PHINMS installation at the same site, a unique PartyID is required for each installation.

3.0 DOWNLOAD AND INSTALL THE PHINMS SOFTWARE

Install PHINMS 3.3 by using the following steps, these steps pertain to *new* installations; instructions for upgrading an existing installation are in Section 4.0.

1. Go to the link in the email sent from the PHINMS Support team**.** This will open the page to download PHINMS (Figure 3.1)

Figure 3.1. PHINMS 3.3 download page

2. Check the box on top of PHINMS 3.3 install file and check the box "I agree: Terms and Conditions" then click the Download button (Figure 3.2).

Figure 3.2. PHINMS 3.3 download page

3. In the Downloads folder double-click on the PHINMS-3.3-install.exe executable file to start the installation. The installation wizard will open, as illustrated in Figure 3.3.
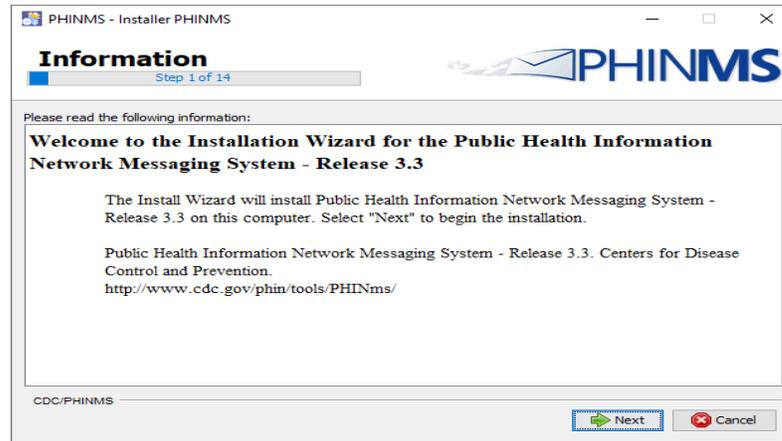
Figure 3.3. Installation Wizard Preparation Screens

4. Click Next. The licensing agreements will open as illustrated in Figure 3.4. The responsibilities of the PHINMS user are listed on this screen.
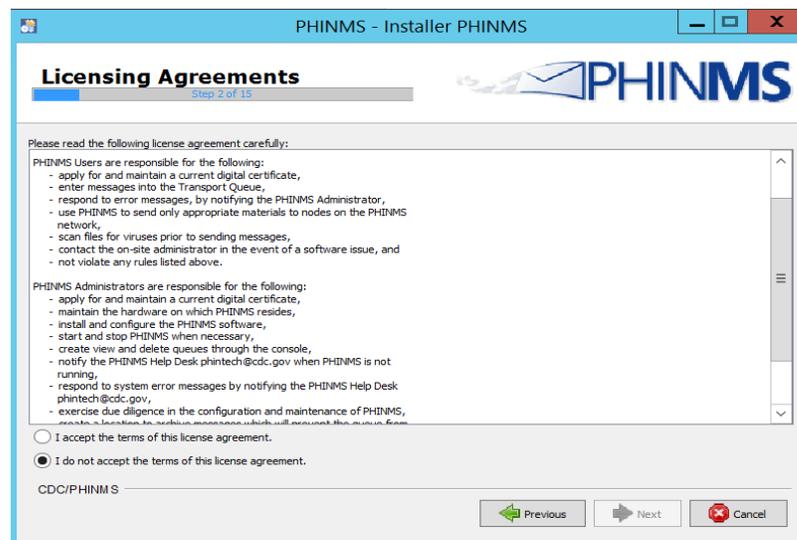
Figure 3.4. End User Licensing Agreements Screen

5. Once you have read the terms of the agreement, select "I accept the terms of the license agreement" and click Next. The user data screen will open as illustrated in Figure 3.5. This screen allows the user to select whether they are completing a new installation or an upgrade of an existing installation.

Figure 3.5. User Data Screen to Select Installation Type

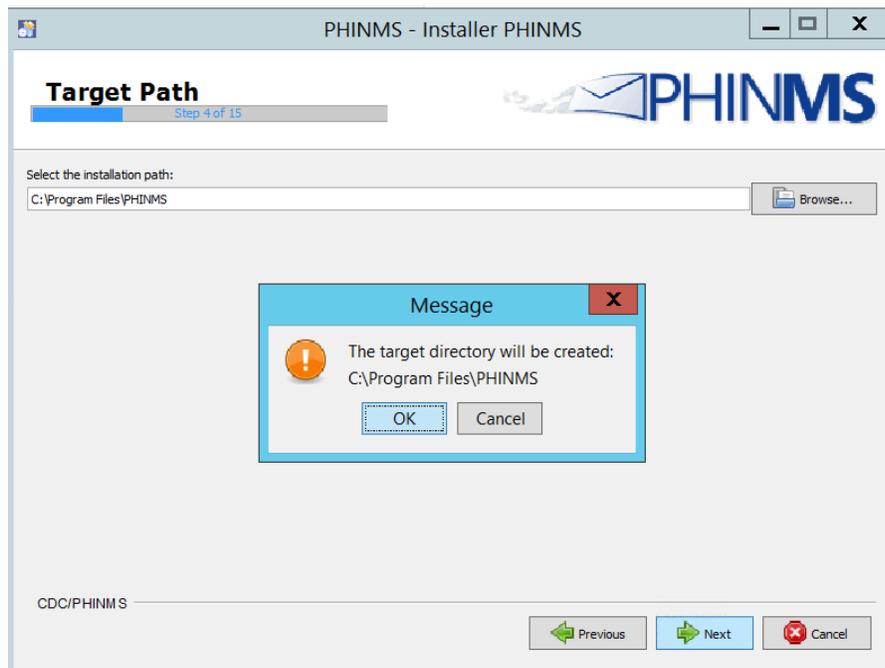6. Select New Install and click Next.

Figure 3.6. Target Path Screen

7. Click OK to select the default target directory or click browse to install to a different directory on your local computer. Click OK then click Next to proceed, a user data screen to enter the domain name and party ID will open (Figure 3.7).
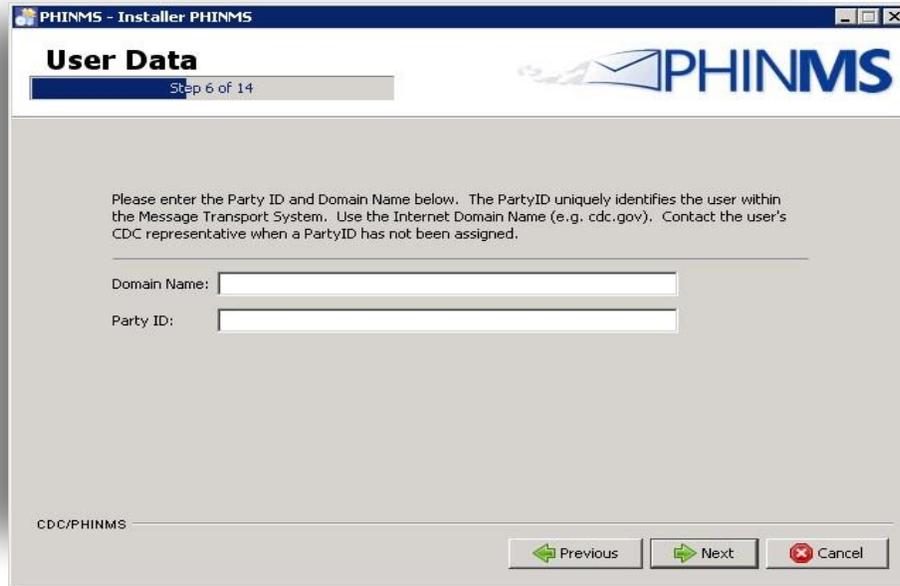
Figure 3.7. PartyID and Domain Name Screen

8. Enter the domain name (defined by user, e.g., cdc.gov) and the assigned party ID then click Next, a user data screen will open requesting the port identification information (Figure 3.8).
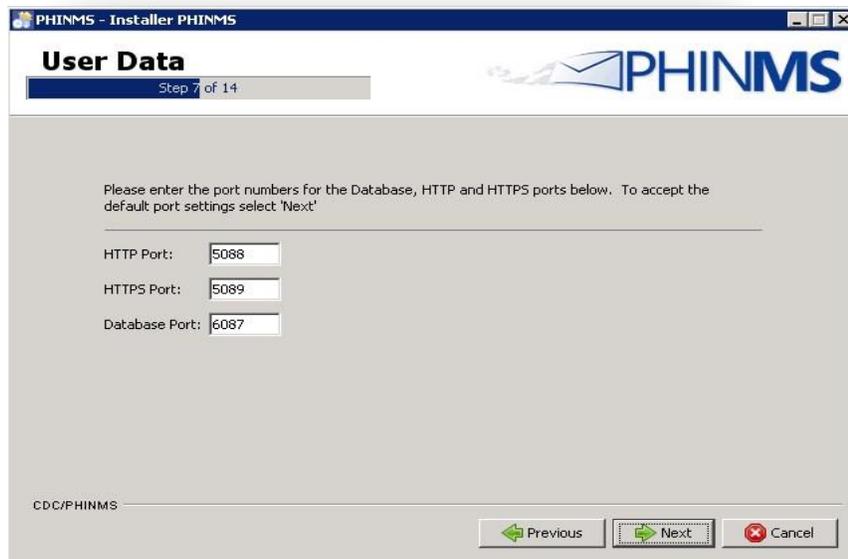

Figure 3.8. Port Numbers Screen

9. The default PHINMS port numbers are prefilled by default. Click Next, the registration screen will open as illustrated in Figure 3.9. It is optional to enter the organization name, administrator name, and email address to register the product with CDC.

Note: Do not check the box that reads, "I want to register this PHINMS instance with PHINS/CDC", currently there is no active registration server.
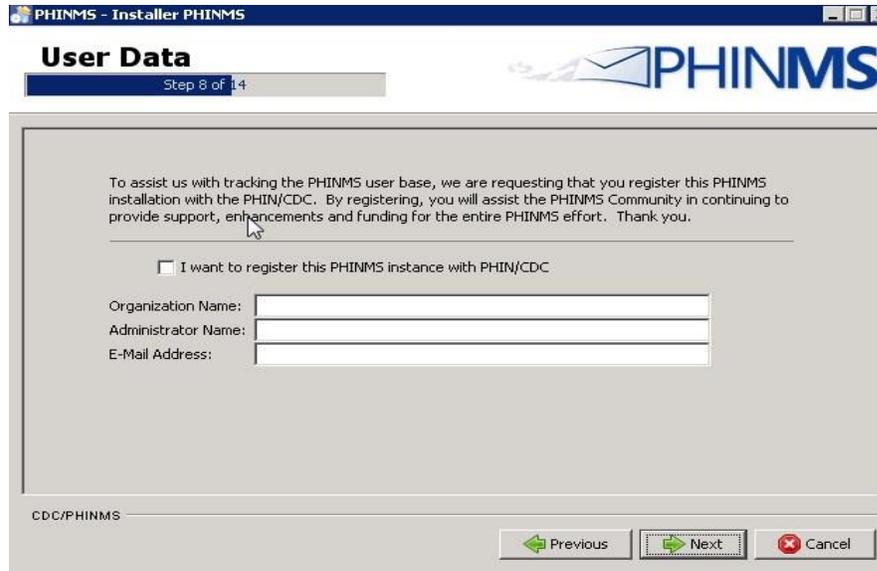

Figure 3.9. Registration Screen

10. Click Next, the select installation packages screen will display, as illustrated in Figure 3.10.

Figure 3.10. Installation Package Screen

11. PHINMS Core is checked by default. Click Next, the system will begin installation, as illustrated in Figure 3.11. Progress bars will indicate the status of the installation.

Figure 3.11. Installation Screen

12. When the installation completes, click Next, the shortcut screen will display, as illustrated in Figure 3.12. This screen displays options to create shortcuts in the PHINMS start menu.
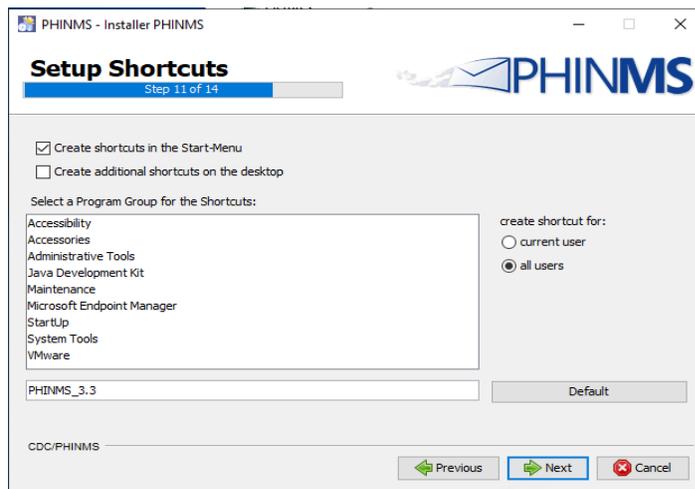

Figure 3.12. Setup Shortcuts Screen

13. Click Next, a screen with options for final actions will display, as illustrated in Figure 3.13.

Figure 3.13. PHINMS Installation Options Screen

14. Select how PHINMS is to be installed on your system (i.e., as a service and start console, service only, or not as a service [just install]) and click Next. The processing screen will display, as illustrated in Figure 3.14.
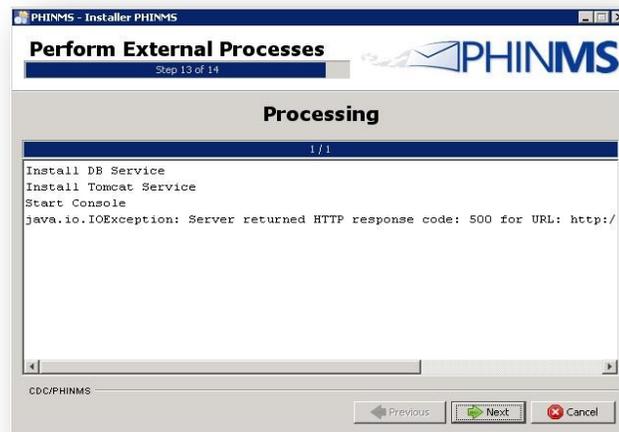

Figure 3.14. PHINMS Processing Screen

Note: Some Java versions may cause the screen to display exception or warning message, this is normal and can be ignored.

15. Click Next to initiate PHINMS for the first time. The Installation Finished window will display as illustrated in Figure 3.15. Click Done.

Figure 3.15. PHINMS Installation Finished Screen

21. The PHINMS console login screen will load, as displayed in Figure 3.16.

Figure 3.16. PHINMS Console Login Screen

22. Enter user name as "system" and password as "Phinms123" and then click Login to access the PHINMS console as displayed in Figure 3.17.
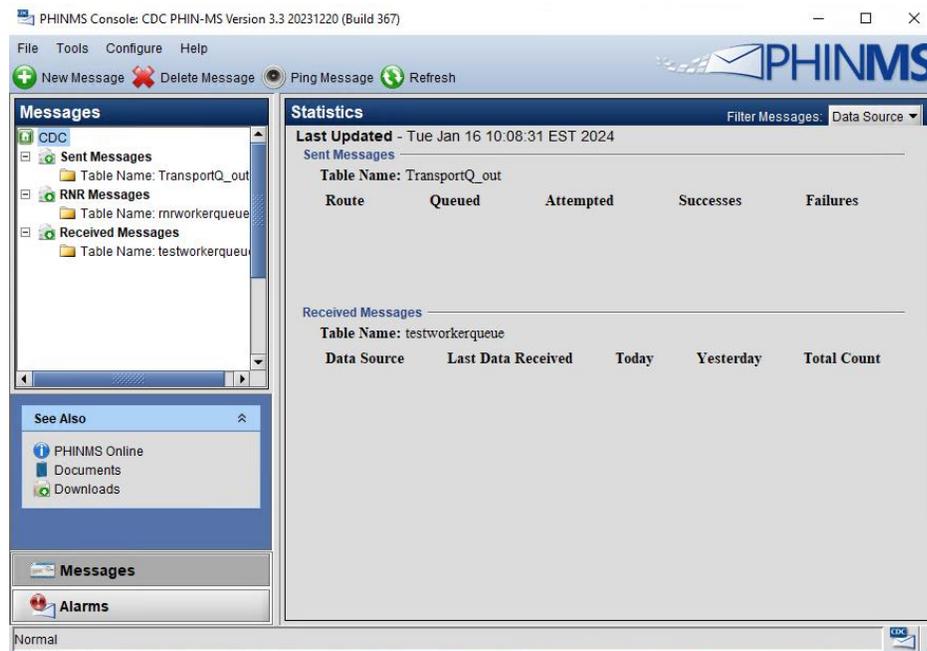
Figure 3.17. PHINMS Console

4.0 UPGRADE PHINMS SOFTWARE

PHINMS 3.3 allows user to upgrade from version 2.8 and newer. Systems using versions earlier than 2.8 must perform a fresh install of PHINMS 3.3.

Note: The PHINMS upgrade will not overwrite the previous versions. It will install PHINMS 3.3 in a new location and pull the configuration files, mainly the TransportQ table configuration information, and use this information to configure the new PHINMS 3.3 application. This process allows user to maintain the previous installation in case there are any problems with the new installation.

Complete the following steps to upgrade to version 3.3 from versions 2.8 through 3.2. PLEASE FOLLOW THESE STEPS CAREFULLY. You will need to know the file directory location of your existing version of PHINMS to complete this process:

1. If open, close the console for the previous version of PHINMS.
2. Stop the PHINMS services for the previous version of PHINMS (Windows Services).
3. Rename the existing instance of PHINMS to PHINMSold.
4. Open the executable file PHINMS-3.3-install.exe. The Installation Wizard will open (Figure 4.1).
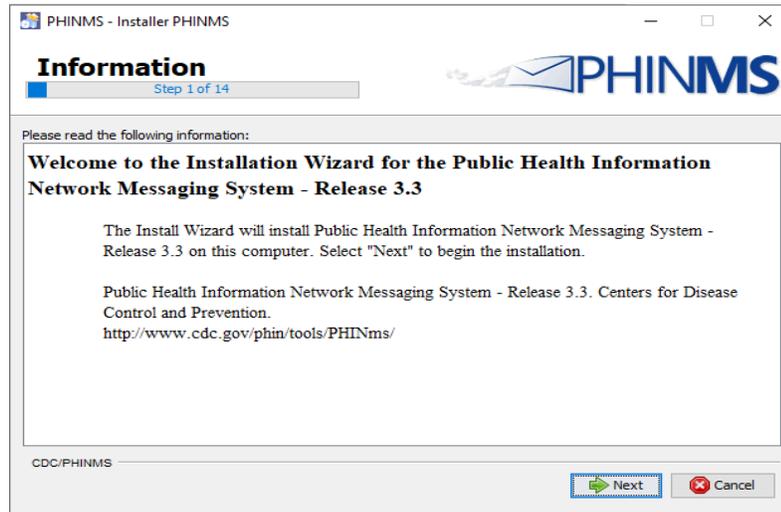
Figure 4.1. Install Shield Wizard Preparation Screens
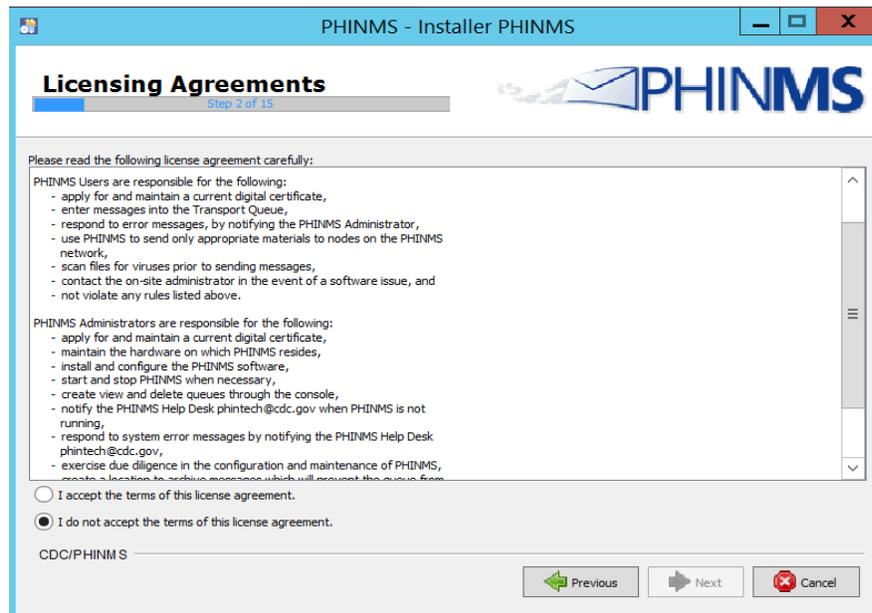
5. Click Next to proceed to the next step (Figure 4.2).

Figure 4.2. End User Agreement Screen

6. Review the licensing agreement and then select, "I accept the terms of this license agreement." and click Next to proceed to step 3 (Figure 4.3).
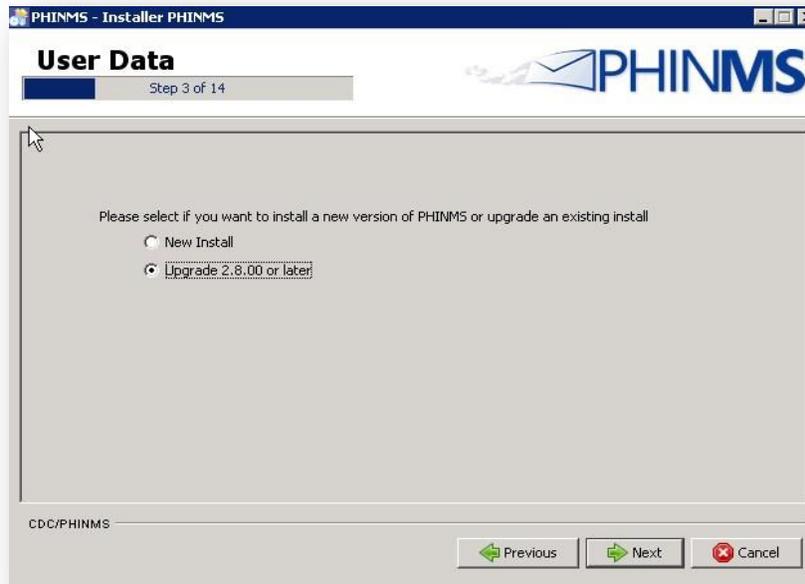
Figure 4.3. New Installation or Upgrade Screen

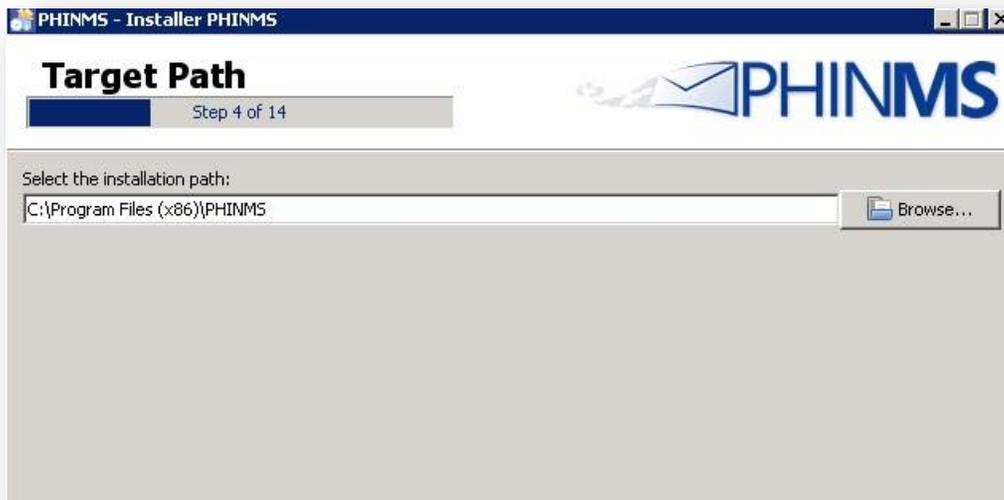7. Select Upgrade 2.8.00 or later and click Next to proceed to step 4 (Figure 4.4).

Figure 4.4. Target Path Selection Screen

8. Confirm that the default installation path is the same path as the previous version PHINMSold. If necessary, click Browse to locate that directory. Once the correct directory is in the installation path, click Next to proceed to Selection Screen for Existing PHINMS (Figure 4.5).

Figure 4.5 Selection Screen for Existing PHINSMS Instance

9. Click Browse and find the file location of the old PHINMS instance (PHINMSold). Once the correct directory shows in the selection bar, click Next to proceed to Port Numbers screen (Figure 4.6).

Figure 4.6. Port Numbers Screen

10. For the remaining steps of this upgrade refer to the previous section 3.0 steps 10 to 22.

5.0 CONFIGURE SQL DATABASES

A Structured Query Language database (HSQLDB) containing a transport queue (TransportQ) is automatically installed with the PHINMS 3.3 application. An external database can be created for the purpose of hosting the messaging queue tables. PHINMS 3.3 will support the following databases for hosting messaging queues (only Microsoft SQL Server were tested with PHINMS 3.3):

- HSQLDB 1.8.0
- Microsoft SQL Server.
- MySQL.
- Oracle.

An HSQL database is provided with the PHINMS installation on the Windows platform as a default database and facilitates installation testing. It is recommended that PHINMS users conduct an evaluation of the tradeoffs between SQL and a high transaction-volume relational database management system (RDBMS) such as others listed above.

All table scripts needed for PHINMS external database configurations for the databases listed above can be found in "PHINMS 3.3 Technical Guide" document PHINMS Installation | CDC.

Note: To use an external database (DB) connection, the appropriate JDBC driver must be imported into PHINMS via the PHINMS Console Tools option. "PHINMS 3.3 Technical Guide" also contains external DB connection string properties.

6.0 SENDER INFORMATION

PHINMS has two components: the sender and the receiver. Sending a test message allows the PHINMS Sender to send messages from the TransportQ to a receiver such as the CDC. Testing the PHINMS installation is a three-part procedure:

1. Ping the PHINMS Sender loopback route.
2. Ping a configured PHINMS route (Collaboration Protocol Agreement [CPA] files must be imported on the receiving side).
3. Ping the PHINMS CDC Staging Receiver (CPA files must be emailed to Phintech@cdc.gov. See Section 6.4 for more information).

6.1 Ping Loopback

The Ping Loopback validates that the PHINMS installation was downloaded and installed successfully on the sender's system. This process is not a test to verify that messages can be sent outside of a firewall if one is present.

Verify that the generated Ping Loopback is sent to the loopback message processor successfully by completing the following steps:

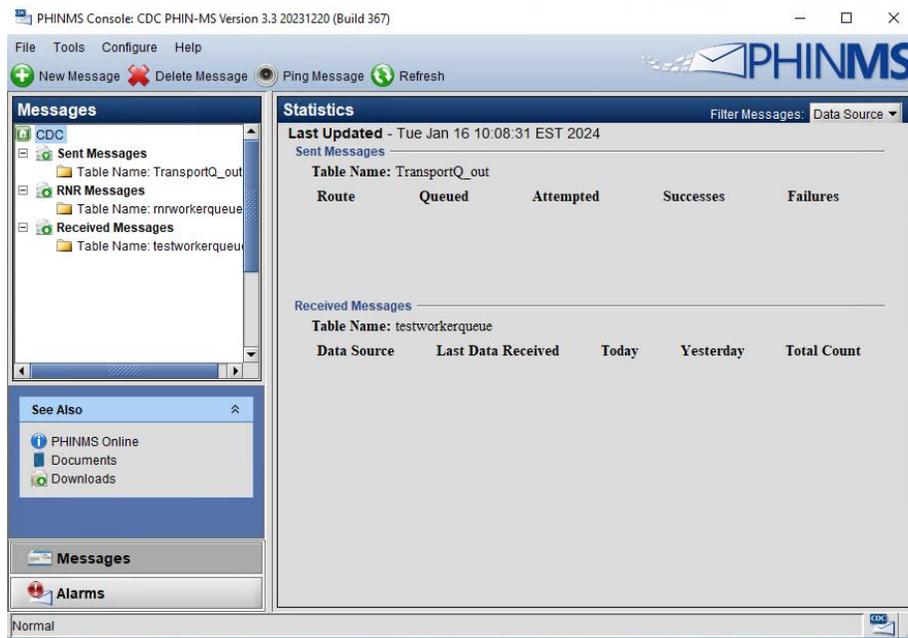1. Open the PHINMS Console (Figure 6.2).

Figure 6.2. PHINMS 3.3 Console

2. Click Ping Message in the top menu bar to display the ping dialog box (Figure 6.3).
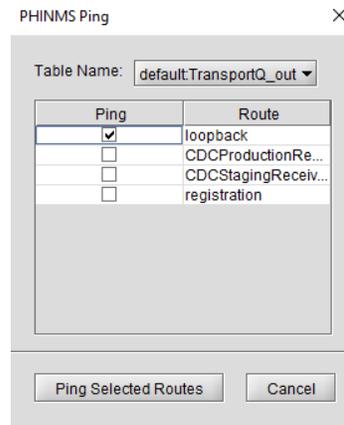

Figure 6.3. PHINMS Ping Screen

3. Select loopback, then click Ping Selected Routes to return to the console with the loopback screen open (Figure 6.4).
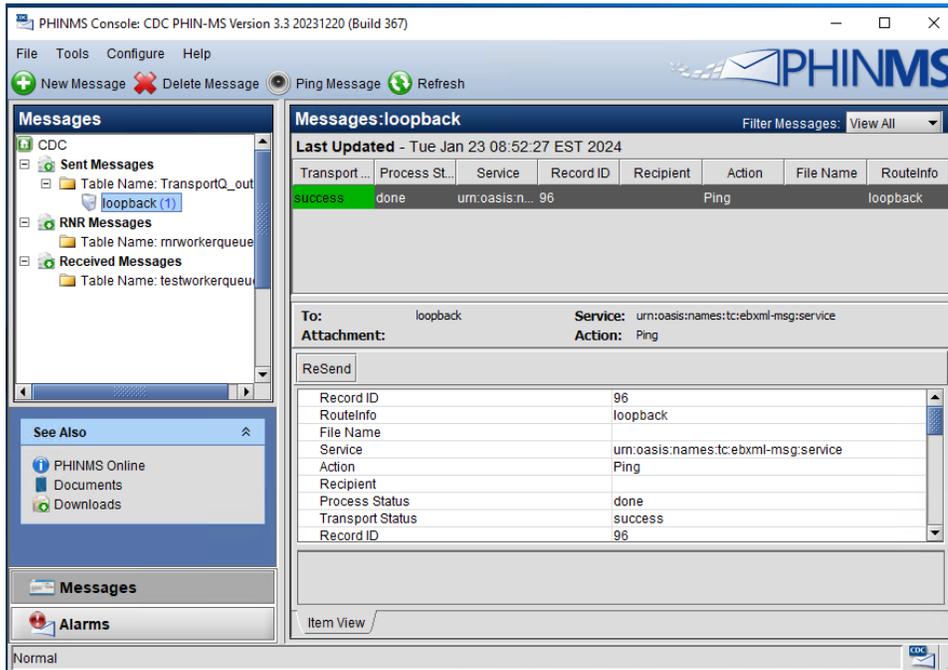
Figure 6.4. Ping Message Screen in PHINMS Console

4.   In the right-hand dropdown menu, select the loopback folder showing the status of the ping.

Note: When the Transport status (first column in the status block) lists a status of "queued" or "attempted," click Refresh in the top menu bar until the status changes.

6.2 Configure CDC Staging Receiver Route Map

The CDC Staging Receiver must be configured before sending a ping. Configure the CDC Staging Receiver by using the steps detailed in this section.

Note: Perform these steps only if sending to CDC. A digital certificate must be obtained before a successful ping test can be sent.

1.   Open the PHINMS 3.3 Console (Figure 6.5).
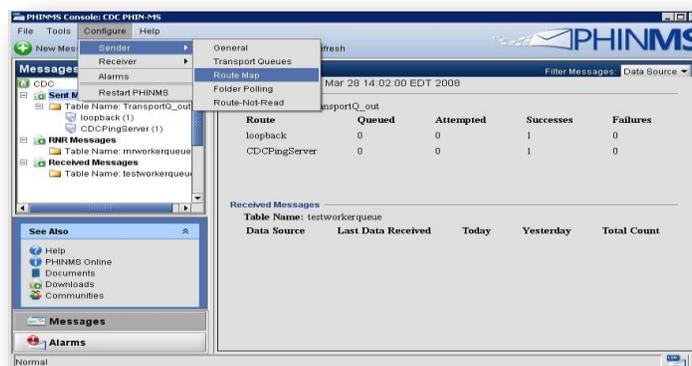
Figure 6.5. PHINMS 3.3 Console

2. Go to the Configure option in the menu bar and select Sender>Route Map as illustrated in Figure 6.5. This action will open the Sender Configuration screen (Figure 6.6).

Figure 6.6. Sender Configuration Screen

3. Select CDCStagingReceiver and click Update to open the Route Map dialog box (Figure 6.7).
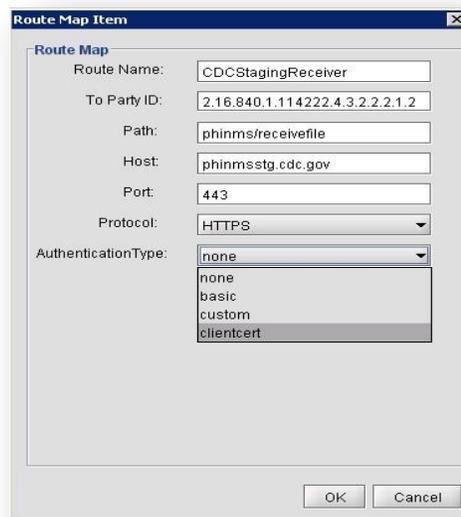
Figure 6.7. Route Map Item Dialog Box

4. Select "clientcert" from the Authentication Type dropdown list. Click OK to return to the Route Map dialog box (Figure 6.8).

Figure 6.8. Route Map Item Dialog Box

5. Enter the (.pfx) path to the stored certificate Key Store. This is the digital certificate issued to the person who will use it to send data to CDC.

6. Enter the associated password in the Password field and click OK to return to the Sender Configuration screen (Figure 6.9).
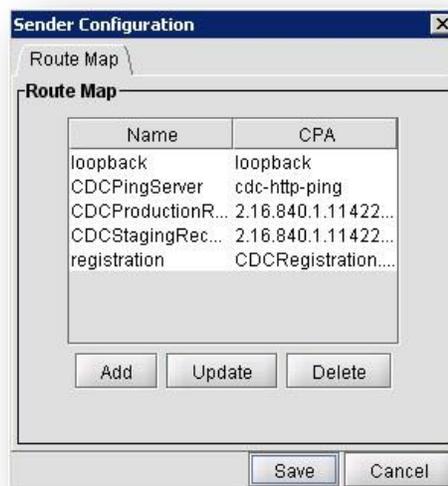
Figure 6.9. Sender Configuration Screen

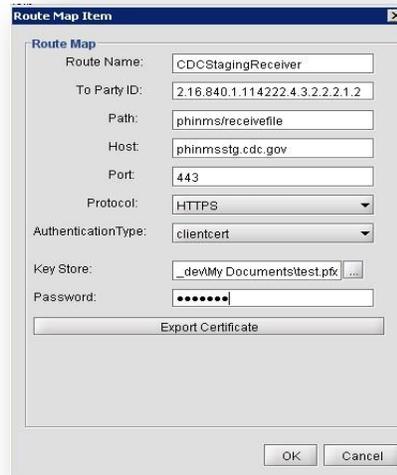7. Click Save to set configuration. If all information has been entered correctly, the system will return a success message (Figure 6.10).

Figure 6.10. Confirmation that Route Configuration Successful

8. Click OK and restart PHINMS by going to the Configure menu in the PHINMS Console menu and selecting Restart PHINMS (Figure 6.11).
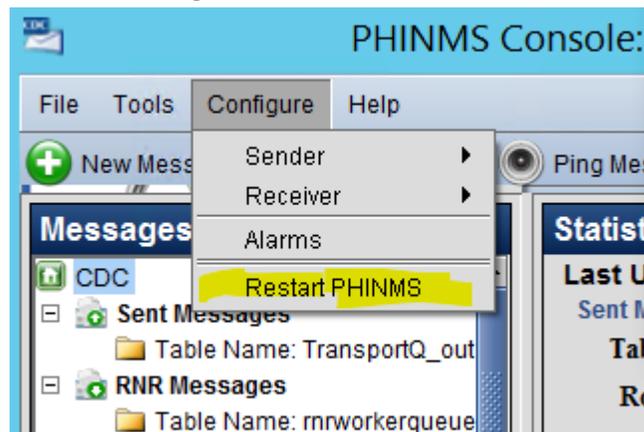
Figure 6.11. Restart PHINMS Console

6.3 Ping a Valid PHINMS Route

The Ping Message validates that the Sender can connect to the Internet and to the selected route. Verify the Ping Message to the selected route is successful by completing the following steps:

1. Open the PHINMS 3.3 Console (Figure 6.12).

Figure 6.12. PHINMS 3.3 Console

2. Select Ping Message in the top menu bar to open the PHINMS Ping screen (Figure 6.13).

Figure 6.13. PHINMS Ping Screen

3. Select route of choice. This example uses CDCStagingReceiver.

Note: You must have a valid digital certificate configured to ping any route requiring client certificate authentication (see section 6.2).

4. Click Ping Selected Routes to return to the console (Figure 6.14).

Figure 6.14. Ping Message Screen in PHINMS Console

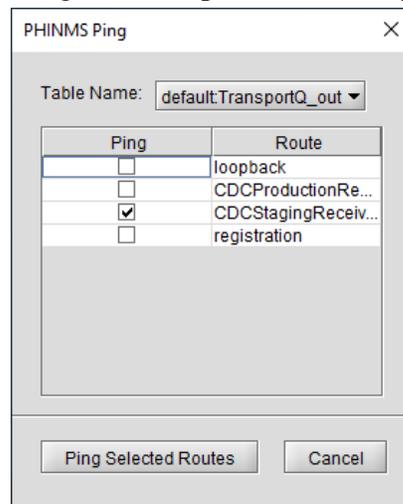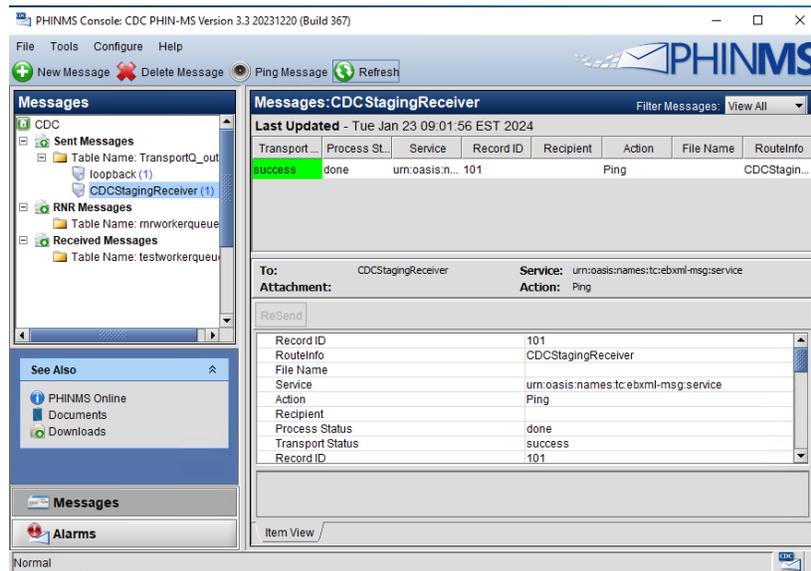5. In the left-hand dropdown menu, select the CDC folder showing the status of the ping.

Note: When the Transport Status (first column in the status block) lists a status of "queued" or "attempted," click Refresh in the top menu bar until the status changes.

6.4 Email CPA File

PHINMS creates a CPA file for each route listed in the PHINMS Route Map tab of the Sender Configuration panel. The PHINMS administrator must export the CPA for any configured route and send the related CPA to the receiving site to import into the receiving PHINMS console. To send to CDC, export the CPA file and send it to the PHIN Help Desk (Phintech@cdc.gov). Only after the PHIN Help Desk has received the CPA file and applied it to the PHINMS Receiver messages will be successfully transmitted from the sender to the CDC.

The required CPA files are in directory (PHINMS install directory)\ config\sender \CPA.

6.5 Export the CPA file

1. Open the PHINMS Console. Using the Tools option in the main menu, select Export CPA Files (Figure 6.15).
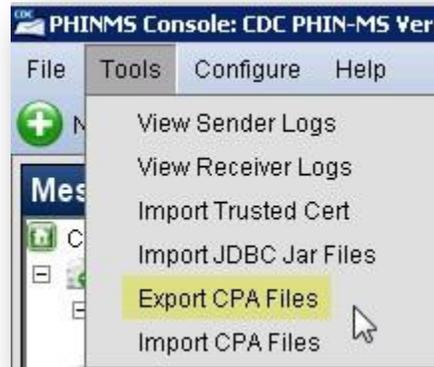
Figure 6.15 PHINMS Tools>Export CPA Files

2. Select the route to export the CPA. For this example, the export is for the CDCStagingReceiver route (Figure 6.16).
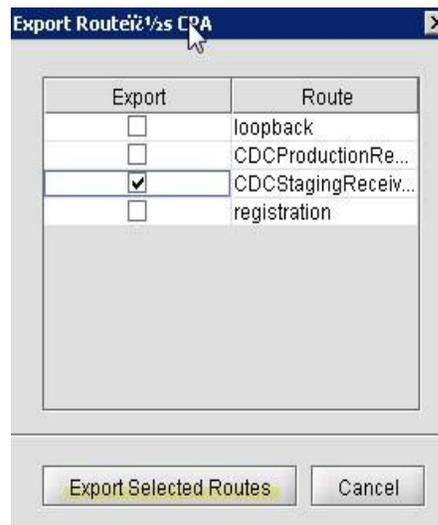
Figure 6.16. Export Route CPA Screen

3. Click Export Selected Routes.
4. Browse to the location where the CPA file will be exported.
5. Email the exported CPA file to the appropriate receiving site (PHIN Helpdesk for the this example).
6. Once the receiving site has confirmed that the CPA file is imported, use the steps in the next Section to test the route.

6.6 Send Test Payload Message

The Send Payload Message option verifies the capability to send an outbound message with an attached file to a receiver. Users must have received a confirmation that the required CPA files have been sent to the PHIN Help Desk before attempting to send a payload message to CDC.

To send the test payload message to the PHINMS Staging Receiver:

1. Open the PHINMS Console (Figure 6.17).
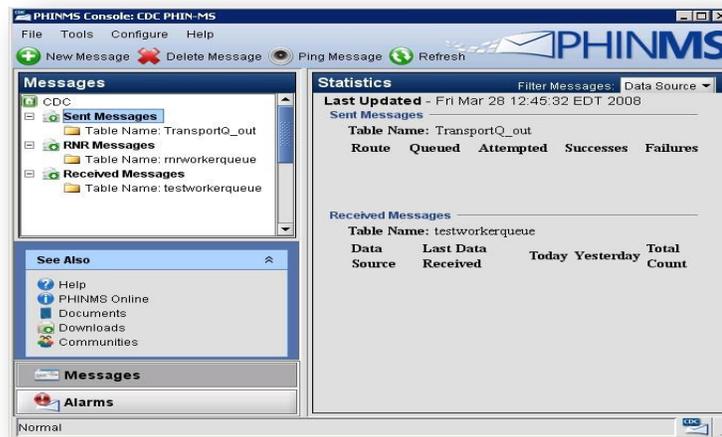

Figure 6.17. PHINMS Console

2. Select New Message from the top menu bar to open the Send Message screen (Figure 6.18).
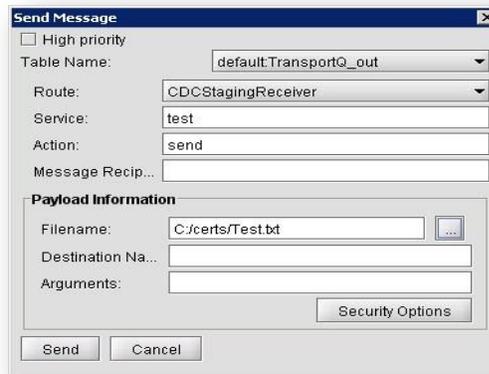
Figure 6.18. PHINMS Send Message Screen

3. Enter the Send Message parameters provided by the receiving site or, if sending to CDCStagingReceiver, use the parameters below:
    –   **Route:** CDC Staging Receiver

- **Service:** test
- **Action:** send
- **Message Recipient:** optional - can be left blank
- **Filename:** browse to the test file to be sent to the receiver
- **Destination Name:** optional - can be left blank
- **Arguments:** optional - can be left blank.

Note: Security options are available for encrypting or signing messages if desired. It is required for data sent to the CDC to be encrypted, contact Help Desk at PHINTech@cdc.gov for assistance in configuring encryption to send data to the CDC.
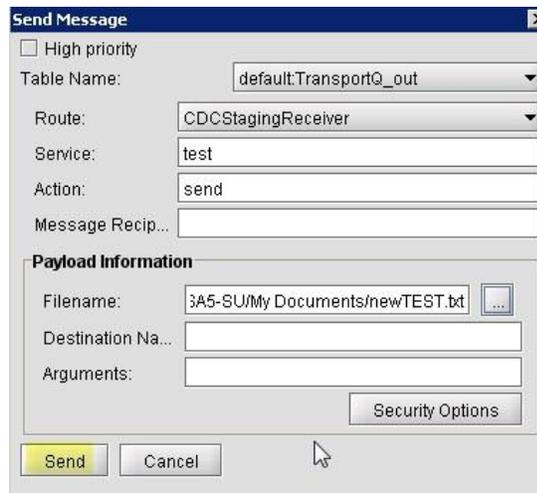
Figure 6.19 Send Message Screen

4. Click Send. If the message is successfully queued, PHINMS will display a confirmation message (Figure 6.20).
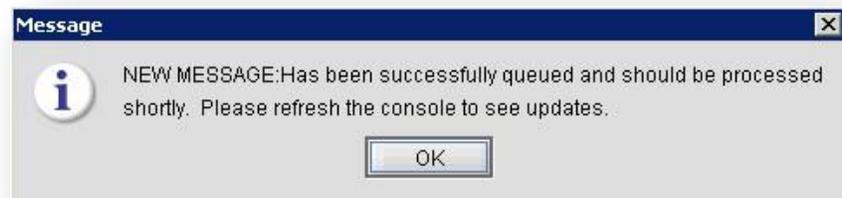
Figure 6.20. Message Sent Confirmation

5. Click OK

7.0 RECEIVER INFORMATION

7.1 Configure WorkerQ

The worker queue (WorkerQ) is the database table used for storing inbound messages. When configured from the receiver configuration screen in the console, the WorkerQ is used to store incoming messages sent to the receiver. The database configuration needs to be completed before creating the WorkerQ table.

If configured from the sender configuration screen in the console, the WorkerQ is used to write the responses to polling requests (route-not-read configuration). More information on sender configuration can be found in the PHINMS Technical Guide.

Create an external database WorkerQ table by using the following steps:

1. Open the PHINMS 3.3 Console (Figure 7.1).
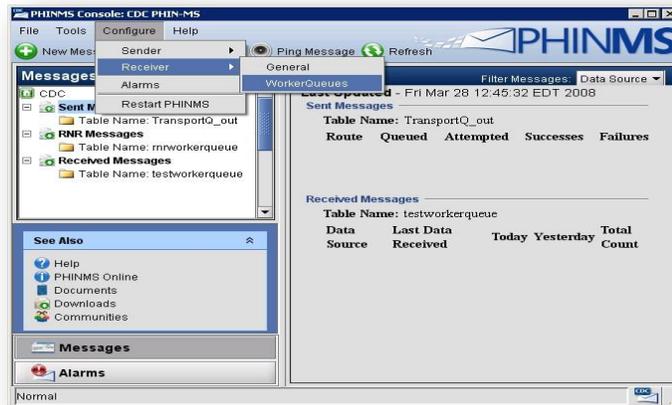
Figure 7.1. PHINMS 3.3 Console

2. Using the Configure dropdown in the main menu, select Receiver>WorkerQueues. The Receiver Configuration screen will open (Figure 7.2).

Figure 7.2. Receiver Configuration - Database

3. Click Add to open the Database Item screen (Figure 7.3). (A user can also update or delete a database once it is added by using the appropriate buttons in Figure 7.2).

Figure 7.3. Database Item

4. Enter the database items. Refer to Table 4 for an explanation of the values.

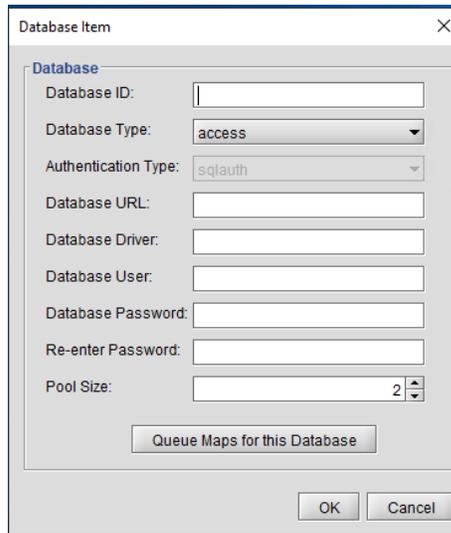| TAG VALUE	DESCRIPTION
Database ID	The unique name for the database connection pool, referenced in the queue map. The service map uses the **databaseId** to map the queue to a specific database. (The unique databaseId is determined by the user.)
TAG VALUE	DESCRIPTION
Database Type	Designates the type of database.
Authentication Type	For SQL Server database type only, the drop-down list will be enabled when SQL Server database type is selected.
Database URL	The URL for the database. The URL depends on the type of database and driver used, (e.g., jdbc:sqlserver://host:portnumber;DatabaseName=database for Microsoft SQL Server and jdbc:oracle://host:port:sid for Oracle).
Database Driver	The type of JDBC driver. The JDBC driver should be appropriate for the type of database, (e.g., com.microsoft.sqlserver.jdbc.SQLServerDriver for Microsoft SQL Server and oracle.jdbc.OracleDriver for Oracle).
Database User	The database user account is provided by the database administrator for login purposes and to automate the login process via PHINMS. A pointer to the database user entry is in the message receiver's encrypted password store. The value is not the database user but the name of the tag within the password file. The value of the tag contains the actual database username. If Authentication Type "windows authentication" is selected this field is greyed out.

Database Password	This password is provided as part of the user account created by the database administrator for login purposes and to automate the login process via PHINMS. A pointer to the database password entry is in the message receiver's encrypted password store. The value is not the database password but the tag within the password file. The value of the tag contains the actual database password. If Authentication Type "windows authentication" is selected this field is greyed out.
Pool Size	Pool size is the number of database connections to open. When setting the pool size, users should ensure that the system can handle the maximum client load while keeping enough memory available.

Table 4. WorkerQ Database Tag Values

Note: If Authentication Type "windows authentication" is selected 'database user' and 'database password' fields will be greyed out. Before using "windows authentication" type for SQL server, Tomcat service logon needs to be changed from "local system" to "local service" (Figure 7.31) and the "sqljdbc_auth.dll" file needs to be present in the C:\Windows\System32\ directory, contact PHINTech@cdc.gov to request for the "sqljdbc_auth.dll" file (Figure 7.32)
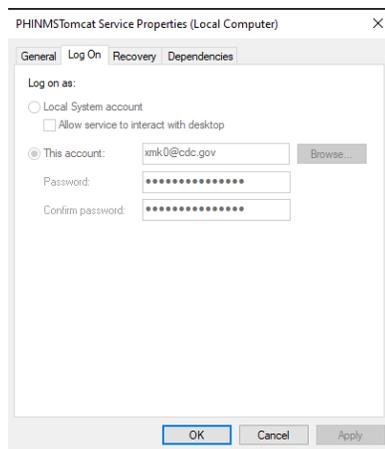
Figure 7.31
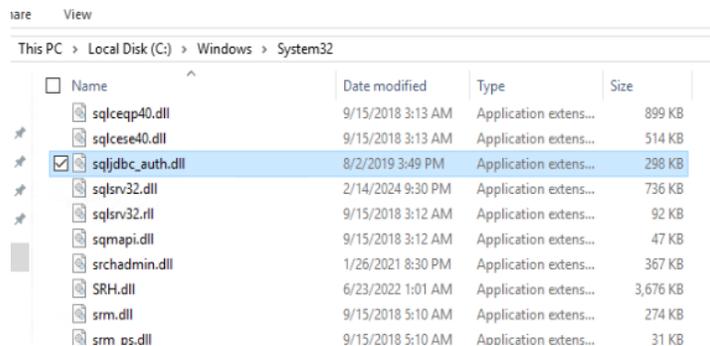
Figure 7.32

5. After entering the database items, click Queue Maps to open the Queue Maps menu (Figure 7.4).

Figure 7.4. Queue Maps Menu

6. Click Add to open the Queue Map entry screen (Figure 7.5).
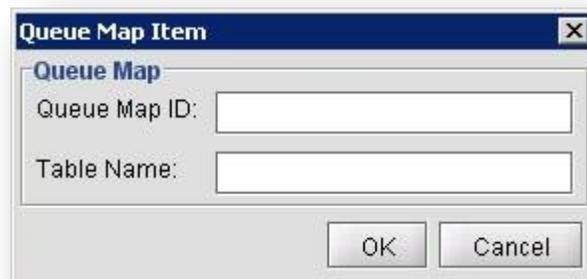
Figure 7.5. Queue Map Item Entry Screen

7. Enter the Queue Map ID (determined by the user).
8. Enter Table Name
   » Click OK
   » Click OK
   » Click OK.
9. Click Save. If configuration was successful, PHINMS will display a confirmation screen (Figure 7.6).

Figure 7.6. WorkerQ Database Configuration Successful

10. Click OK.

11. Using the Configure option in the PHINMS console main menu, select Restart PHINMS.

7.2 Create Service and Action Pair

PHINMS uses message envelopes for each sent message. The envelope has address information tags called Service and Action. These tags are known as character strings and are logically mapped to an application queue on the receiving side. The Service and Action tags determine the message type.

Create a Service and Action pair by completing the following steps:

1. Open the PHINMS 3.3 Console (Figure 7.7).
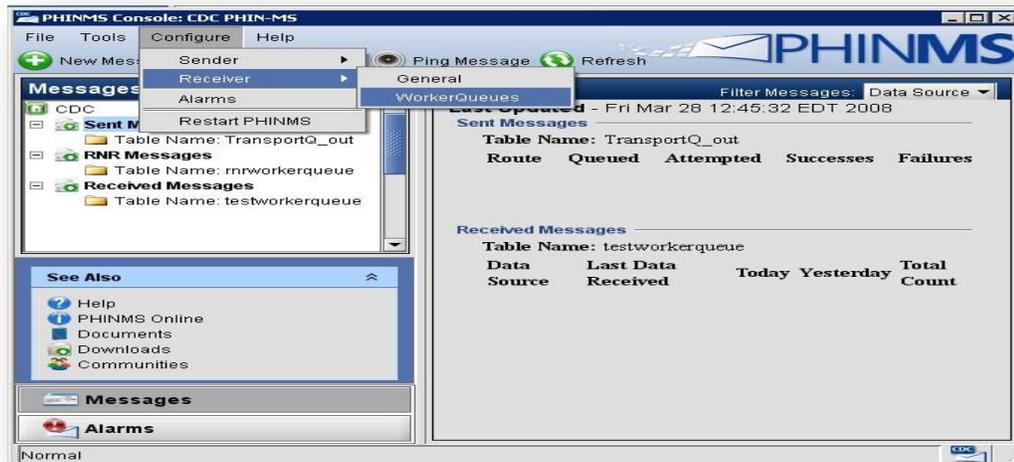
Figure 7.7. PHINMS 3.3 Console

2. Using the Configure dropdown in the PHINMS console main menu, select Receiver>WorkerQueues to open the Receiver Configuration menu (Figure 7.8). Click the Service Map tab (Figure 7.8).
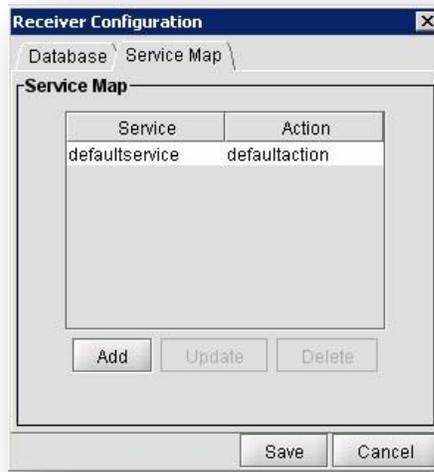
Figure 7.8. Service Map Menu

3.   Click Add to open the Service Map Item menu (Figure 7.9).
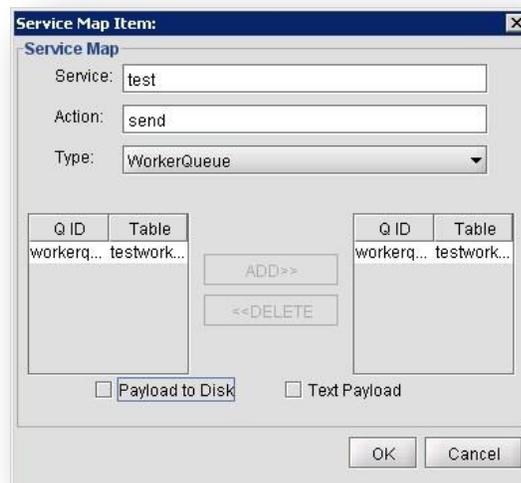
Figure 7.9. Service Map Item Menu

4. Enter Service.
5. Enter Action.
6. Select WorkerQueue from the dropdown list.
7. Highlight WorkerQueue in the Q ID column on the left-hand side.
8. Click the Add button located between the two columns.

9. Click OK to return to the Receiver Configuration screen (Figure 7.10). The selected options will appear in the Service Map list.

Figure 7.10. Confirmation of Service and Action Added

10. Click Save. If the configuration was successful, PHINMS will display a confirmation message (Figure 7.11).

Figure 7.11. Service and Action Successful Configuration

11. Click OK.
12. Using the Configure option in the PHINMS console main menu, select Restart PHINMS.

Figure 7.12. Service Map Item

Note: When Payload to Disk is checked in the Service Map Item menu (Figure 7.12), the incoming payload is written to disk instead of to the database field. The default location for payload to disk is (*...\PHINMS\shared\receiverincoming*).

8.0 UNINSTALL PHINMS

Complete the following steps to uninstall PHINMS:

1. Click the Start button on your computer. Go to All Programs>PHINMS>Uninstall PHINMS. This action will open the DOS menu displayed in Figure 8.1.
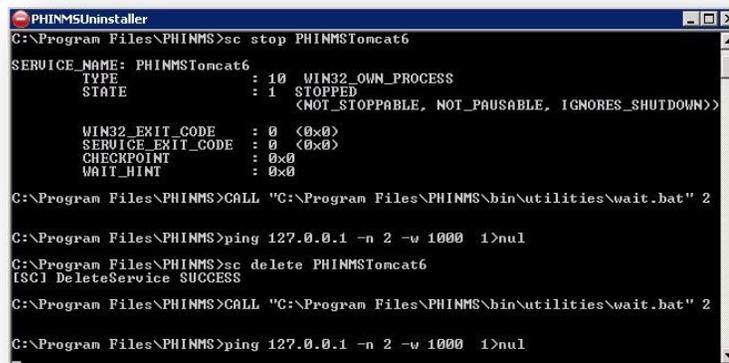
Figure 8.1. PHINMS Uninstaller Screen

2. The DOS window confirms that the application is removed and deleted. This initiates the application uninstaller screen (Figure 8.2).

Figure 8.2. Application Uninstaller

3. Select "Force the deletion of C:\Program Files\PHINMS (i.e., the PHINMS install directory folder) structure," then click Uninstall. The middle progress bar will display the status of the uninstall process. When the program is uninstalled, the status bar will read, "Finished" (Figure 8.3).

Figure 8.3. Successful Uninstall Confirmation

4. Click Quit.
    Note: PHINMS can also be uninstalled by running the Uninstaller file in the …\PHINMS\Uninstaller\ folder.
5. Open the computer's C: drive and navigate to the PHINMS install directory (Figure 8.4).

Figure 8.4. PHINMS Install Directory

6. Delete the PHINMS install directory. These steps will successfully uninstall PHINMS.

9.0 ADDITIONAL FEATURES

9.1 Import CPA

PHINMS allows the user to import the CPA directly from the PHINMS Console. Complete the following steps to import the CPA:

1. Open the PHINMS Console.
2. Open the Tools dropdown from the main menu.
3. Click Import CPA.
4. Select the CPA to import.
5. Click Open.
6. Click OK.

9.2 View Receiver Logs

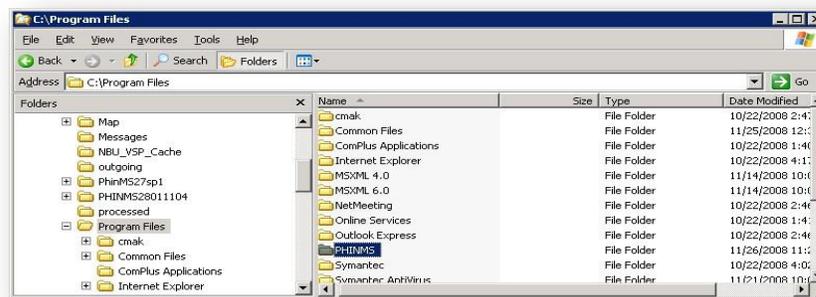The Receiver Logs store information on the status of received messages and can be viewed directly from the PHINMS Console. Viewing the logs allows users to check the status of received messages. Complete the following steps to view the Receiver Logs:

1. Open the PHINMS Console.
2. Open the Tools dropdown from the main menu.
3. Select Receiver Logs.
4. Select Route from the dropdown list.
5. Select Date.
6. Click View to display the log text.

9.3 View Sender Logs

The Sender Logs store information on the status of sent messages and can be viewed directly from the PHINMS Console. Viewing the logs allows users to check the status of sent messages. Complete the following steps to view the Sender Logs:

1. Open the PHINMS Console.
2. Open the Tools dropdown from the main menu.
3. Select View Sender Logs.
4. Select Route from the dropdown list.
5. Select Date.
6. Click View to display the log text.

9.4 Import Trusted Certificate

A trusted certificate consists of a root and intermediate certificate authority (CA) certificate. When the browser is trying to make an SSL (secure socket layer) connection, it needs to validate the certificate chain of the SSL certificate installed on the proxy server on the receiver's end. PHINMS Sender verifies the chain by using CACERTS Key Store file. If the chain does not

match, the sender must import the trusted certificate into the CACERTS Key Store file by using an import option. Complete the following steps to import the trusted certificate:

1. Open the PHINMS Console.
2. Open the Tools dropdown from the main menu.
3. Select Import Trusted Cert.
4. Navigate to the location where the Trusted Certificate is stored.
5. Select the Trusted Certificate (.cer or .pem file) to import.
6. Click Open, then restart PHINMS by going to the Configure menu in the PHINMS Console main menu and selecting Restart PHINMS.

9.5 Import JDBC JAR Files

JDBC Jar Files can be imported directly from the PHINMS Console. Complete the following steps to import JDBC Jar files:

1. Open the PHINMS Console.
2. Open the Tools dropdown from the main menu.
3. Select Import JDBC Jar files.
4. Locate and select the JDBC driver for your database.
5. Click Open.
6. A message will indicate a successful import. Click OK.
7. Restart PHINMS Tomcat Instance located in the Windows services console.

9.6 Change Login Password

PHINMS allows user to change the Console login password. Complete the following steps to change the login password:

1. Open the PHINMS Console.
2. Open the File dropdown from the main menu.
3. Select Change Login Password.
4. Enter the Old Console Password in the appropriate block.
5. Enter the New Console Password and Re-Enter New Console Password in the appropriate blocks.
6. Click Change Password.
7. Click OK.
8. Exit PHINMS Console.
9. Restart PHINMS Apache Tomcat service.

9.7 Sender and Receiver Alarms

PHINMS contains system alarms for the sender and receiver. This feature allows the user to acknowledge and enter a resolution for each alarm. Configure the alarm features by completing the following steps:

1. Open the PHINMS Console.
2. Open the Configure dropdown from the main menu.
3. Select Alarms.
4. Check Report Alarms.

Note: When Report Alarms is selected, the alarms can be viewed in the console and configuration of the Email Alarms feature can be configured.

5. Complete the following fields:
   » SMTP Server - required
   » User Name
   » User Password
   » Re-Enter User Password
   » From Address – required.
6. Click OK.

9.8 Alarm Resolution

The Alarm Resolution feature allows the user to view error and help messages. It also allows the user to store the resolution information. The Alarm Resolution feature can be implemented by using the following steps:

1. Open the PHINMS Console.
2. Select Alarms, located at the lower left-hand corner of the console. The Sender Alarms information will display in the main console window (Figure 9.1).
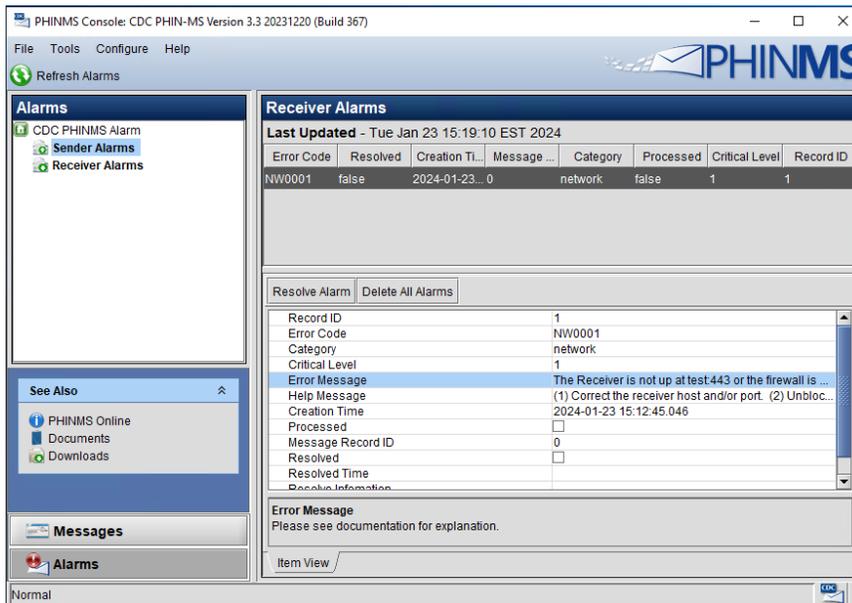

Figure 9.1. Alarms

3. Select the message to be reviewed.

4. Select Resolve Alarms to open the Process Alarm screen (Figure 9.2).
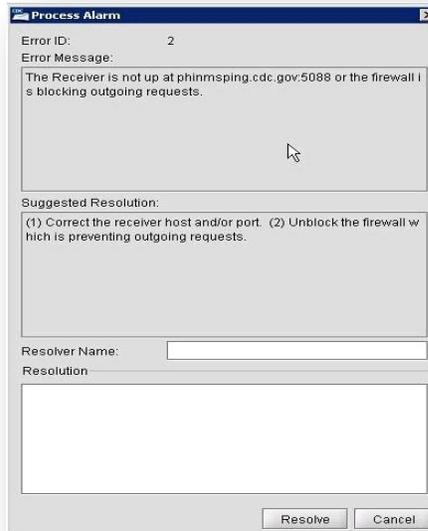
Figure 9.2. Alarm Resolution

5. Review the Error Message and the Suggested Resolution.
6. Enter the name of the person who resolved the alarm in the Resolver Name block.
7. Enter the Resolution in the appropriate block.
8. Click Resolve. PHINMS will confirm successful processing of the alarm (Figure 9.3).

Figure 9.3. Alarm Successfully Processed

9. Click OK.

10. PHINMS also offers the option to delete all alarms by using the Delete All Alarms button in the main alarms window in the Console (Figure 9.1).

9.9 Folder-Based Polling

This feature makes it easier for applications to interface with PHINMS. Senders can configure the console for folder-based polling. This feature allows the sender to store the messages in a folder and

the system will send the messages from the folder instead of a database. The associated route is defined in the console and does not need file descriptors. Configure the Folder Based Polling feature by completing the following steps:

1. Open the PHINMS Console.
2. Open the Configure dropdown from the main menu.
3. Select Sender>Folder Polling.
4. Check Folder Based Polling box.
5. Click Add.
6. Populate the Folder Properties.
7. Select Security Options.
8. Click OK.
9. Click Save.
10. Click OK.
11. Click the PHINMS Console Restart button.
12. Create the following three (3) folders in any directory:
    » Outgoing - used to store messages to be sent.
    » Processed - regional file of messages that have been processed.
    » Acknowledgement - stores the message receipt from the receiver.

9.10 Transport Queue Auto Delete

1. Open the PHINMS Console.
2. Open the Configure dropdown from the main menu.
3. Select Sender>TransportQueues.
4. Select the Transport Queue to be modified.
5. Click Update.
6. Click Queues for this database.
7. Select the table to be modified.
8. Click update.
9. Locate the auto delete section.
10. Enable Auto Delete.
11. Modify the Frequency to your desired setting.
12. Configure a start date and time.
13. Modify Retention Period to your desired setting.
14. Click OK three times, then click Save.
15. Click OK on the acknowledgement.
16. Click Configure.
17. Click Restart PHINMS.

9.11 Worker Queue Auto Delete

1. Open the PHINMS Console.
2. Open the Configure dropdown from the main menu.
3. Select Receiver>WorkerQueues.
4. Select the WorkerQueues to be modified.
5. Click Update.
6. Click Queues for this database.
7. Select the table to be modified.
8. Click Update.
9. Locate the auto delete section.
10. Enable Auto Delete.
11. Modify Frequency to your desired setting.
12. Configure a start date and time.
13. Modify Retention Period to your desired setting.
14. Click OK three times, then click Save.
15. Click OK on the acknowledgement.
16. Click Configure.
17. Click Restart PHINMS.

9.12 Secondary Receiver Decryption Certificate

PHINMS contains an option to configure a secondary keystore for decrypting files. This option is used when there are two valid certificates, a new certificate (primary) and an old/expiring certificate (secondary). If a sender sends an encrypted file, it is possible that the file will be encrypted with a certificate that has not expired.

The primary and secondary key store locations allow the receiver to configure both new and old certificates. If a file is received encrypted with the new certificate, it will decrypt; if it is encrypted with the old certificate, it will still decrypt until the expiration date is reached.

1. Open the PHINMS Console.
2. Open the Configure dropdown from the main menu.
3. Select Receiver>General.
4. Select Security Category.
5. In the Primary Key Store location, enter the path to the new decryption key.
6. Enter the password for the new decryption key.
7. In the Secondary Key Store location, enter the path to the older decryption key.
8. Enter the password.
9. Enter the date the old decryption key expires, in the format yyyy-mm-dd hh:mm:ss.
10. Click Save.

11. Restart PHINMS.

9.13 Secondary Poller Decryption Certificate

Similar to receiver decryption certificate PHINMS contains an option to configure a secondary key store for decrypting polled files. This feature is an enhancement for Route not Read (RnR) pollers. This option is used when there are two valid certificates, a new certificate (primary) and an old/expiring certificate (secondary). If a sender sends an encrypted file, it is possible that the file will be encrypted with a certificate that has not expired.

The primary and secondary key store locations will allow the poller to configure both new and old certificates. If a file is sent to the RnR hub encrypted with the new certificate, it will decrypt; if it is encrypted with the old certificate, it will still decrypt until the expiration date is reached.

1. Open the PHINMS Console.
2. Open the Configure dropdown from the main menu.
3. Select Sender>General.
4. Select Security Category.
5. In the Primary Key Store location, enter the path to the new decryption key.
6. Enter the password for the new decryption key.
7. In the Secondary Key Store location, enter the path to the older decryption key.
8. Enter the password.
9. Enter the date the old decryption key expires, in the format yyyy-mm-dd hh:mm:ss.
10. Click Save.
11. Restart PHINMS.

9.14 Message Signing/Verifying Functionality

For added security since version 3.2 PHINMS includes a nonrepudiation feature. Users have an option to sign their message/payload before sending to the receiver. This allows verification of the sender's identity upon receipt of data. Message signing can be enabled by checking the box in Security Options.