Implementation Guide

Public Health Information Network Messaging System (PHINMS)

Version: 2.7.00 SP1

Prepared by:
U.S. Department of Health & Human Services

Date: November 8, 2007

EXECUTIVE SUMMARY

Public health involves many organizations throughout the PHIN (Public Health Information Network), working together to protect and advance the public's health. These organizations need to use the Internet to securely exchange sensitive data between varieties of different public health information systems. The exchange of data, also known as "messaging" is enabled through messages created using special file formats and a standard vocabulary. The exchange uses a common approach to security and encryption, methods for dealing with a variety of firewalls, and Internet protection schemes. The system provides a standard way for addressing and routing content, a standard and consistent way for information systems to confirm an exchange.

The PHINMS (Public Health Information Network Messaging System) is the software which makes this work. The system securely sends and receives sensitive data over the Internet to the public health information systems using Electronic Business Extensible Markup Language (ebxml) technology.

The PHINMS Implementation Guide provides instructions for installing and configuring the PHINMS 2.7.00 SP1 software.

REVISION HISTORY

VERSION #	IMPLEMENTER	DATE	EXPLANATION
1.0	Michele Bowman	03/01/06	Created version 1.0.0.
2.6.00	Rajeev Seenappa	08/01/06	Provided input to version 2.6.0.
2.6.00	Travis Mayo	08/01/06	Provided input to version 2.6.0.
2.6.00	Wendy Fama	08/11/06	Updated version 2.6.0.
2.7.00	Wendy Fama	11/13/06	Updated to match Release 2.7.00.
2.7.00 SP1	Travis Mayo	03/15/07	Documented 2.7.00 SP1 changes.
2.7.00 SP1	Wendy Fama	03/21/07	Documented 2.7.00 SP1 changes.
2.7.00 SP1	Wendy Fama	04/25/07	Added Port tables.
2.7.00 SP1	Wendy Fama	11/08/07	Updated Digitial Certificate request procedures.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYM LIST

AH	Authentication Header
CDC	Centers for Disease Control and Prevention
CPA	Collaboration Protocol Agreement
CPS	Certification Practice Statement
DMZ	De-Militarized Zone
ebxml	Electronic Business Extensible Markup Language
ESP	Encapsulating Security Protocol
FAQs	Frequently Asked Questions
FTP	File Transfer Protocol
ISAKMP	Internet Security Association and Key Management Protocol
JDBC	Java Database Connectivity
LDAP	Lightweight Directory Access Protocol
PC	Personal Computer
PartyID	Party Identifier
PHIN	Public Health Information Network
PHINMS	Public Health Information Network Messaging System
PHINMSG	Public Health Information Network Messaging
RDBMS	Relational Database Management System
SP	Service Pack
SDN	Secure Data Network
SQL	Structured Query Language
SSL	Secure Socket Layer
TCP	
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 will assist with the installation, configuration, and upgrade of the software. Documentation is continually updated. Ensure the most recent versions are referenced from the PHINMS website at www.cdc.gov/phin/phinms.

The PHINMS Implementation Guide focuses on using PHINMS to send/receive messages from the CDC. When PHINMS is used to send/receive messages from other organizations, then some of the CDC-specific information may not apply (like how to obtain a Digital certificate and PartyID from the CDC).

1.1 PHINMS Topics

- **Quick Tips:** A streamlined list and details used to install and run the PHINMS software. Navigate to the PHINMS website, click the PHINMS Installation link, and then click on the Quick Tips link. The steps are listed in order and should be reviewed prior to using the other topics.
- **Release Notes:** The Release Notes corresponds with the version of software being installed. Proceed to the Release Notes and Installation Guide on the PHINMS website, click the PHINMS Support link, and then click on the Release Notes and Installation Guide link.
- **Implementation Guide:** The Implementation Guide is continually updated. Ensure the latest copy is referenced by retrieving it from the PHINMS website; click the PHINMS Support link, Release Notes, and Installation Guides link.
- **Online Help:** The PHINMS online help along with the Implementation Guide provides screen shots and step-by-step instructions for configuring and using the PHINMS software. Navigate to PHINMS website, click the PHINMS Support link, and click on the PHINMS Software Online Help link. The online help launches in a new browser. The Contents navigation provides procedures needed.
- **FAQs:** The list of Frequently Asked Questions (FAQs) stored on the PHINMS website answers many questions users have previously submitted. The PHINMS Team welcomes questions, suggestions, and/or comments.

Note: Additional information on all Sections within the PHINMS Implementation Guide can be found on the PHINMS website. The interactive, multimedia online help offers a convenient step-by-step instructions, vivid graphics, and screen captures to speed the training time. Detailed information about PHINMS can be located on the web site in the PHINMS Technical Reference Guide.

1.2 Communiqués

The PHINMS team responds to user’s communiqués. Send questions, suggestions, and/or comments concerning PHINMS support or documentation to the PHINMS website using the Contact PHINMS email link located at the top of the home page.

2.0 INSTALLATION

The installation of PHINMS 2.7.00 SP1 requires the following:

- a Java application server used for all three web-based PHINMS components, the Sender, Receiver, and Console,
- one of the following operating systems:
  - Windows 2000,
  - Windows XP,
  - Windows 2003,
  - Linux Red Hat 8.0 or above,
  - or Solaris 8 or above,
- 250M of disk space,
- 512M of memory, and
- local administrator privileges.

Ensure all the correct ports, which may be 5088, 443, and 389 are open on the local host and on the firewall.

Once the requirements above have been met, proceed to Section 2.1. Section 2.1 and Section 2.2 can be accomplished simultaneously.

2.1 Request PartyID

A Party Identifier (PartyID) is required for each organization and every organization sending and receiving messages. A PartyID uniquely identifies a PHINMS installation, also called an instance or node. The PartyID is included with every message informing the recipient of the originator.

Complete the PHINMS software request located at http://www.cdc.gov/phin/software-solutions/phinms/how.html#h-12.2. Information is required about the organization(s) sending and receiving messages. When complete, the Public Health Information Network (PHIN) Deployment Team will email the PartyID to the requestor. Contact the PHIN Help Desk regarding any issues encountered with the PartyID, by sending an email to PHINTech@cdc.gov or calling 1-800-532-9929, option 2.

Setting up the PHINMS software requires the PartyID which is permanent and not required to be stored for later use. The PartyID is stored as long as the PHINMS instance for sending messages to partners is being used by the PHINMS application.

Note: When a need to install PHINMS at more than one site or to install more than one PHINMS installation at the same site, a PartyID is required for each installation. This is not the case with DPIT where only one instance will be sending to the CDC at a time, but two instances are installed during deployment.

The recommended way to install PHINMS 2.7.00 SP1 is to download the application from the File Transport Site (FTP) site. An install disk may be requested from the PHINMS Deployment Team if problems are encountered with the download.

2.2 Request Digital Certificate

This section applies to request a new and a renewal of Digital Certificates. Administrative privileges are required on the personal computer (PC) before applying for the Digital Certificate. Determine administrative privileges for Windows XP or greater by completing the following steps:

1. select Start > Settings> Control Panel > Administrative Tools > Computer Management,
2. expand Local Users and Groups, select Groups,
3. open Administrators, and
4. verify the **user ID** appears in the Members panel under the General tab.

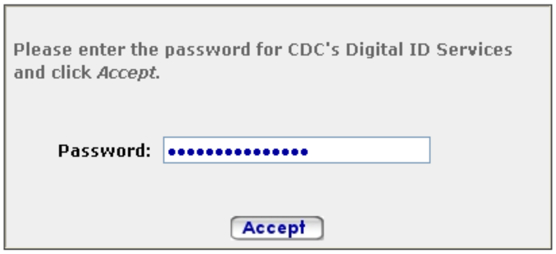
Contact IT Support to provide privileges if the user ID does not appear. Centers for Disease Control and Prevention (CDC) users should contact IT Support at http://itsoservicedesk to request a resource account using the Elevated Privileges link.

The following system requirements must be met before downloading the Digital Certificate:

- Intel-based system with a Pentium 4 CPU or greater,
- Windows XP or greater,
- internet connectivity,
- Internet Explorer 6.x, Netscape Communicator 7.x, or greater, and
- browser cipher strength - 128 bit or greater.

Note: Contact the PHIN helpdesk at 1-800-532-9929, to obtain a password. When requesting a Digital Certificate, complete the following steps:

5. navigate to http://ca.cdc.gov displaying Figure 2.1,



Please enter the password for CDC's Digital ID Services and click *Accept*.

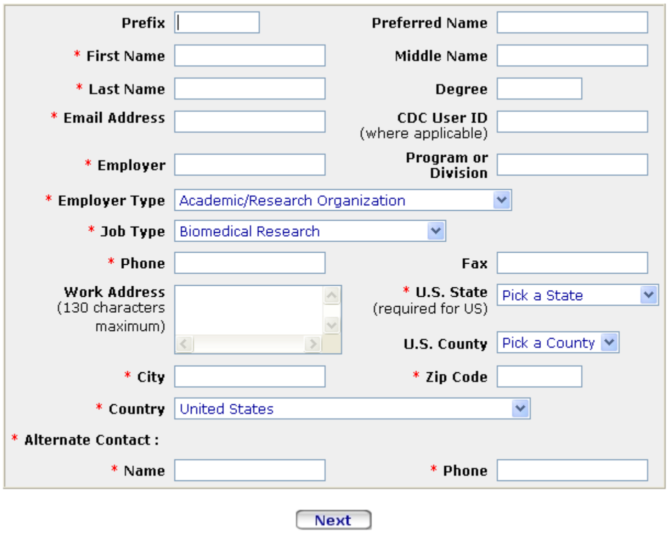
Password: •••••••••••••••

Figure 2.1. Enrollment Password

6. enter the **enrollment password**, click **Accept**, displaying system requirements and Digital Certificate background information,

Note: Complete terms for the VeriSign Certified Practice Statement (CPS) can be found by selecting the “here” link.

7. click **Enroll** located at the bottom of the screen displaying Figure 2.2,



* Employer Type: Academic/Research Organization

* Job Type: Biomedical Research

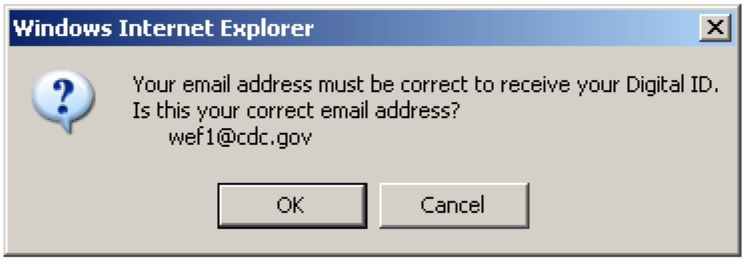
* U.S. State (required for US): Pick a State

U.S. County: Pick a County

* Country: United States

Figure 2.2. Personal Information

8. complete the **required fields** (*), click **Next** displaying Figure 2.3,

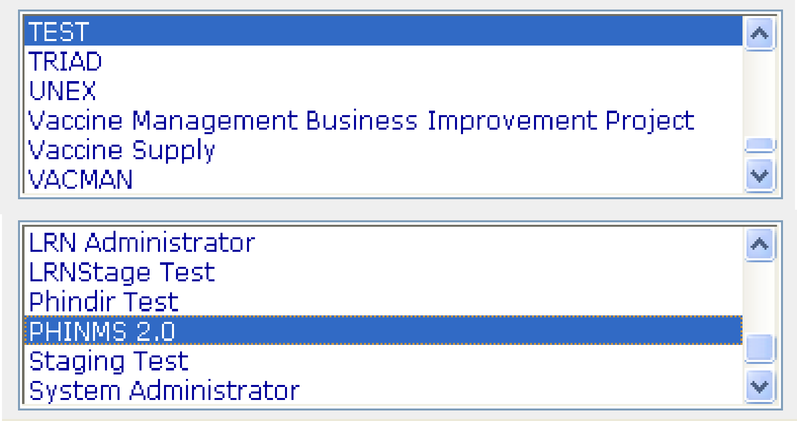


Windows Internet Explorer

Your email address must be correct to receive your Digital ID.
Is this your correct email address?
wef1@cdc.gov

Figure 2.3. Email Verification

9. verify the email address is correct, click **OK** displaying Figure 2.4 if correct and **Cancel** returning to Figure 2.2 allowing the email address to be corrected,

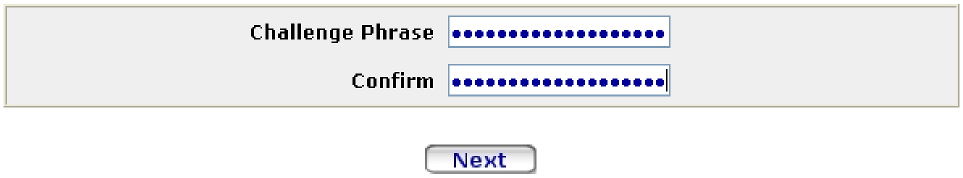


TEST
TRIAD
UNEX
Vaccine Management Business Improvement Project
Vaccine Supply
VACMAN

LRN Administrator
LRNStage Test
Phindir Test
PHINMS 2.0
Staging Test
System Administrator

Figure 2.4. Select a Program and Activities

10. select **Test** to gain access to the staging environment, displaying the notice "Downloading Activities…Please Wait". When the download is complete a list of TEST activities will be displayed, select **PHINMS 2.0** (linked to the current version of PHINMS), click **Next** displaying Figure 2.5, and



Challenge Phrase ●●●●●●●●●●●●●●●●●●

Confirm ●●●●●●●●●●●●●●●●●●

Figure 2.5. Digital ID Certificate Challenge Phrase

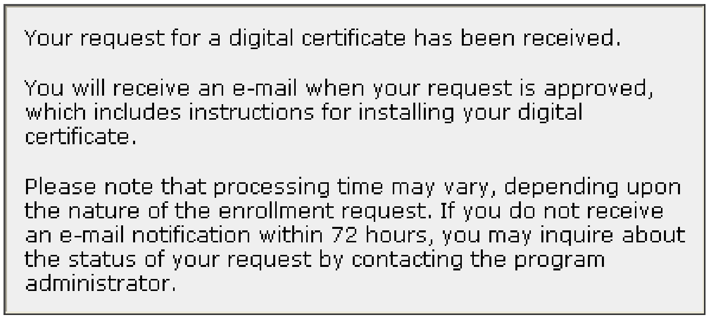
11. enter a **challenge phrase** (guidelines below), click **Next** displaying Figure 2.6.

Note: The SDN environment will indicate special characters are required in the challenge phrase during the enrollment process. The PHINMS software requires the user to refrain from using special characters in the challenge phrase.

Create the challenge phrase using the following guidelines:

- contains at least eight (8) characters in length,
- contains only English letters and numbers,
- contains at least four (4) different numbers or letters,
- can not contain any part of the user name or email address,
- can not spell a word unless the word has three (3) or more numbers or symbols before, after, or within the word,
- can not contain more than two consecutive characters, and
- can not contain special characters such as "+, <, &, @, . (period),etc" which prevents the user access to the software.

Note: The challenge phrase is case-sensitive. Safely store the challenge phrase for security purposes. The challenge phrase is required each time SDN is accessed and is different from the password used to log onto the SDN enrollment site. The challenge phrase along with the Digital Certificate is used to authenticate a SDN user.



Your request for a digital certificate has been received.

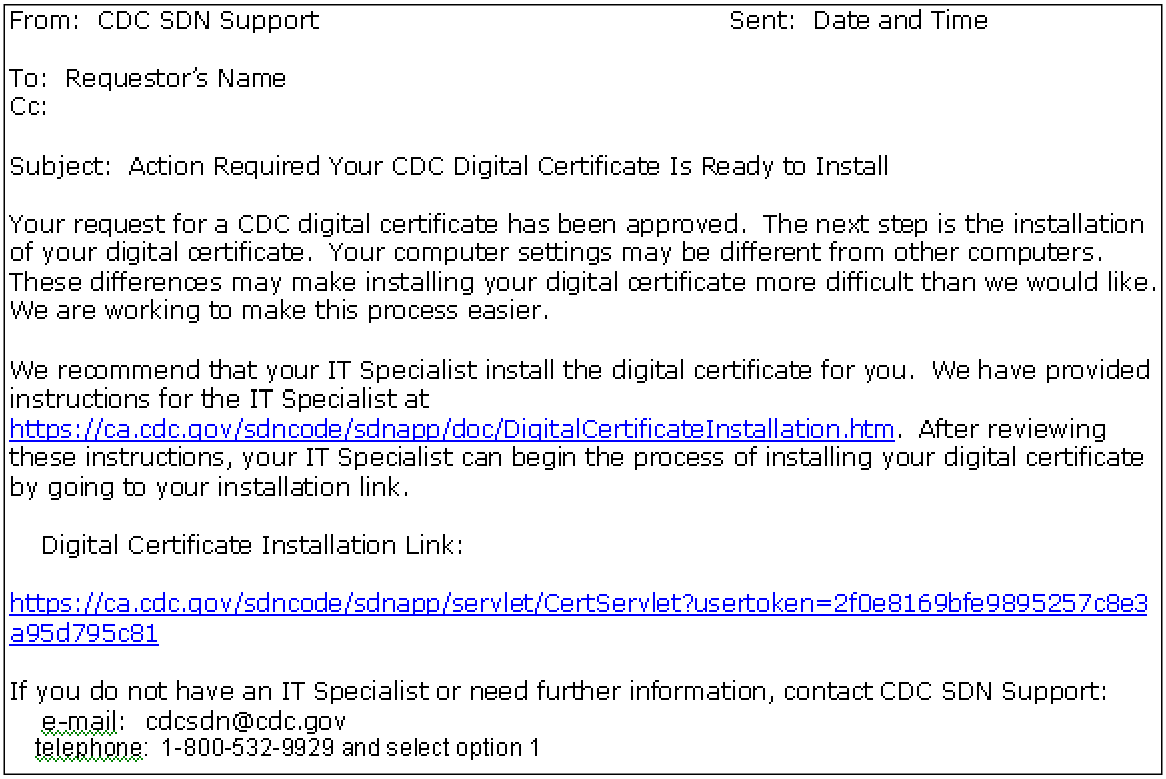
You will receive an e-mail when your request is approved, which includes instructions for installing your digital certificate.

Please note that processing time may vary, depending upon the nature of the enrollment request. If you do not receive an e-mail notification within 72 hours, you may inquire about the status of your request by contacting the program administrator.

Figure 2.6. Digital ID Certificate Request Received

2.2.1 Approved CDC Digital Certificate

Approval notification may take anywhere from 12 to 72 hours via email with instructions similar to those shown in Figure 2.7. Follow the instructions sent in the email before proceeding to Section 2.2.2.



From: CDC SDN Support Sent: Date and Time

To: Requestor's Name
Cc:

Subject: Action Required Your CDC Digital Certificate Is Ready to Install

Your request for a CDC digital certificate has been approved. The next step is the installation of your digital certificate. Your computer settings may be different from other computers. These differences may make installing your digital certificate more difficult than we would like. We are working to make this process easier.

We recommend that your IT Specialist install the digital certificate for you. We have provided instructions for the IT Specialist at https://ca.cdc.gov/sdncode/sdnapp/doc/DigitalCertificateInstallation.htm. After reviewing these instructions, your IT Specialist can begin the process of installing your digital certificate by going to your installation link.

Digital Certificate Installation Link:

https://ca.cdc.gov/sdncode/sdnapp/servlet/CertServlet?usertoken=2f0e8169bfe9895257c8e3a95d795c81

If you do not have an IT Specialist or need further information, contact CDC SDN Support:
e-mail: cdcsdn@cdc.gov
telephone: 1-800-532-9929 and select option 1

Figure 2.7. CDC Digital Certificate Approval Email

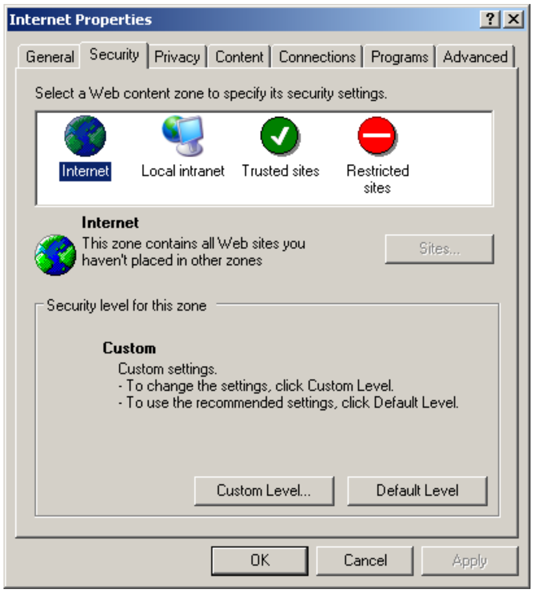
2.2.2 Download Digital Certificate

In order for a successful download of the Digital Certificate insure the following:

- Active X is enabled on the Internet settings,
- all “Pop-Up blockers are turned off, including blockers similar to Yahoo or Google,
- enable Transport Layer Security (TLS) 1.0, and
- the user downloading the Digital Certificate has administrative rights.

Complete the following steps before proceeding to download the Digital Certificate,

12. open **Browser**, select **Tools**, **Internet Options** displaying Figure 2.8,



Select a Web content zone to specify its security settings.

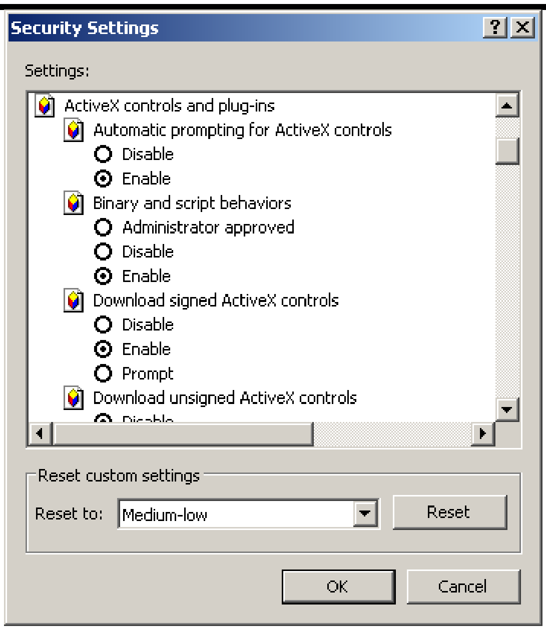
Internet
This zone contains all Web sites you haven't placed in other zones

Security level for this zone

Custom
Custom settings.
- To change the settings, click Custom Level.
- To use the recommended settings, click Default Level.

Figure 2.8. Internet Options

13. select the **Security** tab, click **Custom Level**, displaying Figure 2.9,



Settings:

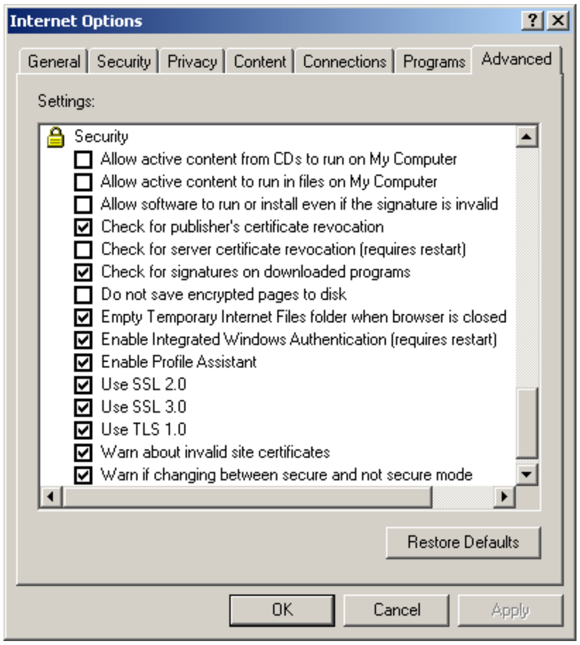
- ActiveX controls and plug-ins
  - Automatic prompting for ActiveX controls
    - ○ Disable
    - ● Enable
  - Binary and script behaviors
    - ○ Administrator approved
    - ○ Disable
    - ● Enable
  - Download signed ActiveX controls
    - ○ Disable
    - ● Enable
    - ○ Prompt
  - Download unsigned ActiveX controls

Reset custom settings

Reset to: Medium-low

Figure 2.9. Security Settings

14. expand **ActiveX controls** and **plug-ins**, select **Enable** under Automatic prompting for ActiveX controls, select **Enable** under Download signed ActiveX controls, click **OK**, returning to the Browser, select the **Advanced** tab, displaying Figure 2.10, and



Settings:

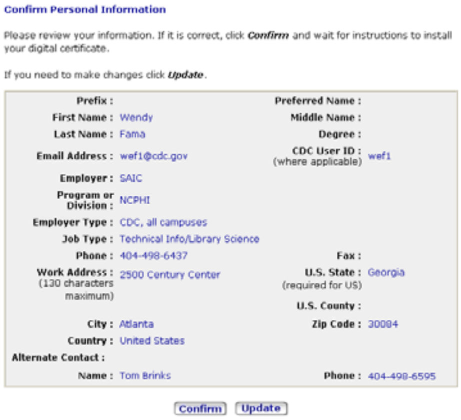
- Security
  - □ Allow active content from CDs to run on My Computer
  - □ Allow active content to run in files on My Computer
  - □ Allow software to run or install even if the signature is invalid
  - ☑ Check for publisher's certificate revocation
  - □ Check for server certificate revocation (requires restart)
  - ☑ Check for signatures on downloaded programs
  - □ Do not save encrypted pages to disk
  - ☑ Empty Temporary Internet Files folder when browser is closed
  - ☑ Enable Integrated Windows Authentication (requires restart)
  - ☑ Enable Profile Assistant
  - ☑ Use SSL 2.0
  - ☑ Use SSL 3.0
  - ☑ Use TLS 1.0
  - ☑ Warn about invalid site certificates
  - ☑ Warn if changing between secure and not secure mode

Figure 2.10. Advanced Internet Options

15. scroll down to Security, select **Use TLS 1.0**, click **Apply**, click **OK**, returning to the Browser, select **Tools**, **Pop-up Blocker**, **Turn Off Pop-up Blocker**.

When the Digital Certificate approved has been given, complete the following steps:

16. navigate to the link provided in the email displaying Figure 2.11,



Confirm Personal Information

Please review your information. If it is correct, click ***Confirm*** and wait for instructions to install your digital certificate.

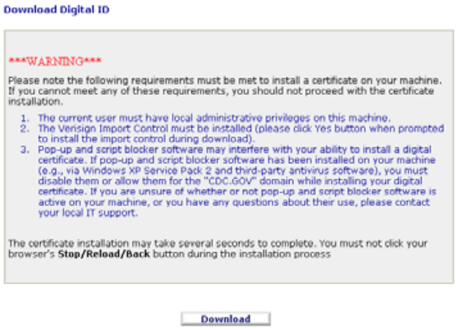
If you need to make changes click ***Update***.

Prefix :		**Preferred Name :**	
First Name :	Wendy	**Middle Name :**	
Last Name :	Fama	**Degree :**	
Email Address :	wef1@cdc.gov	**CDC User ID :** (where applicable)	wef1
Employer :	SAIC		
Program or Division :	NCPHI		
Employer Type :	CDC, all campuses		
Job Type :	Technical Info/Library Science		
Phone :	404-498-6437	**Fax :**	
Work Address : (130 characters maximum)	2500 Century Center	**U.S. State :** (required for US)	Georgia
		U.S. County :	
City :	Atlanta	**Zip Code :**	30084
Country :	United States		
Alternate Contact :			
Name :	Tom Brinks	**Phone :**	404-498-6595

Figure 2.11. Confirm Personal Information

17. confirm personal information is correct. If correct, click **Confirm**, if not click **Update** displaying Figure 2.12,

Note: When the Personal Information is changed, the Digital Certificate download will not be able to be accomplished. Another approval email will be sent which will allow for a successful download of the Digital Certificate.



Download Digital ID

WARNING

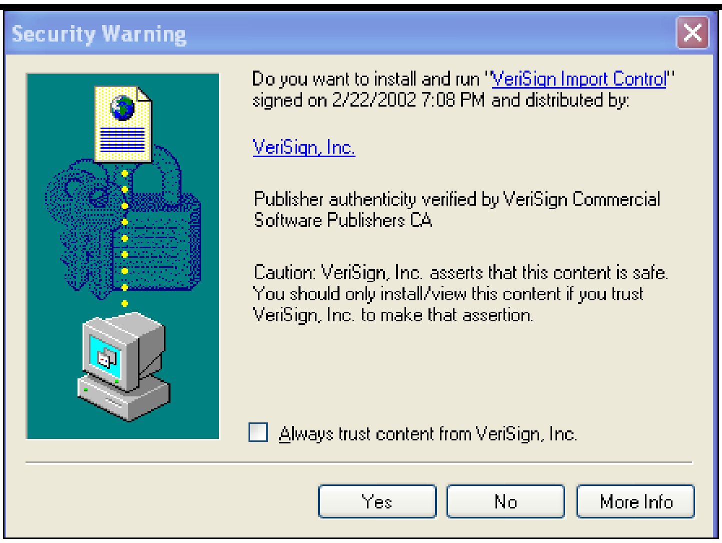
Please note the following requirements must be met to install a certificate on your machine. If you cannot meet any of these requirements, you should not proceed with the certificate installation.

1. The current user must have local administrative privileges on this machine.
2. The Verisign Import Control must be installed (please click Yes button when prompted to install the import control during download).
3. Pop-up and script blocker software may interfere with your ability to install a digital certificate. If pop-up and script blocker software has been installed on your machine (e.g., via Windows XP Service Pack 2 and third-party antivirus software), you must disable them or allow them for the "CDC.GOV" domain while installing your digital certificate. If you are unsure of whether or not pop-up and script blocker software is active on your machine, or you have any questions about their use, please contact your local IT support.

The certificate installation may take several seconds to complete. You must not click your browser's **Stop/Reload/Back** button during the installation process

Figure 2.12. Download Digital ID

18. click **Download** displaying Figure 2.13,



Security Warning

Do you want to install and run "VeriSign Import Control" signed on 2/22/2002 7:08 PM and distributed by:

VeriSign, Inc.

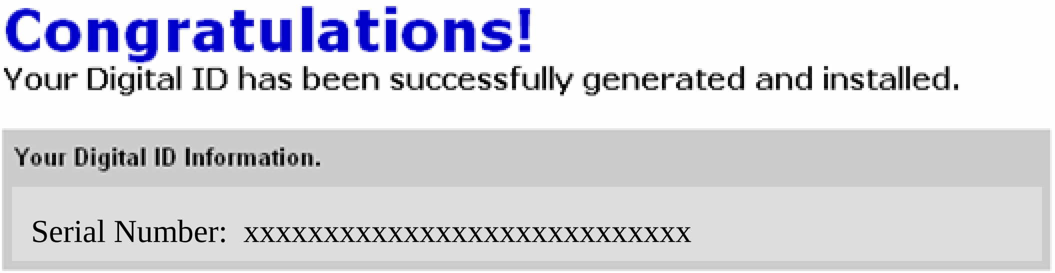
Publisher authenticity verified by VeriSign Commercial Software Publishers CA

Caution: VeriSign, Inc. asserts that this content is safe. You should only install/view this content if you trust VeriSign, Inc. to make that assertion.

□ Always trust content from VeriSign, Inc.

Figure 2.13. Security Warning

19. click **Yes** displaying Figure 2.14, and



Congratulations!

Your Digital ID has been successfully generated and installed.

Your Digital ID Information.

Serial Number: xxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Figure 2.14. Successful Digital ID Download

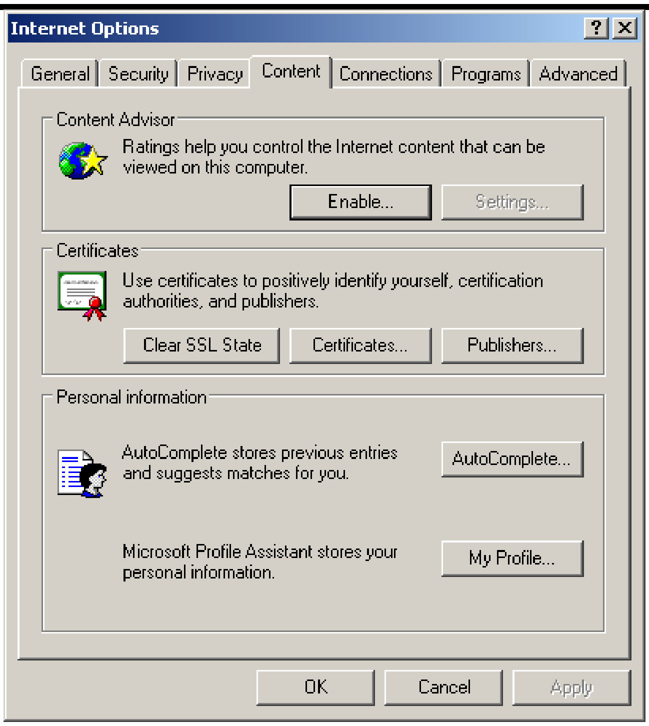
20. proceed to Section 2.3.

2.3 Backup Digital Certification

PHINMS uses the exported Digital Certificate. Digital Certificates are paid with federal tax dollars. Minimize the cost of replacing certificates by creating a copy of the Digital Certificate also referred to as backing up or exporting.

Open an Internet Explorer browser and complete the following:

1. select Internet Explorer Browser,
2. select **Tools**, **Internet Options**, **Content** tab displaying Figure 2.15,



Ratings help you control the Internet content that can be viewed on this computer.

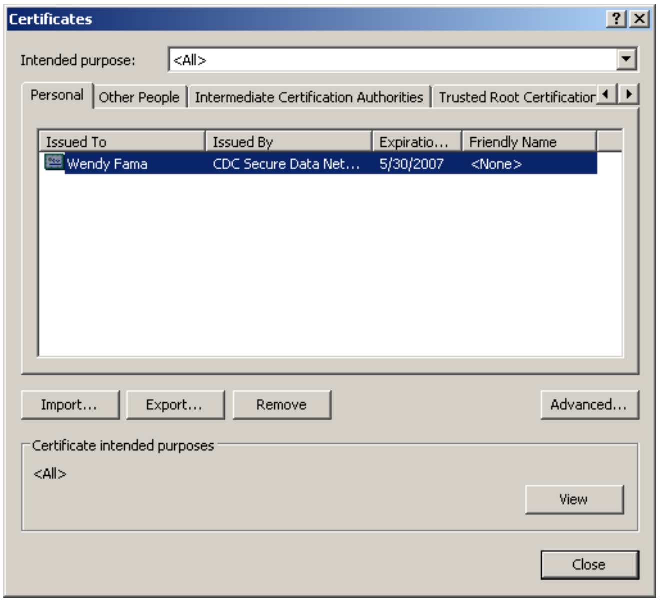
Use certificates to positively identify yourself, certification authorities, and publishers.

AutoComplete stores previous entries and suggests matches for you.

Microsoft Profile Assistant stores your personal information.

Figure 2.15. Internet Options

3. click **Certificates** displaying Figure 2.16,


Certificates
Personal
Other People
Intermediate Certification Authorities
Trusted Root Certificatior
Import...
Export...
Remove
Advanced...
Certificate intended purposes
View
Close

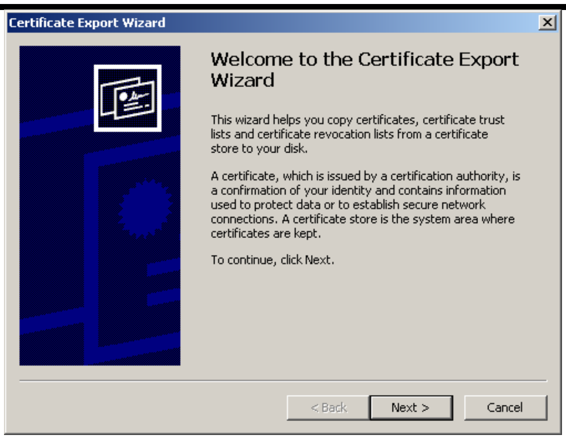
Intended purpose: <All>

Issued To	Issued By	Expiratio...	Friendly Name
Wendy Fama	CDC Secure Data Net...	5/30/2007	<None>

<All>

Figure 2.16. Certificates Dialog Box

4. select the **Certificate** with the appropriate date and issuer, click **Export** displaying Figure 2.17,



Certificate Export Wizard

Welcome to the Certificate Export Wizard

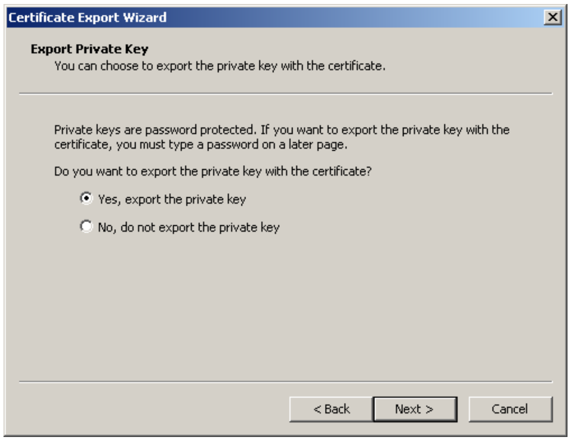
This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

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.

Figure 2.17. Certificate Export Wizard

5. click **Next** displaying Figure 2.18,



Certificate Export Wizard

Export Private Key
You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

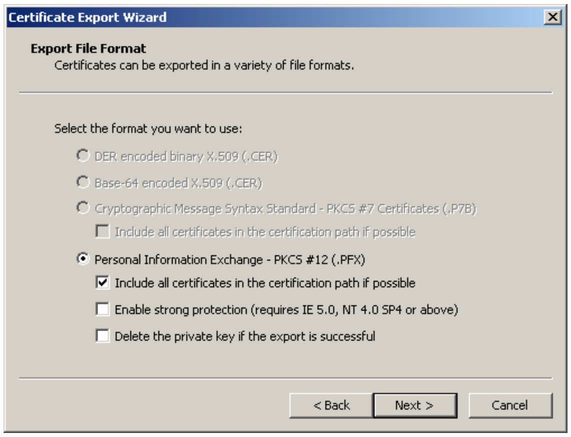
Do you want to export the private key with the certificate?

● Yes, export the private key

○ No, do not export the private key

Figure 2.18. Export Private Key

6. select the **Yes, export the private key**, click **Next** displaying Figure 2.19,



Certificate Export Wizard

Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

● Personal Information Exchange - PKCS #12 (.PFX)

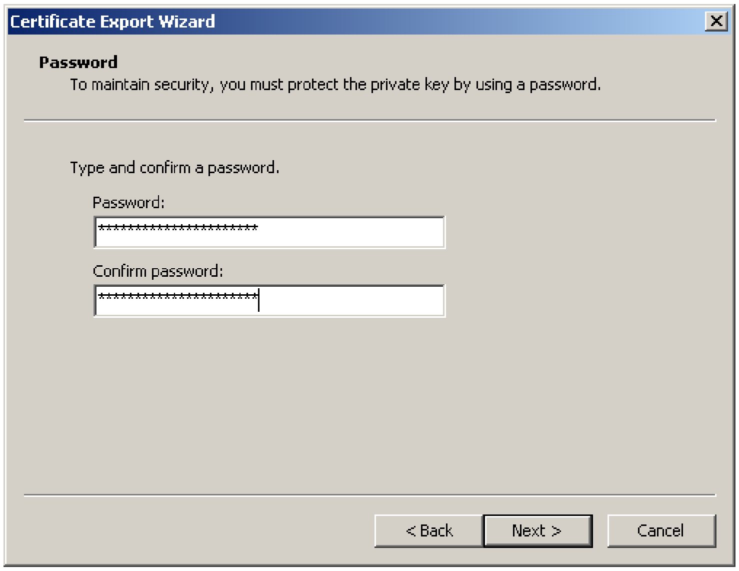
☑ Include all certificates in the certification path if possible

□ Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)

□ Delete the private key if the export is successful

Figure 2.19. Export File Format

7. select Personal Information Exchange - PKCS #12 (.PFX), check Include all certificates in the certification path if possible, uncheck Enable strong protection, uncheck Delete the private key if the export is successful, click Next displaying Figure 2.20,



Certificate Export Wizard

Password
To maintain security, you must protect the private key by using a password.

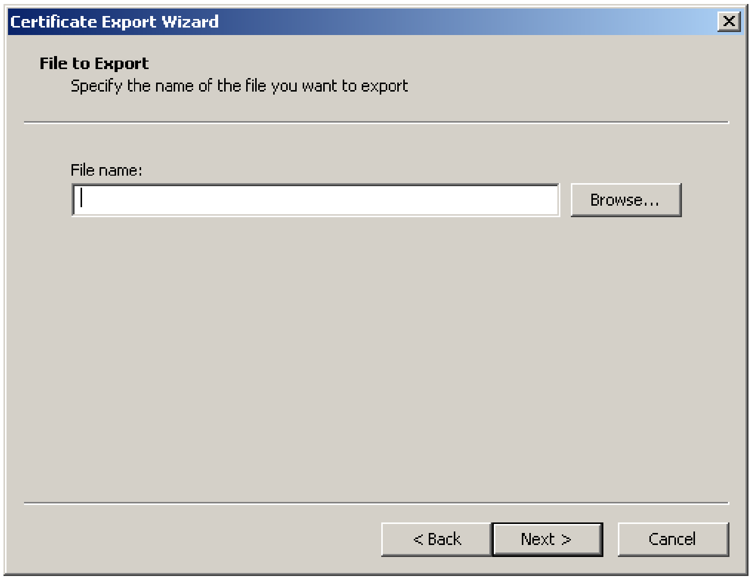
Type and confirm a password.

Password: ***********************

Confirm password: ***********************

Figure 2.20. Password

8. create a **Password**, confirm the **Password** (the challenge phrase used earlier is recommended), safely store the password, click **Next** displaying Figure 2.21,



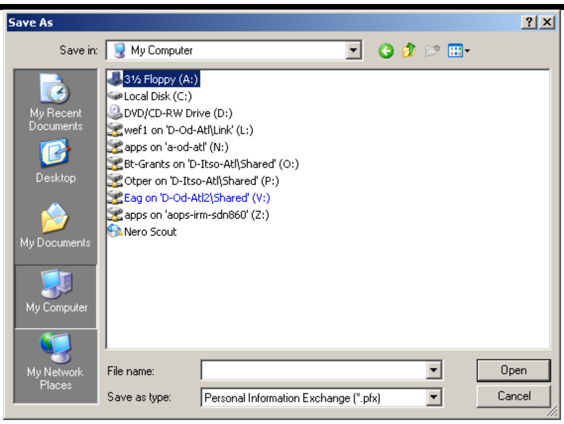
Certificate Export Wizard

File to Export
Specify the name of the file you want to export

File name:

Figure 2.21. File to Export

9. click **Browse** displaying Figure 2.22,



Save in: My Computer

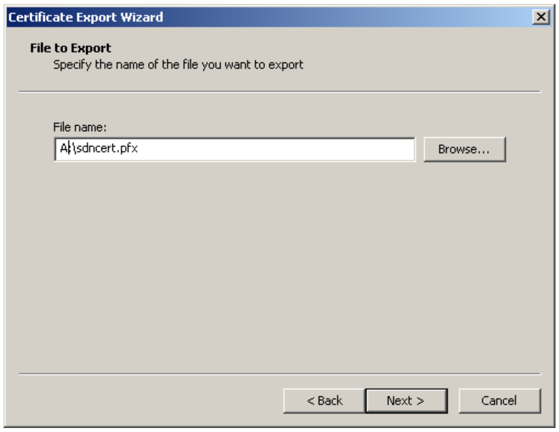
File name:

Save as type: Personal Information Exchange (*.pfx)

Figure 2.22. Save As

10. navigate to a floppy, CD, or shared drive, type **sdncert** in the File name field at the bottom of the Save As dialog box, click **Save** displaying Figure 2.23,

Note: It is not recommended to store a copy of the Digital Certificate on a local drive.



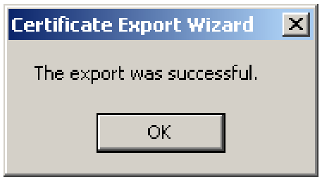
File to Export

Specify the name of the file you want to export

File name: A:\sdncert.pfx

Figure 2.23. Location of Digital Certification

11. the path of the cert is displayed, click **Next**, click **Finish** displaying Figure 2.24, and



The export was successful.

Figure 2.24. Successful Export

12. click OK, Close, OK, exit Browser.

If the Digital Certificate was copied to an external drive, label it SDN Digital Certificate and store it in a safe/secure place, keeping the passwords and the Digital Certificate separate.

2.4 Renew PHINMS Digital Certificates

Refer to Sections 2.2 and 2.3 and complete the request steps to renew a Digital Certificate before it expires.

Current and future PHINMS users with an SDN Digital Certificate will no longer experience forgetting to renew Digital Certificates before they expire and messages not processed by the CDC due to an expired Digital Certificate.

PHINMS users with Digital Certificates will be notified by email at 30 days, 15 days, and 5 days before the expiration date. Users possessing a SDN Digital Certificate but are not a PHINMS user, will not receive email notifications. The emails will contain the following information:

1. the Digital Certificate's expiration date,
2. steps used to register for a new Digital Certificate,
3. a link containing instructions on backing up the previous certificate, and
4. PHIN Help Desk contact information.

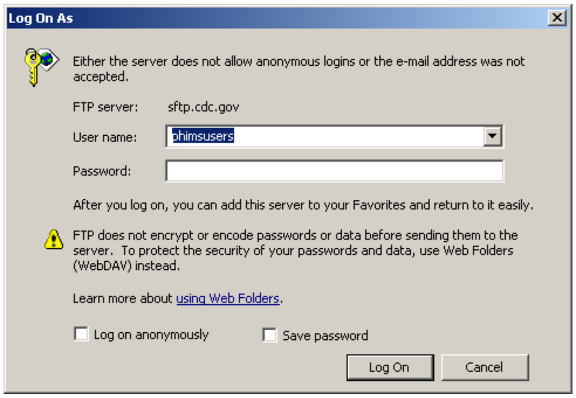
PHINMS Digital Certificates will be disabled on the actual expiration date. This allows time to apply for a new Digital Certificate and continue sending and authenticating messages without disruptions.

3.0 DOWNLOAD PHINMS SOFTWARE

PHINMS Users using PHINMS versions 2.1, 2.5.00, or 2.6.00 SP1 will be required to upgrade to PHINMS 2.7.00 SP1 before upgrading to PHINMS 2.8.00. Refer to the PHINMS 2.7.00 SP1 Implementation guide located on the PHINMS Web Site www.cdc.gov/phin/phinms to upgrade to 2.7.00 SP1. Version 2.7.00 SP1 installation is not necessary for new installs. Install or upgrade to PHINMS 2.8.00 by completing the following the steps below:

Note: A PartyID is required during installation of the PHINMS application. Refer to Section 2.1 if an email was not received with the PartyID information.

1. navigate to FTP site ftp://sftp.cdc.gov displaying Figure 3.1,



Log On As

Either the server does not allow anonymous logins or the e-mail address was not accepted.

FTP server: sftp.cdc.gov

User name: phimsusers

Password:

After you log on, you can add this server to your Favorites and return to it easily.

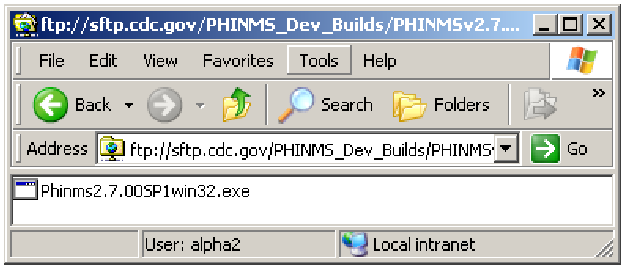
FTP does not encrypt or encode passwords or data before sending them to the server. To protect the security of your passwords and data, use Web Folders (WebDAV) instead.

Learn more about using Web Folders.

☐ Log on anonymously ☐ Save password

Figure 3.1. Log On As

2. enter **User name**, **Password**, click **LogOn**, open the Phinms2.8.00 folder displaying Figure 3.2,



ftp://sftp.cdc.gov/PHINMS_Dev_Builds/PHINMSv2.7....

Address ftp://sftp.cdc.gov/PHINMS_Dev_Builds/PHINMS

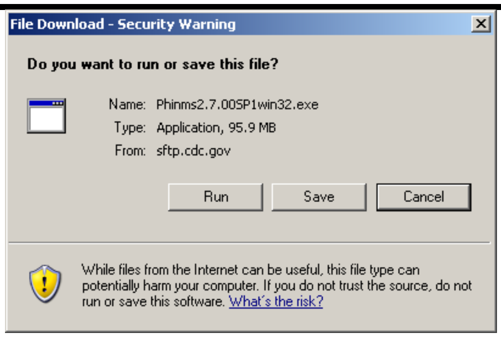
Phinms2.7.00SP1win32.exe

User: alpha2

Local intranet

Figure 3.2. Phinms2.7.0SP1win32.exe

3. double click on **Phinms2.8.00win32.exe** displaying Figure 3.3,



File Download - Security Warning

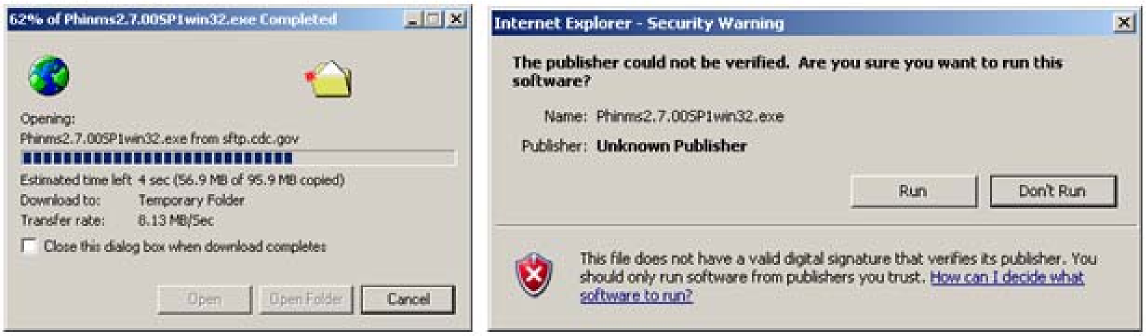
Do you want to run or save this file?

Name: Phinms2.7.00SP1win32.exe
Type: Application, 95.9 MB
From: sftp.cdc.gov

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?

Figure 3.3. File Download - Security Warning

4. click **Run**, Phinms2.8.00win32.exe will download displaying Figure 3.4,



62% of Phinms2.7.00SP1win32.exe Completed

Opening:
Phinms2.7.00SP1win32.exe from sftp.cdc.gov

Estimated time left 4 sec (56.9 MB of 95.9 MB copied)
Download to: Temporary Folder
Transfer rate: 8.13 MB/Sec

□ Close this dialog box when download completes

Internet Explorer - Security Warning

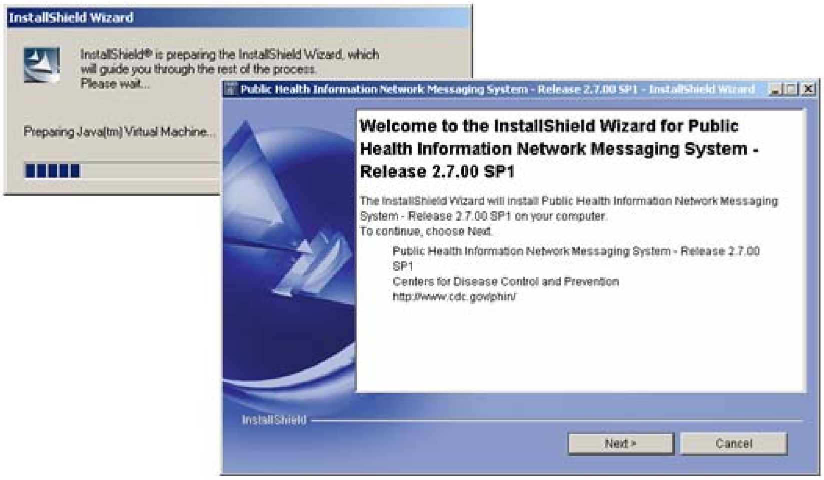
The publisher could not be verified. Are you sure you want to run this software?

Name: Phinms2.7.00SP1win32.exe
Publisher: Unknown Publisher

This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust. How can I decide what software to run?

Figure 3.4. PHINMS 2.8.00 Download and Security - Warning

5. select **Run** the InstallShield screen prepares the InstallShield Wizard (taking a few moments) shown in Figure 3.4,



InstallShield Wizard

InstallShield® is preparing the InstallShield Wizard, which will guide you through the rest of the process. Please wait...

Preparing Java(tm) Virtual Machine...

Public Health Information Network Messaging System - Release 2.7.00 SP1 - InstallShield Wizard

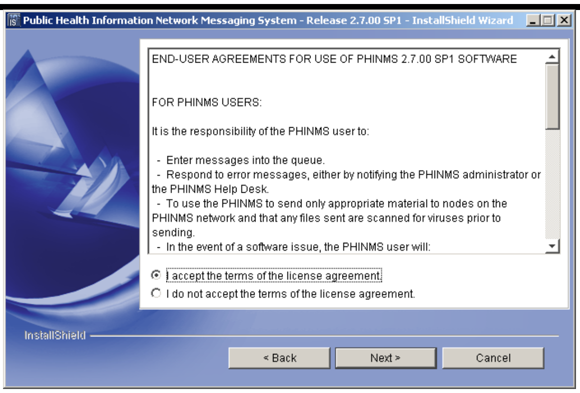
Welcome to the InstallShield Wizard for Public Health Information Network Messaging System - Release 2.7.00 SP1

The InstallShield Wizard will install Public Health Information Network Messaging System - Release 2.7.00 SP1 on your computer.
To continue, choose Next.

Public Health Information Network Messaging System - Release 2.7.00 SP1
Centers for Disease Control and Prevention
http://www.cdc.gov/phin/

Figure 3.5. InstallShield Wizard Preparation

6. select **Next** displaying Figure 3.6,



Public Health Information Network Messaging System - Release 2.7.00 SP1 - InstallShield Wizard

END-USER AGREEMENTS FOR USE OF PHINMS 2.7.00 SP1 SOFTWARE

FOR PHINMS USERS:

It is the responsibility of the PHINMS user to:

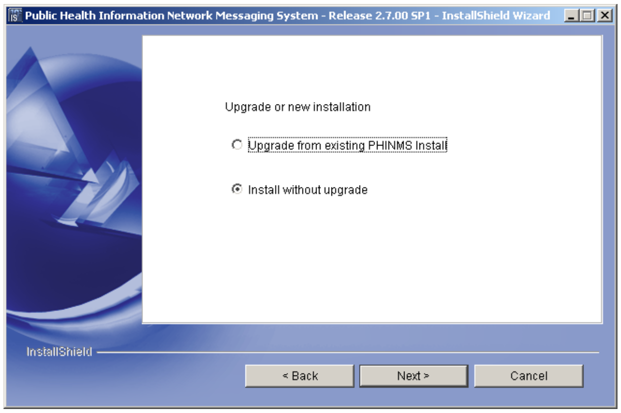
- Enter messages into the queue.
- Respond to error messages, either by notifying the PHINMS administrator or the PHINMS Help Desk.
- To use the PHINMS to send only appropriate material to nodes on the PHINMS network and that any files sent are scanned for viruses prior to sending.
- In the event of a software issue, the PHINMS user will:

● I accept the terms of the license agreement.

○ I do not accept the terms of the license agreement.

Figure 3.6. End User Agreement

7. select **I accept the terms of the license agreement**, click **Next** displaying Figure 3.7,



Public Health Information Network Messaging System - Release 2.7.00 SP1 - InstallShield Wizard

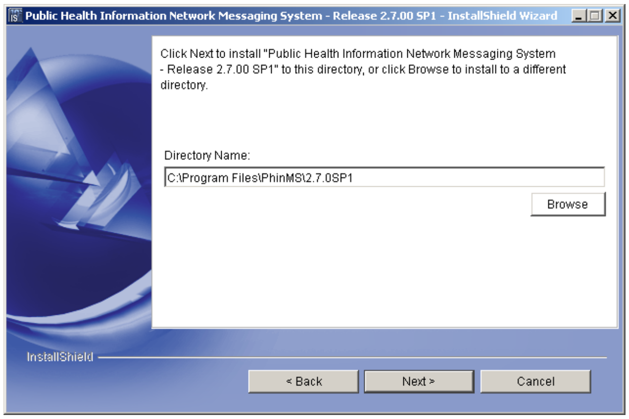
Upgrade or new installation

○ Upgrade from existing PHINMS Install

● Install without upgrade

Figure 3.7. Upgrade or New Installation Screen

8. select **Install without upgrade**, click **Next** displaying Figure 3.8,



Public Health Information Network Messaging System - Release 2.7.00 SP1 - InstallShield Wizard

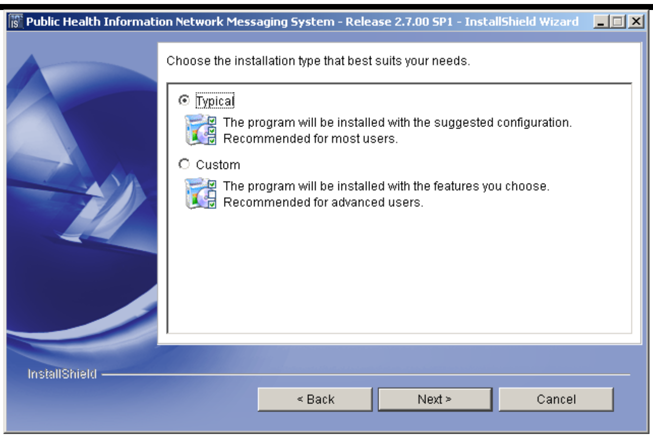
Click Next to install "Public Health Information Network Messaging System - Release 2.7.00 SP1" to this directory, or click Browse to install to a different directory.

Directory Name:

C:\Program Files\PhinMS\2.7.0SP1

Figure 3.8. Directory Name

9. select **Browse** to install a different directory or **Next** displaying Figure 3.9,


Public Health Information Network Messaging System - Release 2.7.00 SP1 - InstallShield Wizard
InstallShield
< Back
Next >
Cancel

Choose the installation type that best suits your needs.

● Typical

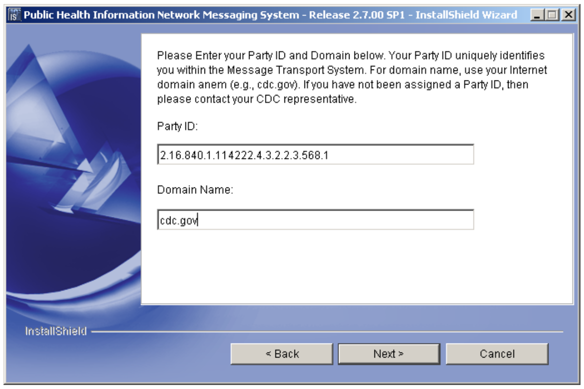
The program will be installed with the suggested configuration. Recommended for most users.

○ Custom

The program will be installed with the features you choose. Recommended for advanced users.

Figure 3.9. Installation Type

10. select **Typical**, click **Next** displaying Figure 3.10,


Public Health Information Network Messaging System - Release 2.7.00 SP1 - InstallShield Wizard
InstallShield
< Back
Next >
Cancel

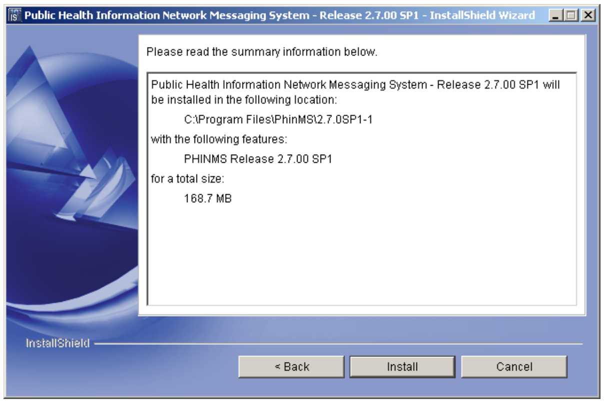
Please Enter your Party ID and Domain below. Your Party ID uniquely identifies you within the Message Transport System. For domain name, use your Internet domain anem (e.g., cdc.gov). If you have not been assigned a Party ID, then please contact your CDC representative.

Party ID: 2.16.840.1.114222.4.3.2.2.3.568.1

Domain Name: cdc.gov

Figure 3.10. PartyID and Domain Name

11. enter the **PartyID**, **Domain Name**, click **Next** displaying Figure 3.11,


Public Health Information Network Messaging System - Release 2.7.00 SP1 - InstallShield Wizard
InstallShield
< Back
Install
Cancel

Please read the summary information below.

Public Health Information Network Messaging System - Release 2.7.00 SP1 will be installed in the following location:

C:\Program Files\PhinMS\2.7.0SP1-1

with the following features:

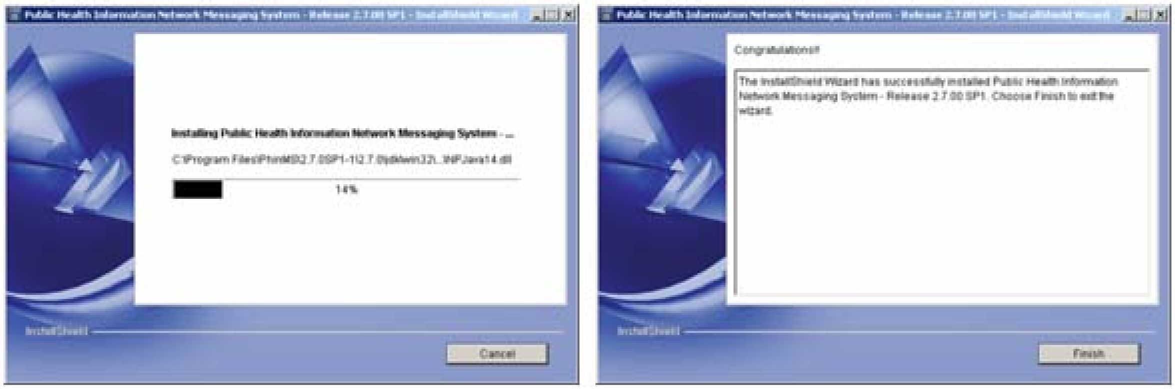
PHINMS Release 2.7.00 SP1

for a total size:

168.7 MB

Figure 3.11. Installation Location

12. click **Install** displaying Figure 3.12,



Public Health Information Network Messaging System - Release 2.7.00 SP1 - InstallShield Wizard

Installing Public Health Information Network Messaging System - ...

C:\Program Files\PhinMS\2.7.0SP1-1\2.7.0\jdk\win32\...\INF\Java14.dll

14%

Congratulations!!

The InstallShield Wizard has successfully installed Public Health Information Network Messaging System - Release 2.7.00 SP1. Choose Finish to exit the wizard.

Figure 3.12. Installing and Congratulations PHINMS

13. click **Finish**, displaying Figure 3.13,

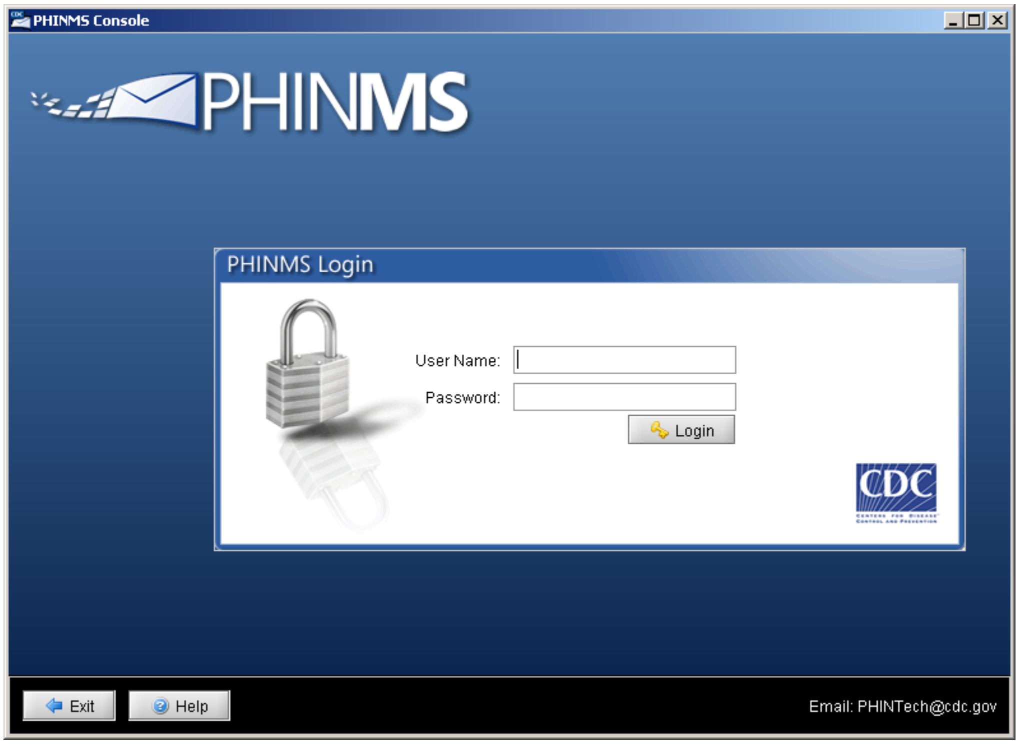
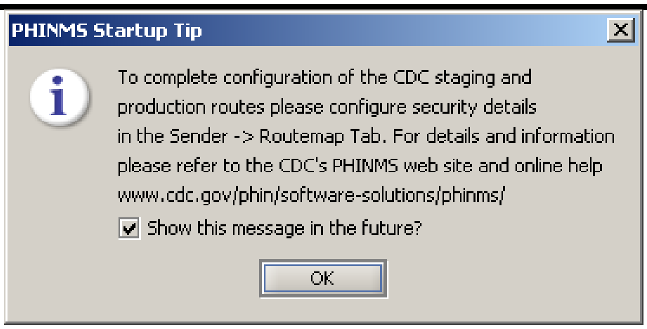


Figure 3.13. PHINMS 2.8.00 Console Login

14. enter **User name**, **Password**, click **Login** displaying Figure 3.14, and



PHINMS Startup Tip

To complete configuration of the CDC staging and production routes please configure security details in the Sender -> Routemap Tab. For details and information please refer to the CDC's PHINMS web site and online help www.cdc.gov/phin/software-solutions/phinms/

☑ Show this message in the future?

Figure 3.14. PHINMS Startup Tip

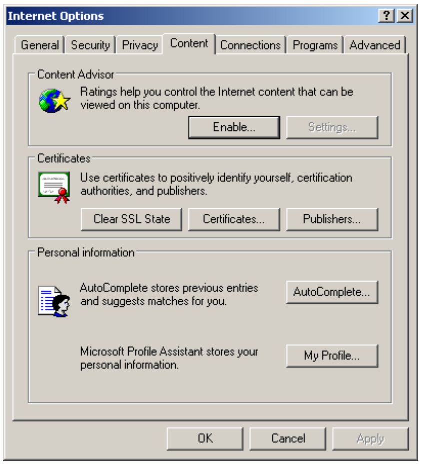
15. click **OK**.

Proceed to 5.0 to configure the PHINMS 2.8.00 Console.

3.1 Export SDN Private Key

Complete the following steps to prepare the .pfx file for Keystore entry when PHINMS 2.8.00 and the Digital ID Certificate have successfully been downloaded:

1. open **Internet Explorer browser**,
2. select **Tools** > **Internet Options** > **Content** displaying Figure 3.15,



Content Advisor

Ratings help you control the Internet content that can be viewed on this computer.

Certificates

Use certificates to positively identify yourself, certification authorities, and publishers.

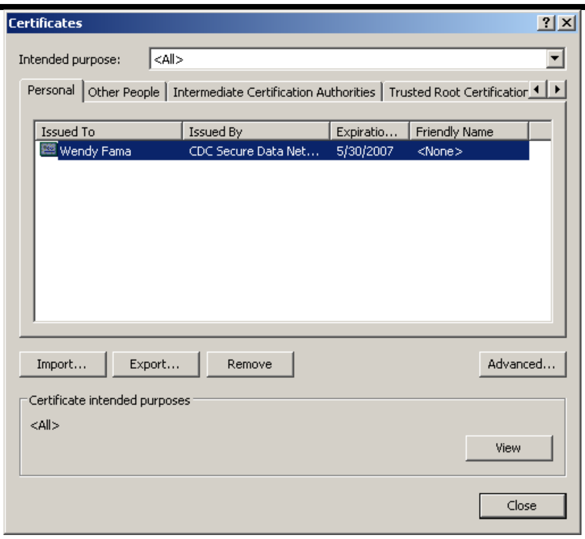
Personal information

AutoComplete stores previous entries and suggests matches for you.

Microsoft Profile Assistant stores your personal information.

Figure 3.15. Internet Options

3. click **Certificates**, displaying the certificates shown in Figure 3.16,



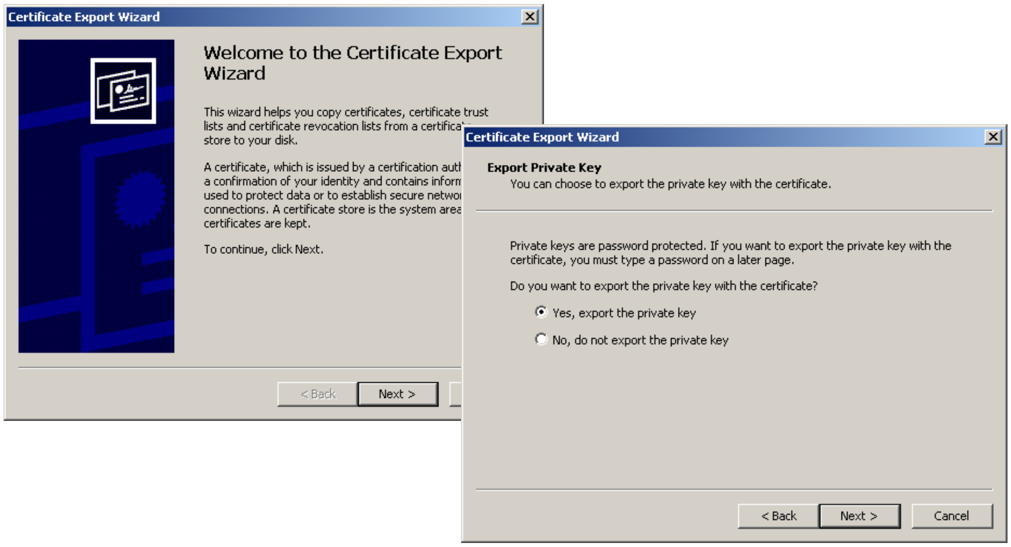
Intended purpose: <All>

Issued To	Issued By	Expiratio...	Friendly Name
Wendy Fama	CDC Secure Data Net...	5/30/2007	<None>

Certificate intended purposes
<All>

Figure 3.16. Certificates

4. select the certificate to export, click **Export** displaying the left screen of Figure 3.17,



Welcome to the Certificate Export Wizard

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

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

To continue, click Next.

Export Private Key
You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

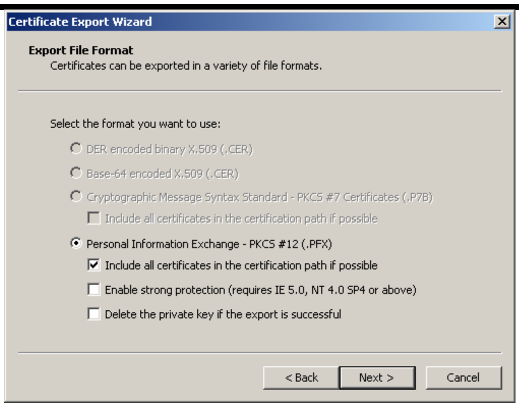
Do you want to export the private key with the certificate?

● Yes, export the private key

○ No, do not export the private key

Figure 3.17. Certificate Export Wizard

5. click **Next**, select **Yes, export the private key**, click **Next** displaying Figure 3.18,



Certificate Export Wizard

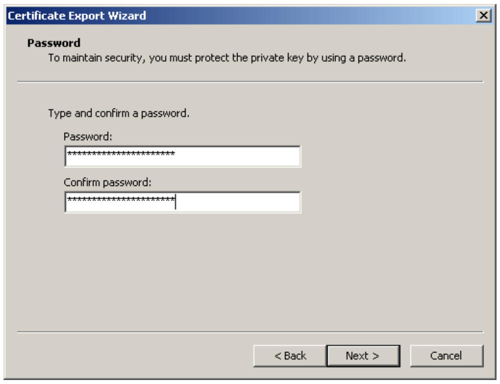
Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)
○ Base-64 encoded X.509 (.CER)
○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
□ Include all certificates in the certification path if possible
● Personal Information Exchange - PKCS #12 (.PFX)
☑ Include all certificates in the certification path if possible
□ Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)
□ Delete the private key if the export is successful

Figure 3.18. Export File Format

6. select **Personal information Exchange**, check **Include all certificates in the certification path if possible**, uncheck **Enable Strong Protection**, uncheck **Delete the private key if the export is successful**, click **Next** displaying Figure 3.19,



Certificate Export Wizard

Password
To maintain security, you must protect the private key by using a password.

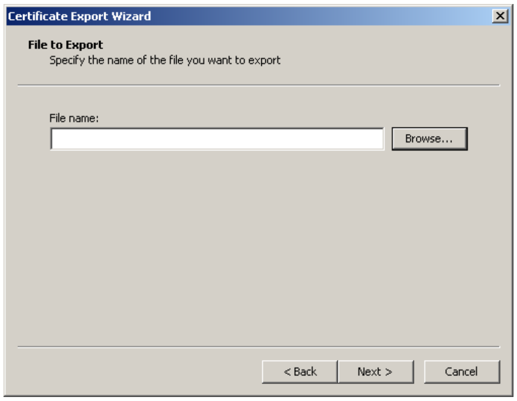
Type and confirm a password.

Password: **********************

Confirm password: **********************

Figure 3.19. Password

7. enter and confirm the **Password** (SDN Challenge Phrase is recommended), click **Next** displaying Figure 3.20,



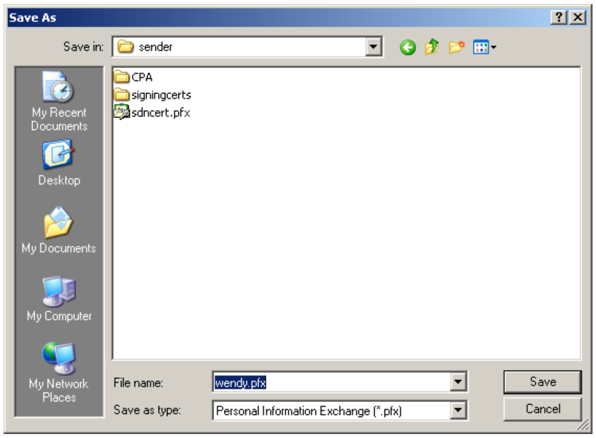
Certificate Export Wizard

File to Export
Specify the name of the file you want to export

File name:

Figure 3.20. File to Export

8. select **Browse** displaying Figure 3.21,



Save in: sender

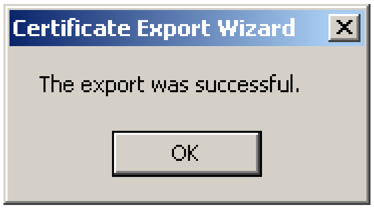
File name: wendy.pfx

Save as type: Personal Information Exchange (*.pfx)

Figure 3.21. Save As

9. navigate to **C:\Program Files\PhinMS\2.8.00\tomcat-5.0.19\phinms\config\**, name the **.pfx file**, click **Save**, displaying the File name on the File to Export screen, click **Next**,

10. click **Finish**, displaying Figure 3.22, and



The export was successful.

Figure 3.22. Export was Successful

11. close **Browser**.

Note: Never send a private key along with the password to another user.

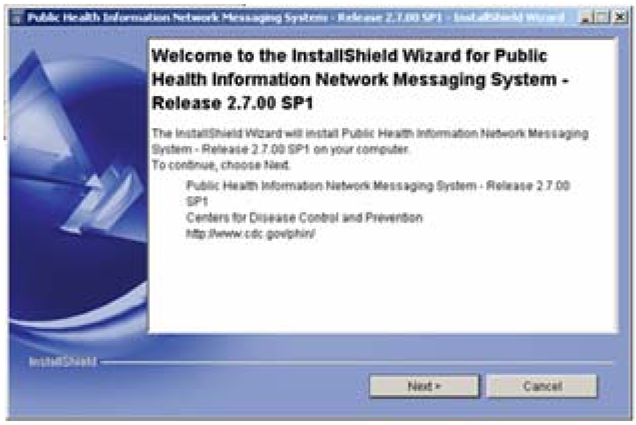
4.0 UPGRADE PHINMS SOFTWARE

PHINMS version 2.7.00 SP1 allows upgrading from the following:

- 2.1 Sender to 2.7.00 SP1 Sender,
- 2.1 Receiver to 2.7.00 SP1 Receiver on Tomcat server,
- 2.5, 2.6, 2.7 to 2.7.00 SP1 on Tomcat server, or
- upgrade pre-2.7.00 Receivers to 2.7.00 SP1 on non-Tomcat application server.

Complete the following steps to upgrade to 2.7.00 SP1:

1. open the executable file **Phinms2.7.00SP1win32.exe** from the 2.7.00 SP1 folder displaying Figure 4.1,



Public Health Information Network Messaging System - Release 2.7.00 SP1 - InstallShield Wizard

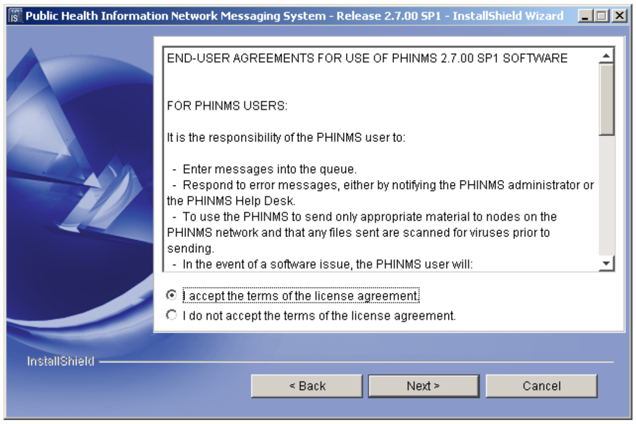
Welcome to the InstallShield Wizard for Public Health Information Network Messaging System - Release 2.7.00 SP1

The InstallShield Wizard will install Public Health Information Network Messaging System - Release 2.7.00 SP1 on your computer.
To continue, choose Next.

Public Health Information Network Messaging System - Release 2.7.00 SP1
Centers for Disease Control and Prevention
http://www.cdc.gov/phin/

Figure 4.1. Upgrade Welcome

2. select **Next** displaying Figure 4.2,



Public Health Information Network Messaging System - Release 2.7.00 SP1 - InstallShield Wizard

END-USER AGREEMENTS FOR USE OF PHINMS 2.7.00 SP1 SOFTWARE

FOR PHINMS USERS:

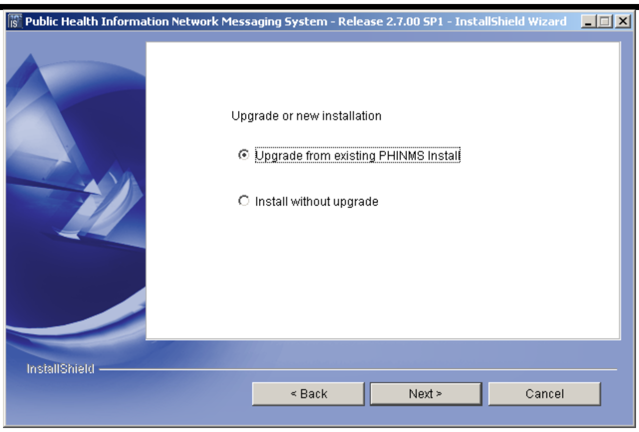
It is the responsibility of the PHINMS user to:

 - Enter messages into the queue.
 - Respond to error messages, either by notifying the PHINMS administrator or the PHINMS Help Desk.
 - To use the PHINMS to send only appropriate material to nodes on the PHINMS network and that any files sent are scanned for viruses prior to sending.
 - In the event of a software issue, the PHINMS user will:

● I accept the terms of the license agreement.
○ I do not accept the terms of the license agreement.

Figure 4.2. End User Agreement

3. select **I accept the terms of the license agreement**, click **Next** displaying Figure 4.3,



Public Health Information Network Messaging System - Release 2.7.00 SP1 - InstallShield Wizard

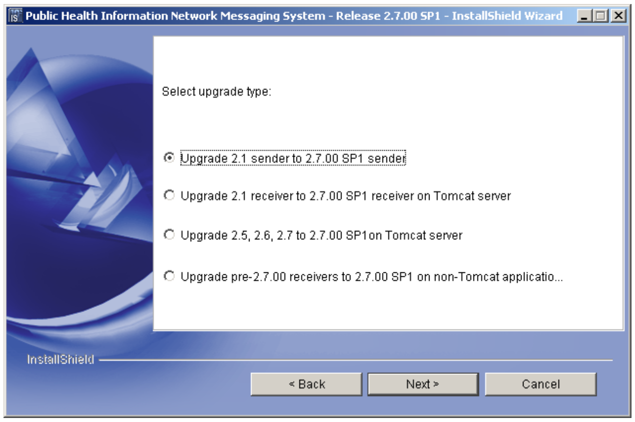
Upgrade or new installation

● Upgrade from existing PHINMS Install

○ Install without upgrade

Figure 4.3. Upgrade or New Installation

4. select **Upgrade from existing PHINMS install**, click **Next** displaying Figure 4.4, and



Public Health Information Network Messaging System - Release 2.7.00 SP1 - InstallShield Wizard

Select upgrade type:

● Upgrade 2.1 sender to 2.7.00 SP1 sender

○ Upgrade 2.1 receiver to 2.7.00 SP1 receiver on Tomcat server

○ Upgrade 2.5, 2.6, 2.7 to 2.7.00 SP1on Tomcat server

○ Upgrade pre-2.7.00 receivers to 2.7.00 SP1 on non-Tomcat applicatio...

Figure 4.4. Upgrade Type

5. select the upgrade type, click **Next**, continue the upgrade by picking up step 9 in Section 3.0.

5.0 CONFIGURE SQL DATABASE

A Microsoft Access database containing a Transport Queue (TransportQ) is automatically installed with the PHINMS 2.7.00 SP1 application. An external database can be created for the purpose of hosting the messaging queue tables. PHINMS 2.7.00 SP1 will support the following databases for hosting messaging queues:

- Microsoft Access,
- Microsoft Structured Query Language (SQL) Server,
- Oracle 9i,
- MySQL 4.1, and
- HSQLDB 1.8.0.

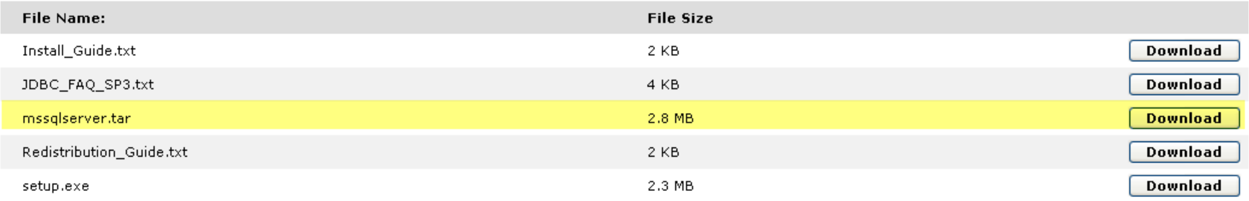
A Microsoft Access database is provided with the PHINMS installation on the Windows platform as a default database and facilitates testing installation. Evaluation of the tradeoffs between Microsoft Access and a high transaction volume Relational Database Management System (RDBMS) such as others listed above is recommended.

This section explains the procedures for creating and configuring a Microsoft SQL database.

5.1 Create SQL Database

Complete the following steps to connect to an external PHINMS SQL database such as Microsoft SQL Server:

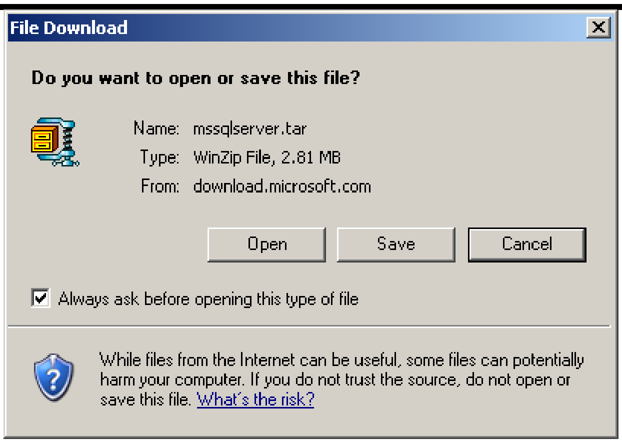
1. navigate to http://www.microsoft.com/downloads/details.aspx?FamilyID=07287b11-0502-461a-b138-2aa54bfdc03a&DisplayLang=en displaying Figure 5.1,



File Name:	File Size	
Install_Guide.txt	2 KB	Download
JDBC_FAQ_SP3.txt	4 KB	Download
mssqlserver.tar	2.8 MB	Download
Redistribution_Guide.txt	2 KB	Download
setup.exe	2.3 MB	Download

Figure 5.1. Download mssqlserver.tar

2. select **mssqlserver.tar download** which are the Java Database Connectivity (JDBC) drivers from Microsoft displaying Figure 5.2,



Do you want to open or save this file?

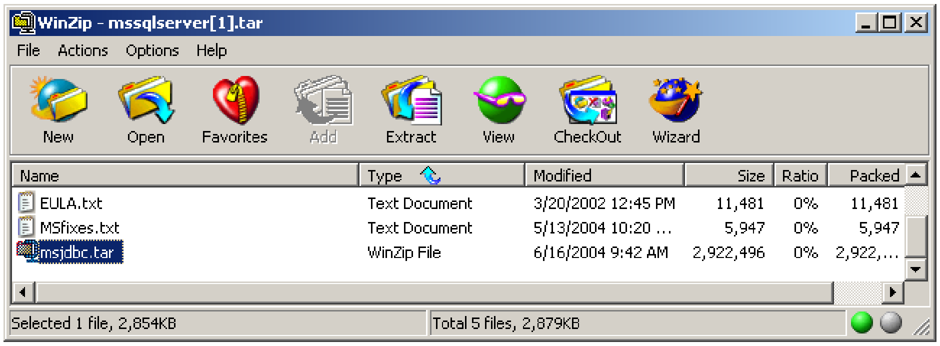
Name: mssqlserver.tar
Type: WinZip File, 2.81 MB
From: download.microsoft.com

☑ Always ask before opening this type of file

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

Figure 5.2. File Download

3. select **Open** displaying Figure 5.3,

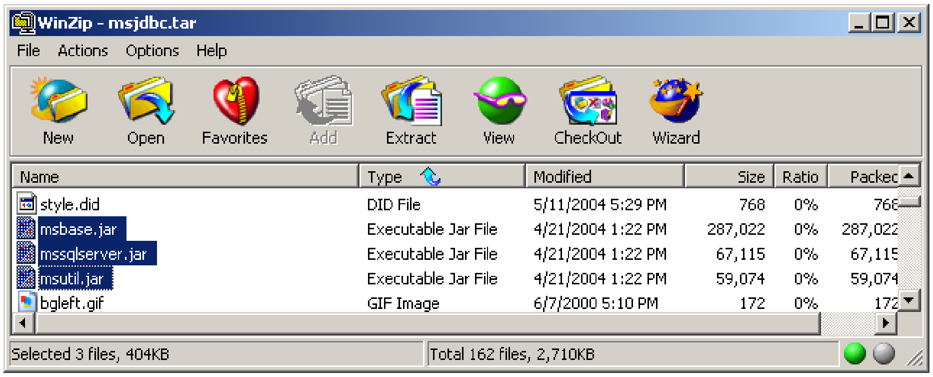


Name	Type	Modified	Size	Ratio	Packed
EULA.txt	Text Document	3/20/2002 12:45 PM	11,481	0%	11,481
MSfixes.txt	Text Document	5/13/2004 10:20 ...	5,947	0%	5,947
msjdbc.tar	WinZip File	6/16/2004 9:42 AM	2,922,496	0%	2,922,...

Selected 1 file, 2,854KB
Total 5 files, 2,879KB

Figure 5.3. Save As

4. double-click **msjdbc.tar** displaying Figure 5.4,

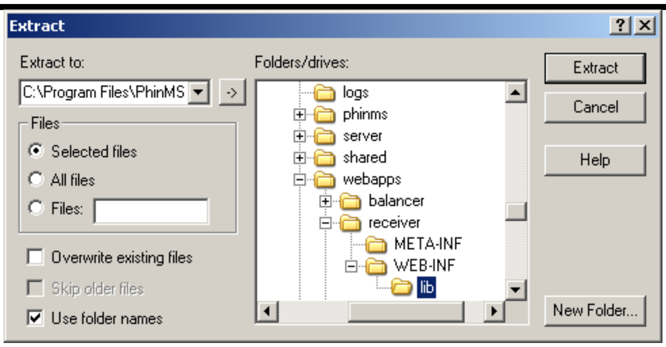


Name	Type	Modified	Size	Ratio	Packec
style.did	DID File	5/11/2004 5:29 PM	768	0%	766
msbase.jar	Executable Jar File	4/21/2004 1:22 PM	287,022	0%	287,022
mssqlserver.jar	Executable Jar File	4/21/2004 1:22 PM	67,115	0%	67,115
msutil.jar	Executable Jar File	4/21/2004 1:22 PM	59,074	0%	59,074
bgleft.gif	GIF Image	6/7/2000 5:10 PM	172	0%	172

Selected 3 files, 404KB
Total 162 files, 2,710KB

Figure 5.4. WinZip - msjbdc.tar

5. scroll down and select **msbase.jar**, **mssqlserver.jar**, **msutil.jar**, click **Extract** displaying Figure 5.5,



Extract to: C:\Program Files\PhinMS

Files

● Selected files

○ All files

○ Files:

☐ Overwrite existing files

☐ Skip older files

☑ Use folder names

Figure 5.5. Extract Files

6. extract to **\Program Files\PhinMS\2.8.00\tomcat-5.0.19\webapps\Receiver\WEB-INF\lib**, click **Extract**, close WinZip window,
7. open **Microsoft SQL Server Enterprise Manager** shown in Figure 5.6,

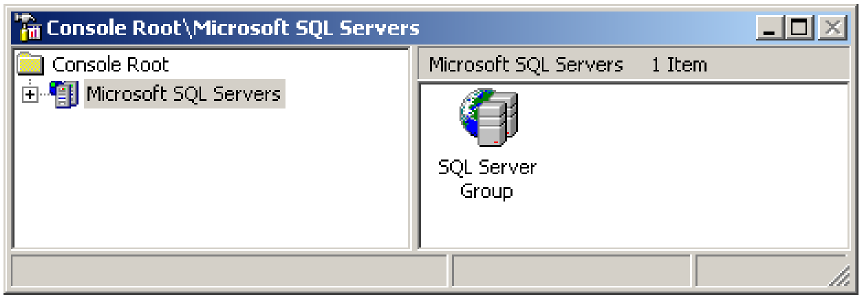
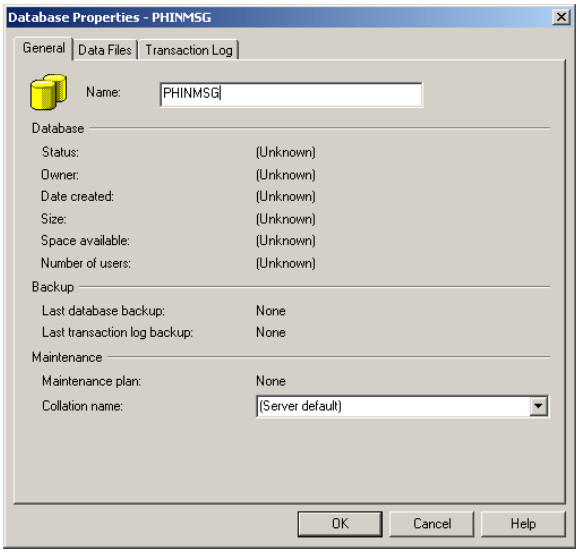

Console Root\Microsoft SQL Servers
Console Root
Microsoft SQL Servers
Microsoft SQL Servers 1 Item
SQL Server Group

Figure 5.6. Microsoft SQL Server Enterprise Manager

8. click **Microsoft SQL Servers**, **SQL Server Group**, **Local** server, right click on **Database**, select **New Database** displaying Figure 5.7,



Name: PHINMSG

Database

Status:	(Unknown)
Owner:	(Unknown)
Date created:	(Unknown)
Size:	(Unknown)
Space available:	(Unknown)
Number of users:	(Unknown)

Backup

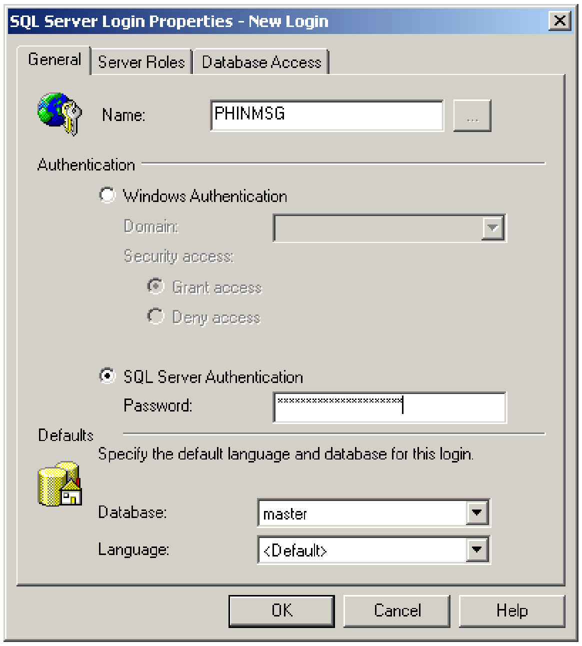
Last database backup:	None
Last transaction log backup:	None

Maintenance

Maintenance plan:	None
Collation name:	(Server default)

Figure 5.7. Database Properties

9. type **PHINMSG** in the Name field, click **OK** database,
10. open **PHINMSG** database, right click **Users**, select **New Database User**, check **public** and **db_owner**, select **New** for the login name from the dropdown list displaying Figure 5.8, and



SQL Server Login Properties - New Login

Name: PHINMSG

Authentication

○ Windows Authentication

Domain:

Security access:

● Grant access

○ Deny access

● SQL Server Authentication

Password: **********************

Defaults

Specify the default language and database for this login.

Database: master

Language: <Default>

Figure 5.8. SQL Server Login Properties - New Login

11. type **PHINMSG** in the Name field, enter a password (challenge phrase is recommended), click **OK**, confirm password, click **OK**, successfully creating the PHINMS user if the access reads Permit.

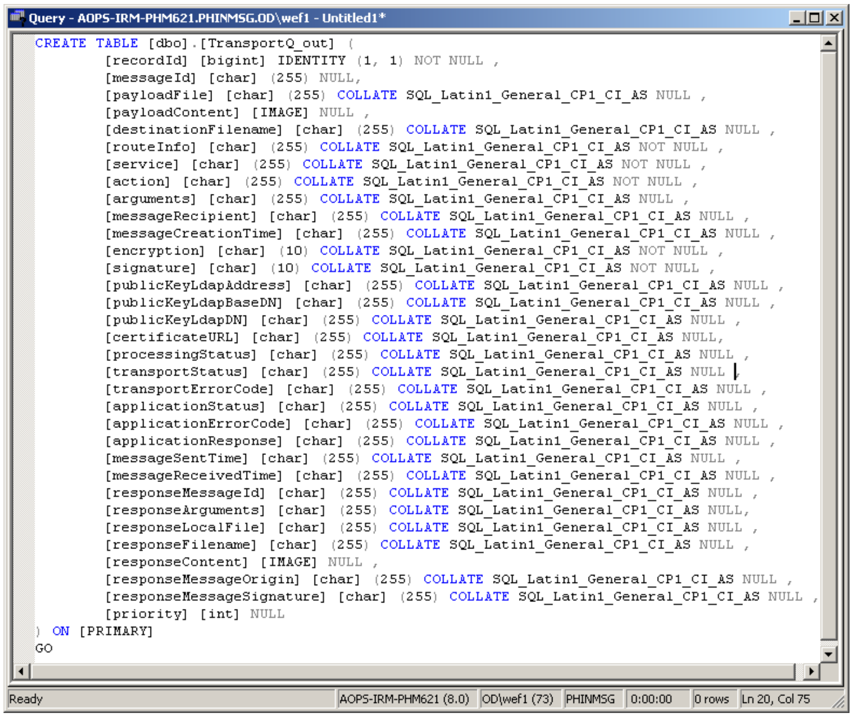
5.2 Create TransportQ_out Table

To create the **TransportQ_out** table in the Public Health Information Network Messaging (PHINMSG) database using the Microsoft TransportQ script, complete the following steps:

1. copy **SQL script** listed below

```
CREATE TABLE [dbo].[TransportQ_out] (
    [recordId] [bigint] IDENTITY (1, 1) NOT NULL ,
    [messageId] [char] (255) NULL,
    [payloadFile] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
    [payloadContent] [IMAGE] NULL ,
    [destinationFilename] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
    [routeInfo] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NOT NULL ,
    [service] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NOT NULL ,
    [action] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NOT NULL ,
    [arguments] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
    [messageRecipient] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
    [messageCreationTime] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
    [encryption] [char] (10) COLLATE SQL_Latin1_General_CP1_CI_AS NOT NULL ,
    [signature] [char] (10) COLLATE SQL_Latin1_General_CP1_CI_AS NOT NULL ,
    [publicKeyLdapAddress] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
    [publicKeyLdapBaseDN] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
    [publicKeyLdapDN] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
    [certificateURL] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL,
    [processingStatus] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
    [transportStatus] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
    [transportErrorCode] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
    [applicationStatus] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
    [applicationErrorCode] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
    [applicationResponse] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
    [messageSentTime] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
    [messageReceivedTime] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
    [responseMessageId] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
    [responseArguments] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL,
    [responseLocalFile] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
    [responseFilename] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
    [responseContent] [IMAGE] NULL ,
    [responseMessageOrigin] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
    [responseMessageSignature] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
    [priority] [int] NULL
) ON [PRIMARY]
GO
```

2. open the **SQL Server Enterprise Manager**, select **PHINMSG, Tools, SQL Query Analyzer**, displaying Figure 5.9,

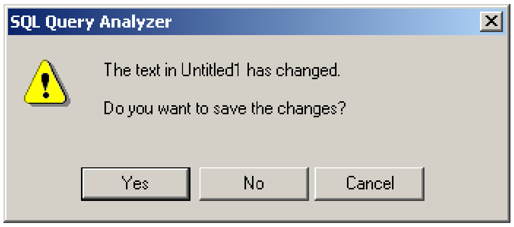


```
CREATE TABLE [dbo].[TransportQ_out] (
        [recordId] [bigint] IDENTITY (1, 1) NOT NULL ,
        [messageId] [char] (255) NULL,
        [payloadFile] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
        [payloadContent] [IMAGE] NULL ,
        [destinationFilename] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
        [routeInfo] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NOT NULL ,
        [service] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NOT NULL ,
        [action] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NOT NULL ,
        [arguments] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
        [messageRecipient] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
        [messageCreationTime] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
        [encryption] [char] (10) COLLATE SQL_Latin1_General_CP1_CI_AS NOT NULL ,
        [signature] [char] (10) COLLATE SQL_Latin1_General_CP1_CI_AS NOT NULL ,
        [publicKeyLdapAddress] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
        [publicKeyLdapBaseDN] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
        [publicKeyLdapDN] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
        [certificateURL] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL,
        [processingStatus] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
        [transportStatus] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
        [transportErrorCode] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
        [applicationStatus] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
        [applicationErrorCode] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
        [applicationResponse] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
        [messageSentTime] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
        [messageReceivedTime] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
        [responseMessageId] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
        [responseArguments] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL,
        [responseLocalFile] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
        [responseFilename] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
        [responseContent] [IMAGE] NULL ,
        [responseMessageOrigin] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
        [responseMessageSignature] [char] (255) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
        [priority] [int] NULL
) ON [PRIMARY]
GO
```

Figure 5.9. Query Analyzer

3. paste the SQL script from step one (1) into the query analyzer, select **Execute Query** (F5),

4. close the **Query Analyzer** window displaying Figure 5.10,

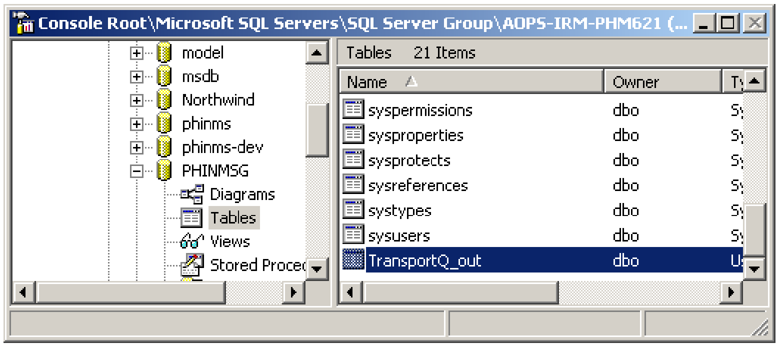


The text in Untitled1 has changed.

Do you want to save the changes?

Figure 5.10. Query Analyzer Prompt

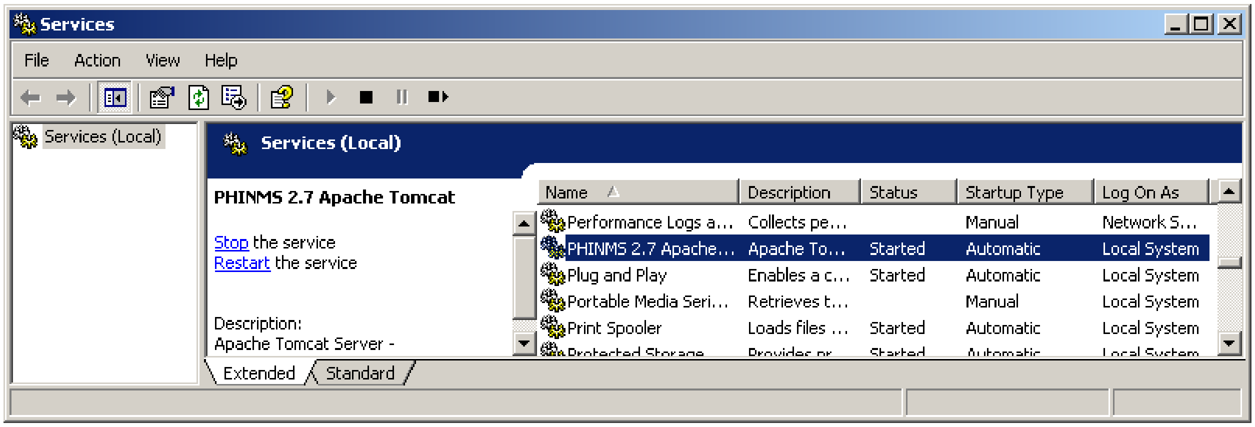
5. click **Yes** navigate to **\Program Files\PhinMS\2.8.0\tomcat-5.0.19\phinms**, save as **TransportQ_out**, close window, verify the table was successfully created in the Tables folder shown in Figure 5.11,



Name	Owner	Ty
syspermissions	dbo	Sy
sysproperties	dbo	Sy
sysprotects	dbo	Sy
sysreferences	dbo	Sy
systypes	dbo	Sy
sysusers	dbo	Sy
TransportQ_out	dbo	U

Figure 5.11. TransportQ_out Table

6. select **Control Panel** from Microsoft Start, **Administrative Tools**, **Services** displaying Figure 5.12,



PHINMS 2.7 Apache Tomcat

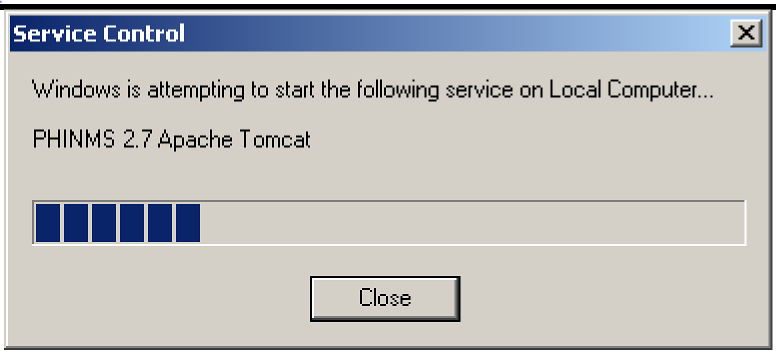
Stop the service
Restart the service

Description:
Apache Tomcat Server -

Name	Description	Status	Startup Type	Log On As
Performance Logs a...	Collects pe...		Manual	Network S...
PHINMS 2.7 Apache...	Apache To...	Started	Automatic	Local System
Plug and Play	Enables a c...	Started	Automatic	Local System
Portable Media Seri...	Retrieves t...		Manual	Local System
Print Spooler	Loads files ...	Started	Automatic	Local System
Protected Storage	Provides pr...	Started	Automatic	Local System

Figure 5.12. Services

7. select **PHINMS 2.7 Apache Tomcat**, click **Restart the service** displaying Figure 5.13, and



Windows is attempting to start the following service on Local Computer...

PHINMS 2.7 Apache Tomcat

Figure 5.13. Service Control

8. close the windows.

Note: During configuration if problems are encountered, open the log file from Window Explorer **\Program Files\PhinMS\2.8.0\tomcat-5.0.19\phinms\logs\Sender** which will document the error.

6.0 SENDER INFORMATION

PHINMS Version 2.8.00 installation has two components - the Sender and the Receiver. Sending a test message allows the PHINMS Sender to send messages to the TransportQ and to the CDC. Testing the PHINMS installation is a three-part procedure which includes the following:

- ping the PHINMS Sender loopback route,
- ping the PHINMS CDC Ping Server (phinmsping.cdc.gov), and
- ping the PHINMS CDC Staging Receiver. (Requires CPA files be emailed to Phintech@cdc.gov. Refer to Section 6.3.1 for more information.

Figure 6.1 displays a diagram to assist with understanding the PHINMS authentication process.

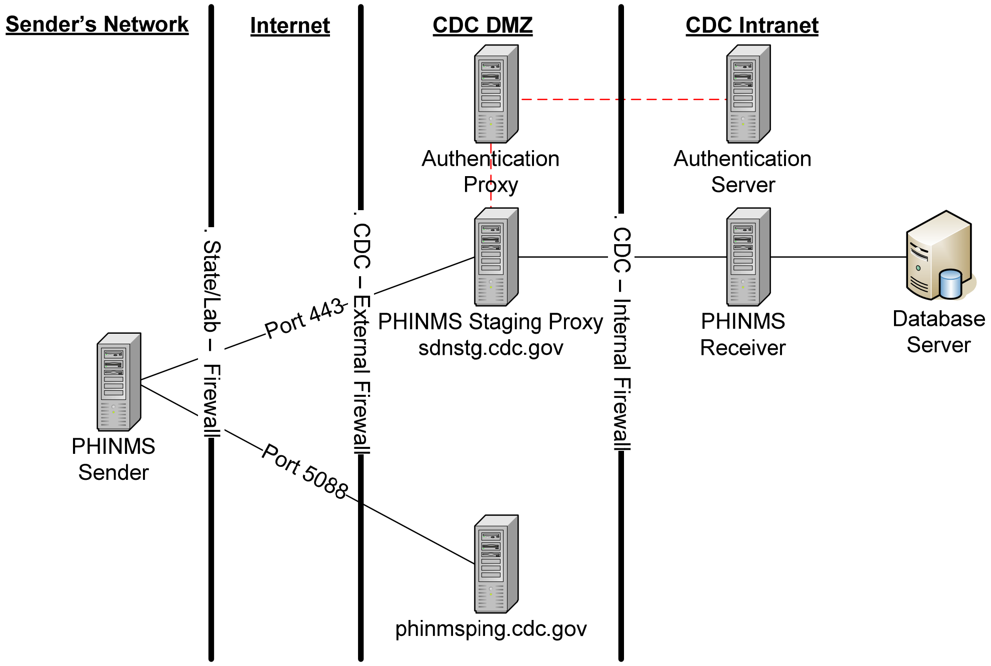


Figure 6.1. CDC PHINMS Topology

6.1 Ping Loopback

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

Verify the generated ping loopback is successfully sent to the loopback message processor by completing the following steps:

1. open the **PHINMS 2.7.00 SP1 Console** displaying Figure 6.2,

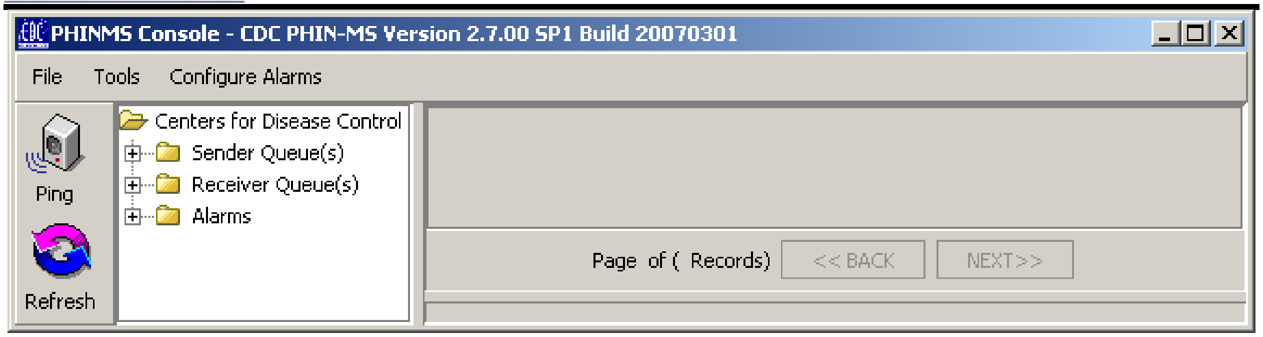
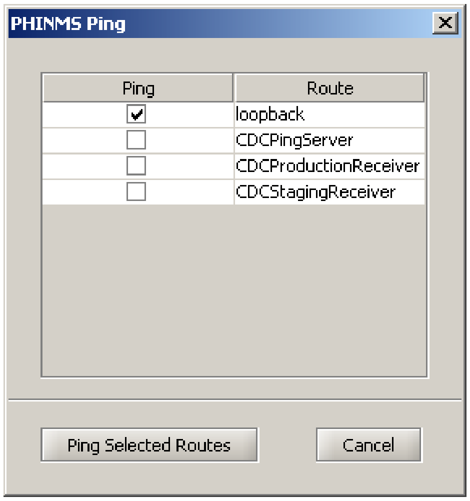


Figure 6.2. PHINMS 2.7.00 SP1 Console

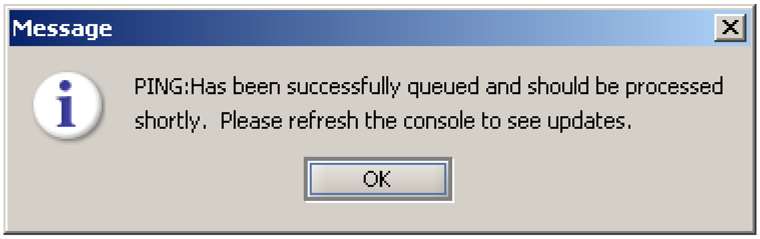
2. expand **Sender Queue(s)**, expand **Transport**, select **TransportQ_out**, select **Ping** displaying Figure 6.3,



Ping	Route
☑	loopback
□	CDCPingServer
□	CDCProductionReceiver
□	CDCStagingReceiver

Figure 6.3. PHINMS Ping

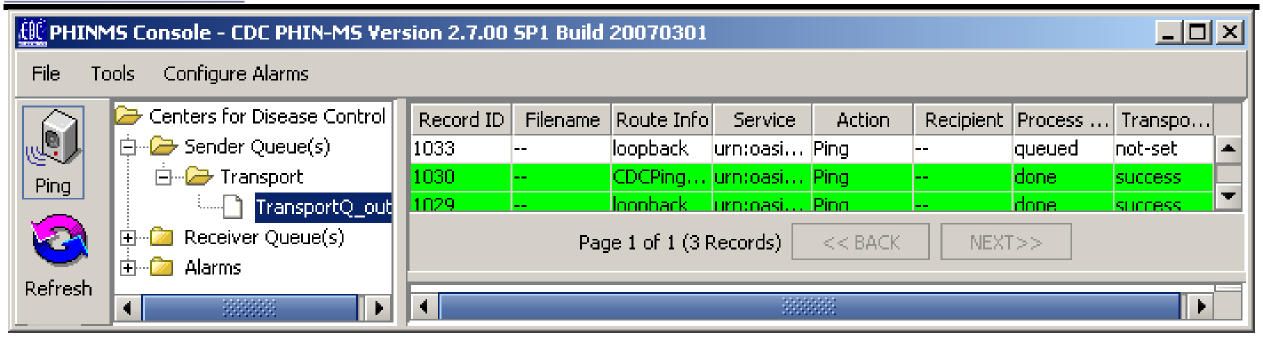
3. check **loopback**, click **Ping Selected Routes** displaying Figure 6.4,



PING:Has been successfully queued and should be processed shortly. Please refresh the console to see updates.

Figure 6.4. Ping Message

4. click **OK**, a Record ID has been created indicating a queued process status shown in Figure 6.5, and



Record ID	Filename	Route Info	Service	Action	Recipient	Process ...	Transpo...
1033	--	loopback	urn:oasi...	Ping	--	queued	not-set
1030	--	CDCPing...	urn:oasi...	Ping	--	done	success
1029	--	loopback	urn:oasi...	Ping	--	done	success

Page 1 of 1 (3 Records)

Figure 6.5. Queued Record ID

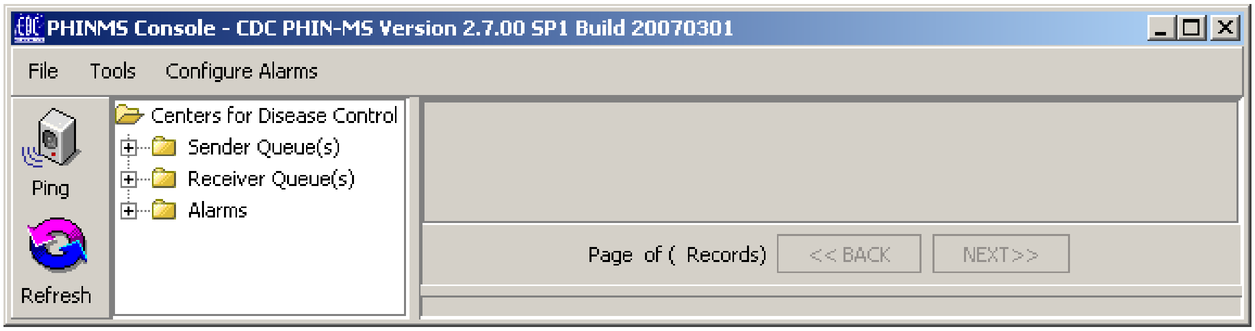
5. click **Refresh** changing the status to attempted, click **Refresh** again changing the status to done indicating success.

6.2 Ping CDC Ping Server

The ping CDCPingServer validates the Sender can connect to the internet and to the CDC without the need for authentication (security credentials). The CDC Ping Server is dedicated to answering Ping requests and will not receive any real messages. Port 5088 needs to be open on the firewall at the Sender's location to generate a ping to the CDCPingServer.

Verify the message ping to the CDC Ping Server is successful by completing the following steps:

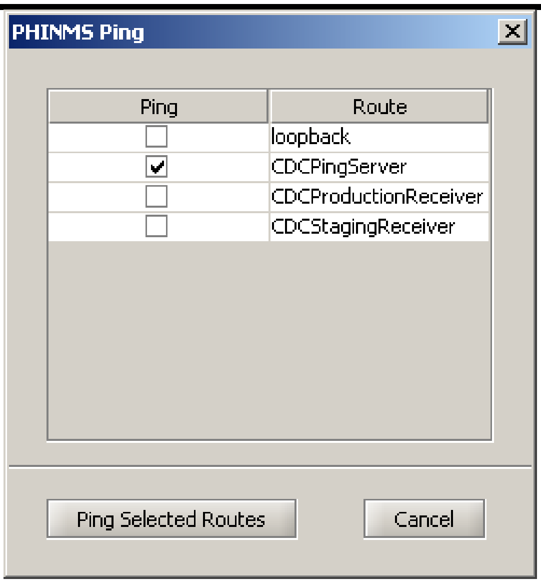
1. open the **PHINMS 2.7.00 SP1 Console** displaying Figure 6.6,


PHINMS Console - CDC PHIN-MS Version 2.7.00 SP1 Build 20070301
File
Tools
Configure Alarms
Ping
Refresh
Centers for Disease Control
Sender Queue(s)
Receiver Queue(s)
Alarms
<< BACK
NEXT>>

Page of (Records)

Figure 6.6. PHINMS 2.7.00 SP1 Console

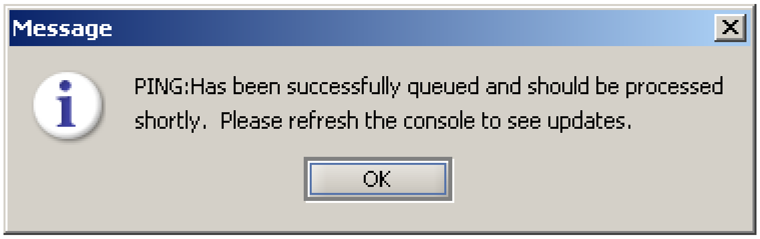
2. expand **Sender Queue(s)**, expand **Transport**, select **TransportQ_out**, select **Ping** displaying Figure 6.7,



Ping	Route
□	loopback
☑	CDCPingServer
□	CDCProductionReceiver
□	CDCStagingReceiver

Figure 6.7. PHINMS CDC Ping

3. check **CDCPingServer**, click **Ping Selected Routes** displaying Figure 6.8, and



PING:Has been successfully queued and should be processed shortly. Please refresh the console to see updates.

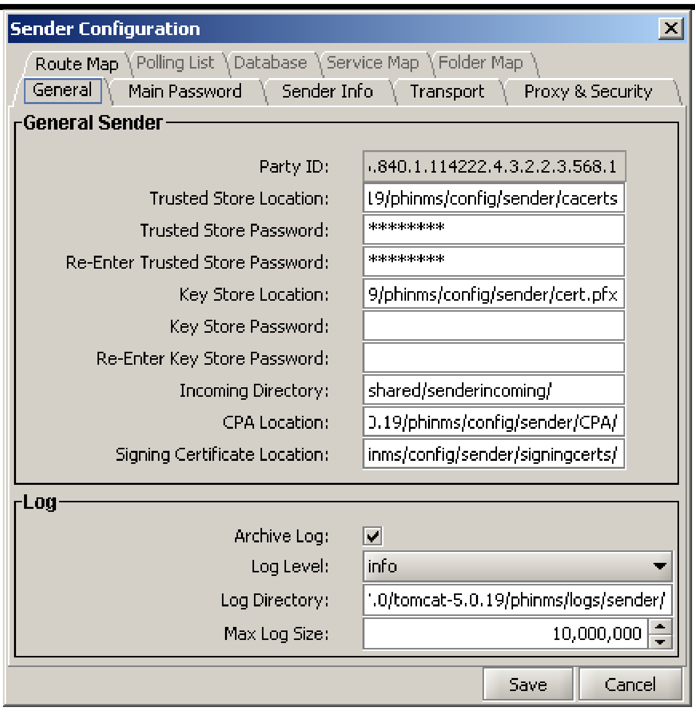
Figure 6.8. Ping Message

4. click **OK**, a Record ID has been created indicating a queued, click **Refresh** changing the status to attempted, click **Refresh** again changing the status to done indicating success.

6.3 Configure CDC Staging Receiver

The CDC Staging Receiver requires to be configured before sending a Ping. Configure the CDCStagingReceiver using the following steps:

1. select **Snd Cfg** displaying Figure 6.9,



General Sender

Party ID: ı.840.1.114222.4.3.2.2.3.568.1

Trusted Store Location: l9/phinms/config/sender/cacerts

Trusted Store Password: ********

Re-Enter Trusted Store Password: ********

Key Store Location: 9/phinms/config/sender/cert.pfx

Key Store Password:

Re-Enter Key Store Password:

Incoming Directory: shared/senderincoming/

CPA Location: J.19/phinms/config/sender/CPA/

Signing Certificate Location: inms/config/sender/signingcerts/

Log

Archive Log: ☑

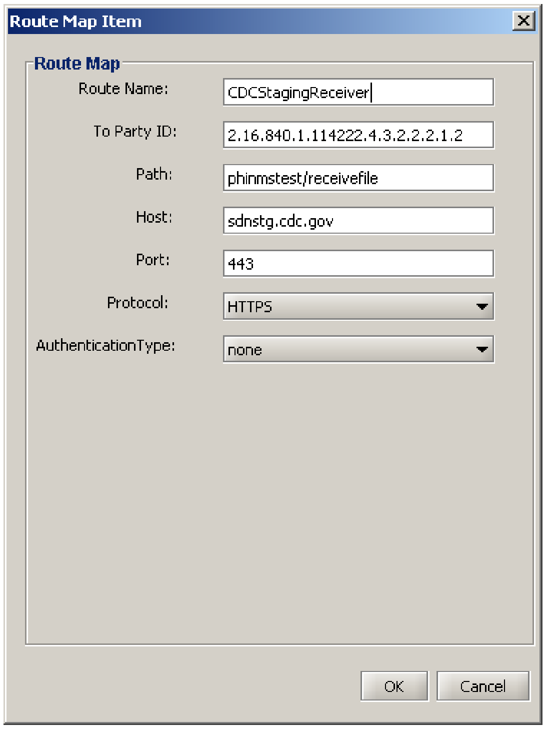
Log Level: info

Log Directory: '.0/tomcat-5.0.19/phinms/logs/sender/

Max Log Size: 10,000,000

Figure 6.9. Sender Configuration

2. select the **Route Map**, **CDCStagingReceiver**, click **Update** displaying Figure 6.10,



Route Map

Route Name: CDCStagingReceiver

To Party ID: 2.16.840.1.114222.4.3.2.2.1.2

Path: phinmstest/receivefile

Host: sdnstg.cdc.gov

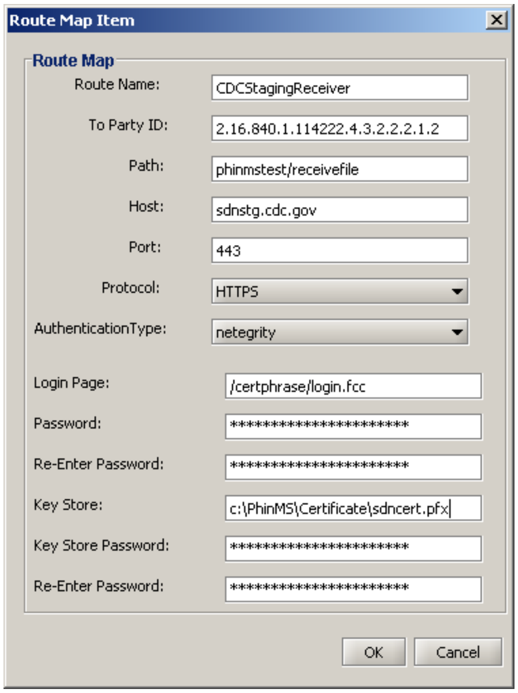
Port: 443

Protocol: HTTPS

AuthenticationType: none

Figure 6.10. Route Map Item

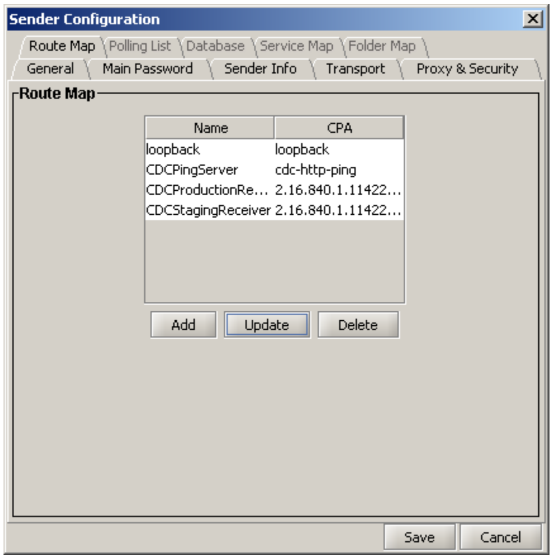
3. select **Netegrity** as the AuthenticationType displaying Figure 6.11,



Route Name: CDCStagingReceiver
To Party ID: 2.16.840.1.114222.4.3.2.2.2.1.2
Path: phinmstest/receivefile
Host: sdnstg.cdc.gov
Port: 443
Protocol: HTTPS
AuthenticationType: netegrity
Login Page: /certphrase/login.fcc
Password: **********************
Re-Enter Password: **********************
Key Store: c:\PhinMS\Certificate\sdncert.pfx
Key Store Password: **********************
Re-Enter Password: **********************

Figure 6.11. CDC Route Map Configuration

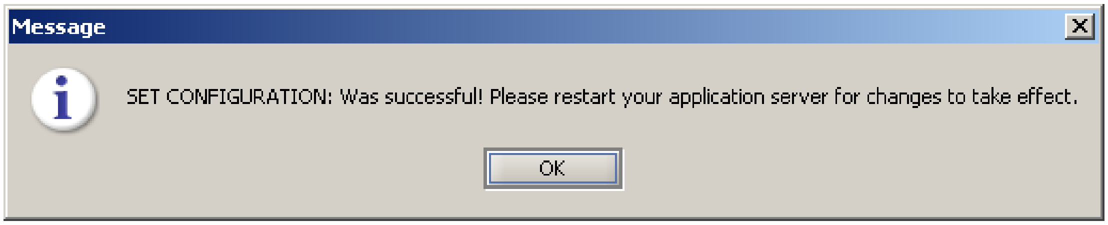
4. type **/certphrase/login.fcc** in the Login Page field, enter the **SDN Challenge Phrase**, confirm **SDN Challenge Phrase**, enter the path to the stored certificate keystore (.pfx file), enter the **Key Store Password**, confirm the **Key Store Password**, click **OK**, displaying Figure 6.12,



Name	CPA
loopback	loopback
CDCPingServer	cdc-http-ping
CDCProductionRe...	2.16.840.1.11422...
CDCStagingReceiver	2.16.840.1.11422...

Figure 6.12. CDC Route Map

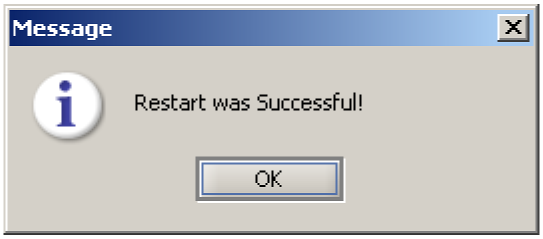
5. click **Save**, displaying Figure 6.13,



SET CONFIGURATION: Was successful! Please restart your application server for changes to take effect.

Figure 6.13. CDC Route Configuration Successful

6. click **OK**, restart the PHINMS application displaying Figure 6.14, and



Restart was Successful!

Figure 6.14. Restart Successful

7. click OK.

6.3.1 Email CPA File

PHINMS creates a Collaboration Protocol Agreement (CPA) file for each route listed on the Route Map tab of the Sender Configuration panel.

The PHINMS Administrator must send the PHINMS Helpdesk (Phintech@cdc.gov) the CPA files for each route specifying either the CDC Production Receiver or the CDC Staging Receiver. Only after the PHINMS helpdesk has received the CPA file and applied it to the PHINMS Receiver can there be a successful transmission of messages from the Sender to the Receiver.

The CPA files required to be sent are located in directory x:\install dir\2.7.00\tomcat-5.0.19\phinms\config\Sender\CPA.

Note: Information on CPA can be found in the PHINMS Technical Reference Guide.

6.4 Ping CDC Staging Receiver

The ping PHINMS Staging Receiver validates end-to-end success of the Sender's ability to connect to the CDC over the internet, authenticate with the CDC's Authentication Server, and communicate with the Staging Receiver.

Verify the generated ping message is successfully sent to the CDC Staging Receiver message processor by completing the following steps:

1. open the **PHINMS 2.7.00 SP1 Console** displaying Figure 6.15,

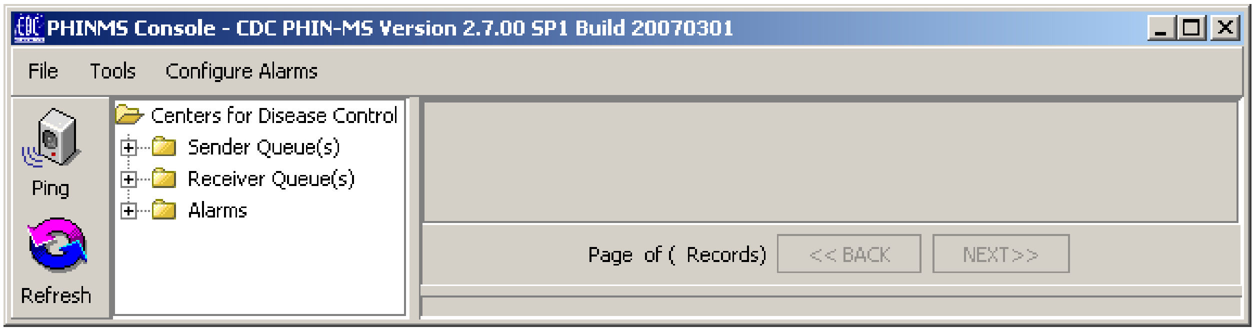
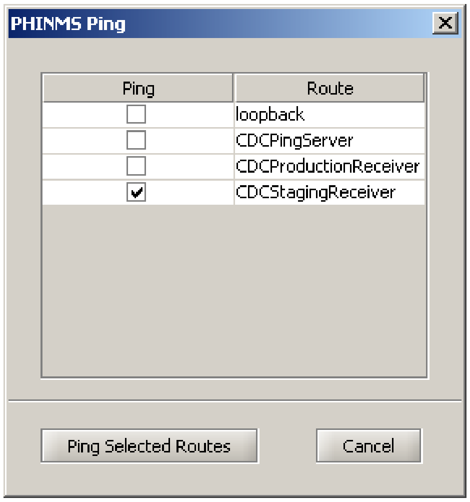


Figure 6.15. PHINMS 2.7.00 SP1 Console

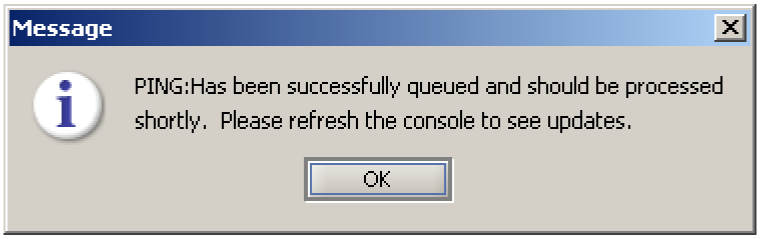
2. expand **Sender Queue(s)**, expand **Transport**, select **TransportQ_out**, select **Ping** displaying Figure 6.16,



Ping	Route
□	loopback
□	CDCPingServer
□	CDCProductionReceiver
☑	CDCStagingReceiver

Figure 6.16. PHINMS Ping

3. check **CDCStagingReceiver**, click **Ping Selected Routes** displaying Figure 6.17, and



PING:Has been successfully queued and should be processed shortly. Please refresh the console to see updates.

Figure 6.17. Ping Message

4. click **OK**, a Record ID has been created indicating a queued, click **Refresh** changing the status to attempted, click **Refresh** again changing the status to done indicating success.

6.5 Send Test Payload Message

The send payload message verifies the capability to send an outbound message with an attached file to a Receiver.

Note: Ensure the CPA files have been sent to the PHIN Help desk before attempting to send a payload message. Refer to Section 6.3.1 for CPA information.

Send the payload message test to the PHINMS Staging Receiver by completing the following steps:

1. open the **PHINMS 2.7.00 SP1 Console** displaying Figure 6.18,

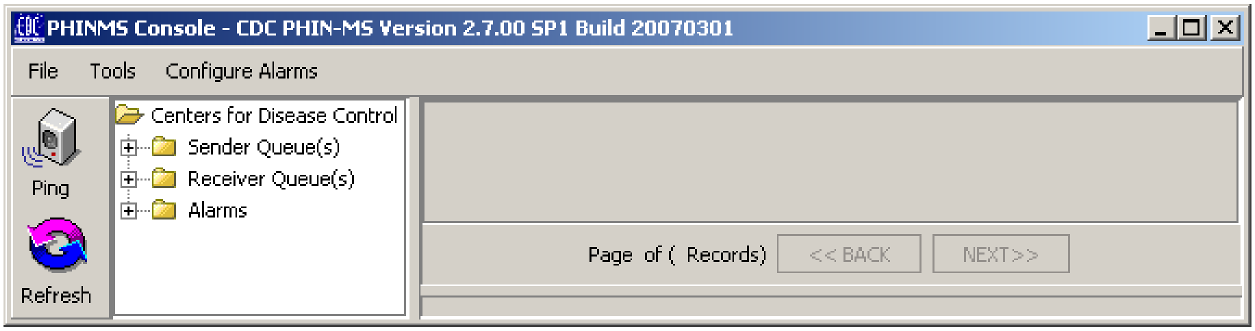
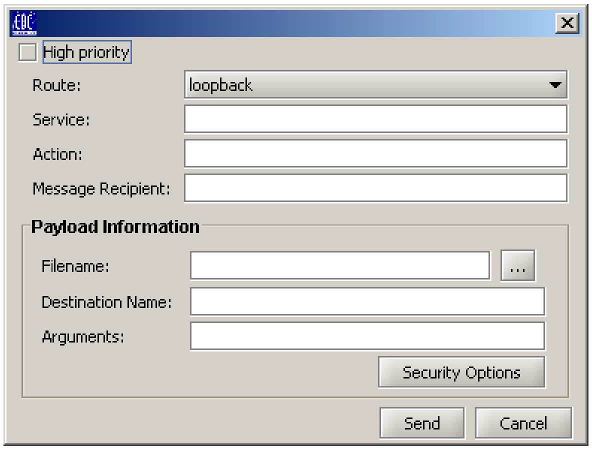


Figure 6.18. PHINMS 2.7.00 SP1 Console

2. expand **Sender Queue(s)**, expand **Transport**, select **TransportQ_out**, select **Message** displaying Figure 6.19,


☐ High priority

Route: loopback

Service:

Action:

Message Recipient:

Payload Information

Filename:

Destination Name:

Arguments:

Figure 6.19. PHINMS Ping

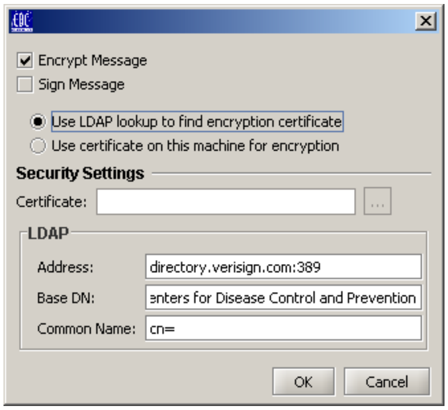
3. enter the following parameters:
   - Route: **CDC Staging Receiver**,
   - Service: **QueueTransfer**,
   - Action: **Test**,

- Message Recipient: **optional - can be left blank**,
- Filename: **browse for a file to attach**,
- Destination Name: **optional - can be left blank**,
- Arguments: **optional - can be left blank**,

4. proceed to **Step 5** if using Security Options and to **Step 8** if not,

Note: Security Options are optional for encrypting or signing messages.

5. click **Security Options** displaying Figure 6.20,



☑ Encrypt Message
□ Sign Message

● Use LDAP lookup to find encryption certificate
○ Use certificate on this machine for encryption

Security Settings

Certificate:

LDAP

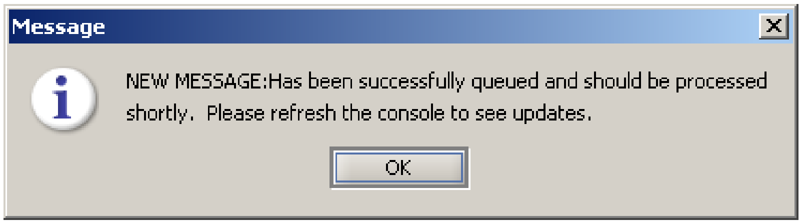
Address: directory.verisign.com:389

Base DN: enters for Disease Control and Prevention

Common Name: cn=

Figure 6.20. Security Options

6. enter the following parameters:
   - check **Encrypt Message**,
   - select **Use LDAP lookup to find encryption certificate**,
   - Address: **directory.verisign.com:389**,
   - BaseDN: **o=Centers for Disease Control and Prevention**,
   - Common Name: **cn=cdc phinms**,
7. click **OK**,
8. click **Send** displaying Figure 6.21, and



Message

NEW MESSAGE:Has been successfully queued and should be processed shortly. Please refresh the console to see updates.

Figure 6.21. New Message Notification

9. click **OK**.

6.6 Create Route Map

Messages sent using PHINMS need to address a specific recipient in the PHINMS 2.7.00 SP1 Console. Each Route is mapped to the recipient's attributes, such as the URL, transport protocol, and authentication type.

Obtain the partner's PartyID, the authentication type, and the security credentials.

Create a Route by completing the following steps:

1. open the **PHINMS 2.7.00 SP1 Console** displaying Figure 6.22,

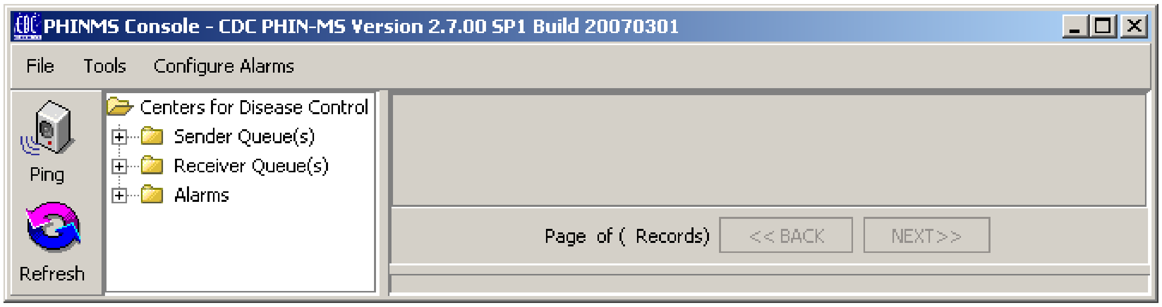
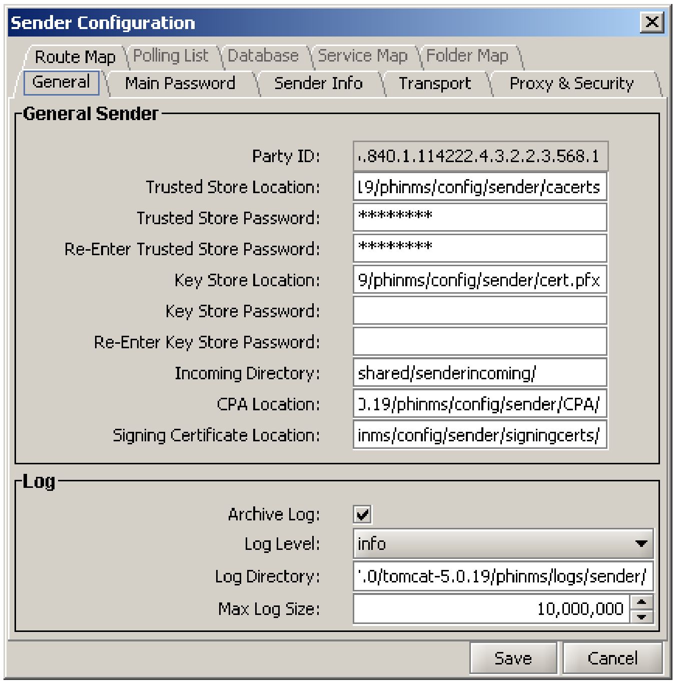


Figure 6.22. PHINMS 2.7.00 SP1 Console

2. double click **Snd Cfg** displaying Figure 6.23,



General Sender

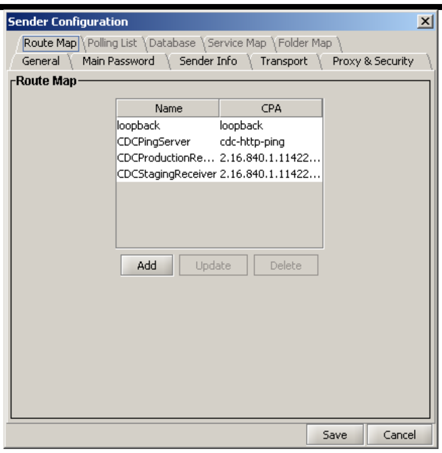
Party ID: ..840.1.114222.4.3.2.2.3.568.1
Trusted Store Location: 19/phinms/config/sender/cacerts
Trusted Store Password: ********
Re-Enter Trusted Store Password: ********
Key Store Location: 9/phinms/config/sender/cert.pfx
Key Store Password:
Re-Enter Key Store Password:
Incoming Directory: shared/senderincoming/
CPA Location: 0.19/phinms/config/sender/CPA/
Signing Certificate Location: inms/config/sender/signingcerts/

Log

Archive Log: ☑
Log Level: info
Log Directory: '.0/tomcat-5.0.19/phinms/logs/sender/
Max Log Size: 10,000,000

Figure 6.23. Sender Configuration

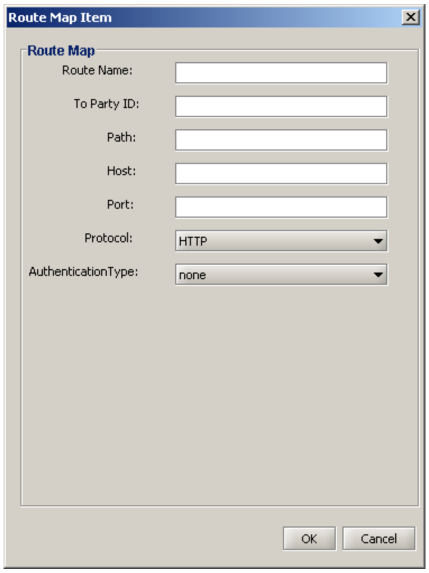
3. select **Route Map** tab displaying Figure 6.24,



Name	CPA
loopback	loopback
CDCPingServer	cdc-http-ping
CDCProductionRe...	2.16.840.1.11422...
CDCStagingReceiver	2.16.840.1.11422...

Figure 6.24. Route Map

4. select **Add** displaying Figure 6.25,



Route Name:

To Party ID:

Path:

Host:

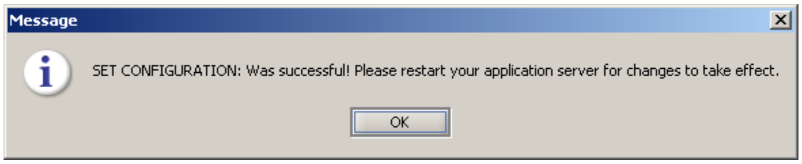
Port:

Protocol: HTTP

AuthenticationType: none

Figure 6.25. Route Map Item

5. enter **Route Name**, **To Party ID**, **Path**, **Host**, **Port**, **Protocol**, **AuthenticationType**, click **OK**, click **Save** displaying Figure 6.26, and



SET CONFIGURATION: Was successful! Please restart your application server for changes to take effect.

Figure 6.26. Set Configuration

6. click **OK**.

7.0 RECEIVER INFORMATION

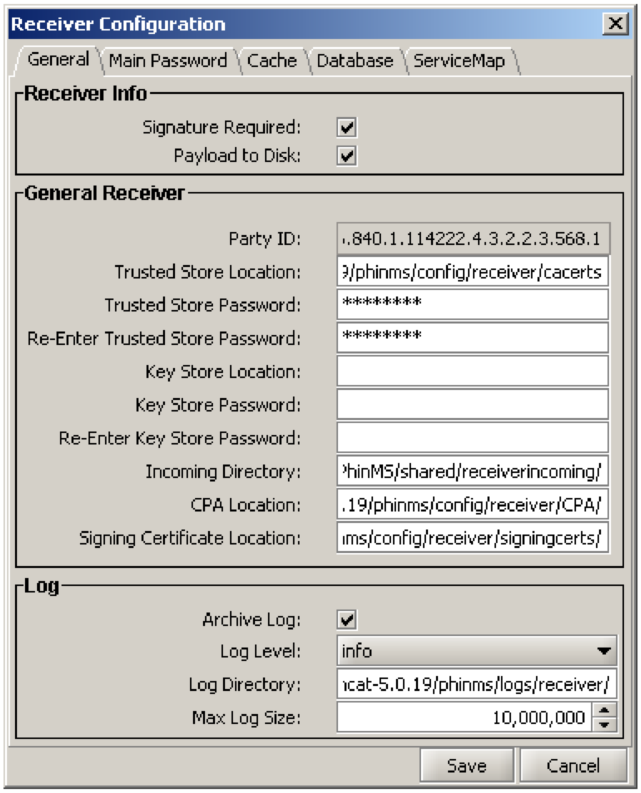
7.1 Configure WorkerQ

The Worker Queue (WorkerQ) is the database table used for storing inbound messages. When configured from the Receiver configuration screen in the Console, it is used to drop incoming messages sent to the Receiver. The database configuration needs to be completed before creating WorkerQ table. The instructions to configure a database connection to the external database are in Section 5.0.

If configured from the Sender configuration screen in the Console, it is used to write the responses to polling requests (route-not-read configuration). More information on Sender configuration can be located in the PHINMS Technical Reference Guide.

Create an external database WorkerQ table by following steps below:

1. select **Rcv Cfg** displaying Figure 7.1,



Receiver Info

Signature Required: ☑
Payload to Disk: ☑

General Receiver

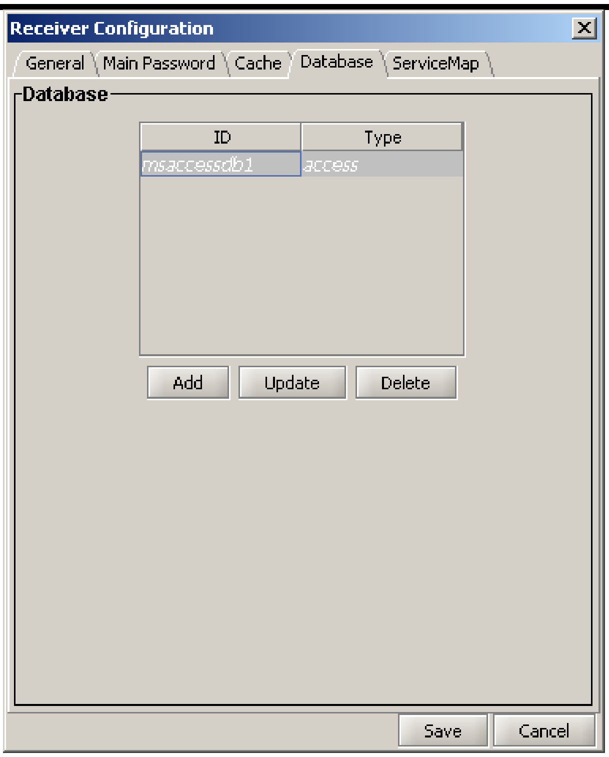
Party ID: ı.840.1.114222.4.3.2.2.3.568.1
Trusted Store Location: ?/phinms/config/receiver/cacerts
Trusted Store Password: ********
Re-Enter Trusted Store Password: ********
Key Store Location:
Key Store Password:
Re-Enter Key Store Password:
Incoming Directory: ᐳhinMS/shared/receiverincoming/
CPA Location: .19/phinms/config/receiver/CPA/
Signing Certificate Location: ıms/config/receiver/signingcerts/

Log

Archive Log: ☑
Log Level: info
Log Directory: ıcat-5.0.19/phinms/logs/receiver/
Max Log Size: 10,000,000

Figure 7.1. Receiver Configuration

2. select the **Database** tab displaying Figure 7.2,

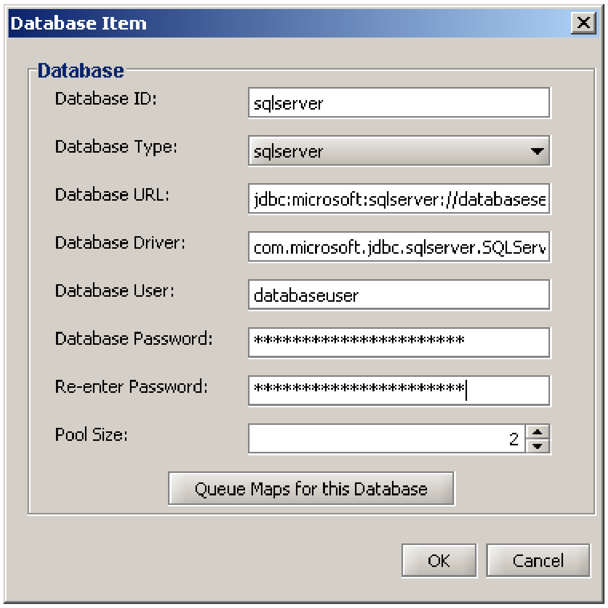


Database

ID	Type
msaccessdb1	access

Figure 7.2. Database Configuration

3. click **Add** displaying Figure 7.3,



Database

Database ID: sqlserver

Database Type: sqlserver

Database URL: jdbc:microsoft:sqlserver://databasese

Database Driver: com.microsoft.jdbc.sqlserver.SQLServ

Database User: databaseuser

Database Password: ***********************

Re-enter Password: ***********************

Pool Size: 2

Figure 7.3. Database Item

4. enter the database items using Table 1 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.
Database Type	Designates the type of database.
Database URL	The URL to the database. The URL depends on the type of database and driver used such as **jdbc:microsoft: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 such as **com.microsoft.jdbc.sqlserver.SQLServerDriver** for Microsoft SQL Server and **oracle.jdbc.OracleDriver** for Oracle.
Database User	A pointer to the database user entry 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 user name.
Database Password	A pointer to the database password entry 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.
Pool Size	The number of database connections to open. When setting the pool size ensure the system can handle the maximum client load while keeping enough memory available.

Table 1. WorkerQ Database Tag Values

5. click **Queue maps For This Database** displaying Figure 7.4,

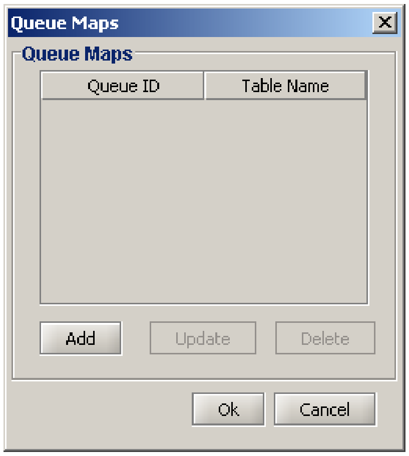
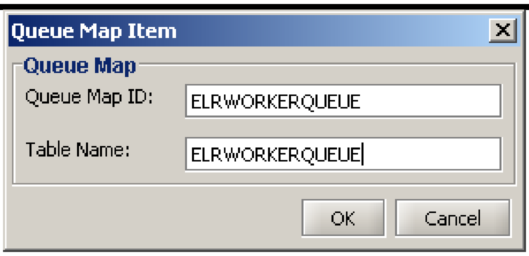


Figure 7.4. Queue Maps

6. click **Add** displaying Figure 7.5,



Queue Map ID: ELRWORKERQUEUE

Table Name: ELRWORKERQUEUE

Figure 7.5. Queue Map Item

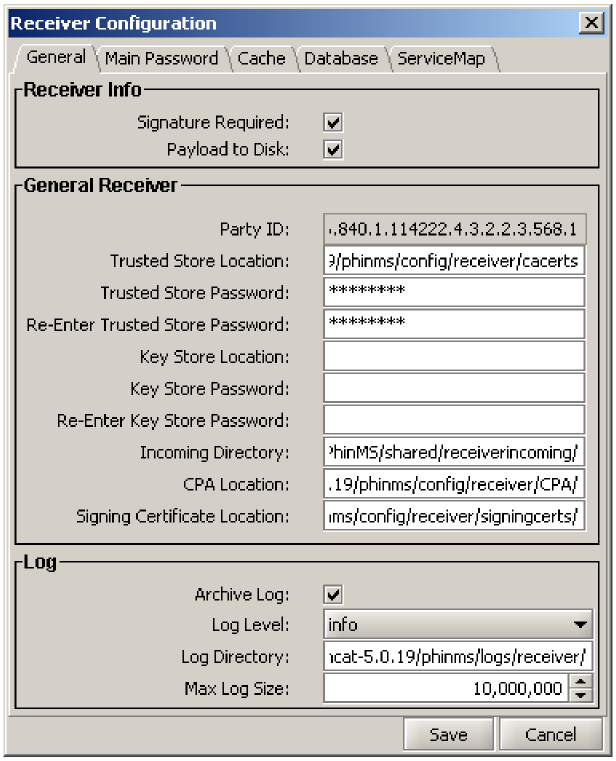
7. enter **Queue Map ID** and **Table Name**,
8. click **OK**, **OK**, **OK**, **OK**, **Save**, and
9. select **Restart**.

7.2 Create Service and Action Pair

Each message sent using PHINMS 2.7.00 SP1 has a message envelope. The envelope has addressing information tags called Service and Action known as character strings. Character strings 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. select **Rcv Cfg** displaying Figure 7.6,



Signature Required: ☑

Payload to Disk: ☑

Party ID: ı.840.1.114222.4.3.2.2.3.568.1

Trusted Store Location: ∋/phinms/config/receiver/cacerts

Trusted Store Password: *********

Re-Enter Trusted Store Password: *********

Key Store Location:

Key Store Password:

Re-Enter Key Store Password:

Incoming Directory: ›hinMS/shared/receiverincoming/

CPA Location: .19/phinms/config/receiver/CPA/

Signing Certificate Location: ıms/config/receiver/signingcerts/

Archive Log: ☑

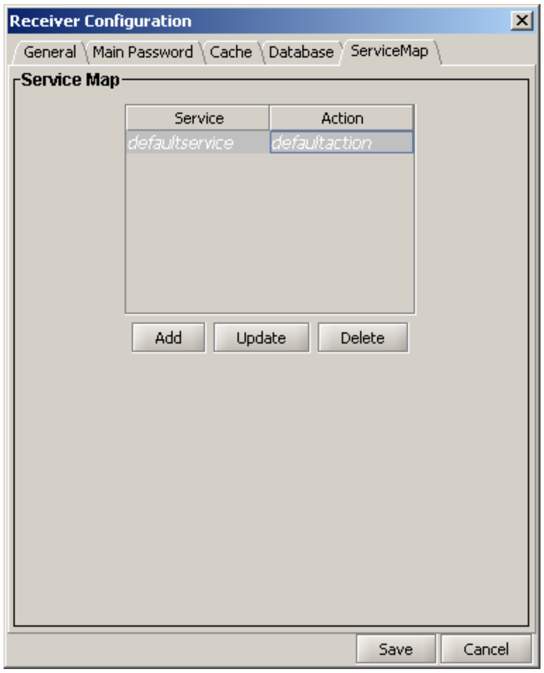
Log Level: info

Log Directory: ıcat-5.0.19/phinms/logs/receiver/

Max Log Size: 10,000,000

Figure 7.6. Receiver Configuration

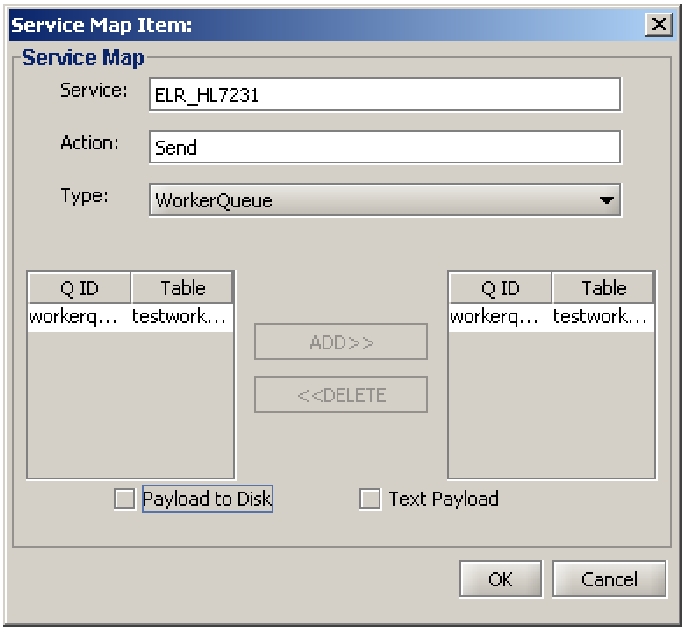
2. select the **Service Map** tab displaying Figure 7.7,



Service	Action
defaultservice	defaultaction

Figure 7.7. Service Map

3. click **Add** displaying Figure 7.8,



Service: ELR_HL7231

Action: Send

Type: WorkerQueue

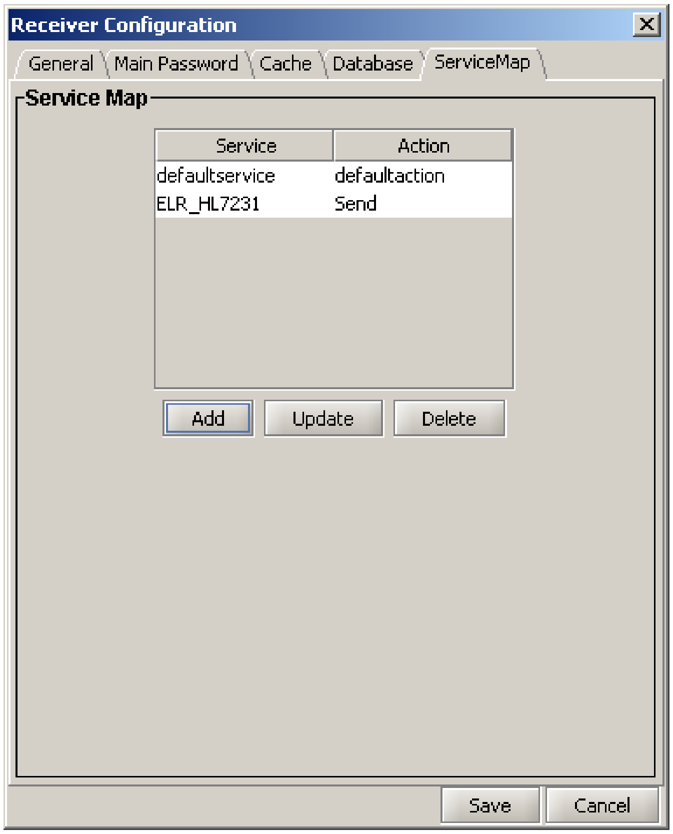
Q ID	Table
workerq...	testwork...

Q ID	Table
workerq...	testwork...

☐ Payload to Disk ☐ Text Payload

Figure 7.8. Service Map Item

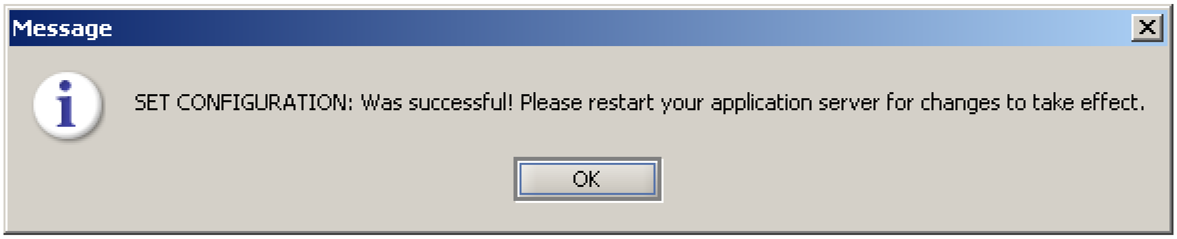
4. enter **Service**, **Action**, select **WorkerQueue** from the dropdown list, highlight **workerqueue** located under Q ID in the left table, click **Add**, click **OK** displaying Figure 7.9,



Service	Action
defaultservice	defaultaction
ELR_HL7231	Send

Figure 7.9. Service and Action Added

5. select **Save** displaying Figure 7.10, and



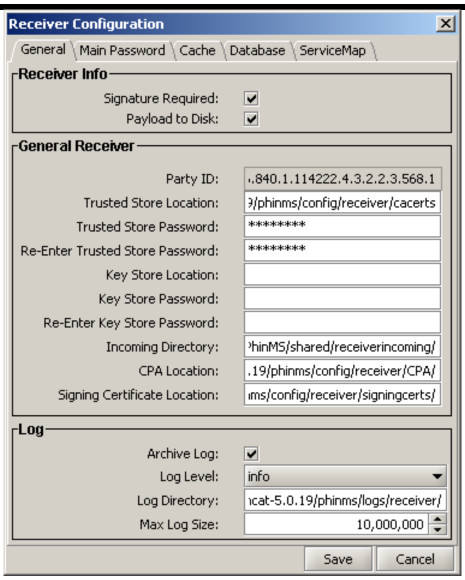
SET CONFIGURATION: Was successful! Please restart your application server for changes to take effect.

Figure 7.10. Successful Configuration

6. select **Restart**.

7.3 Configure Service Map

1. select **Rcv Cfg** displaying Figure 7.11,



Receiver Info

Signature Required: ☑
Payload to Disk: ☑

General Receiver

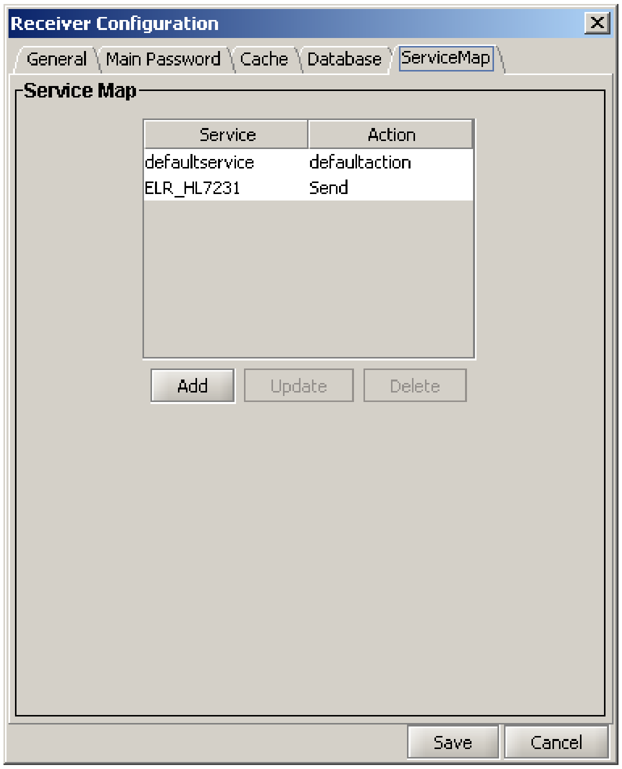
Party ID: ,.840.1.114222.4.3.2.2.3.568.1
Trusted Store Location: ɜ/phinms/config/receiver/cacerts
Trusted Store Password: ********
Re-Enter Trusted Store Password: ********
Key Store Location:
Key Store Password:
Re-Enter Key Store Password:
Incoming Directory: ›hinMS/shared/receiverincoming/
CPA Location: .19/phinms/config/receiver/CPA/
Signing Certificate Location: ıms/config/receiver/signingcerts/

Log

Archive Log: ☑
Log Level: info
Log Directory: ıcat-5.0.19/phinms/logs/receiver/
Max Log Size: 10,000,000

Figure 7.11. Receiver Configuration

2. select **Service Map** displaying Figure 7.12,

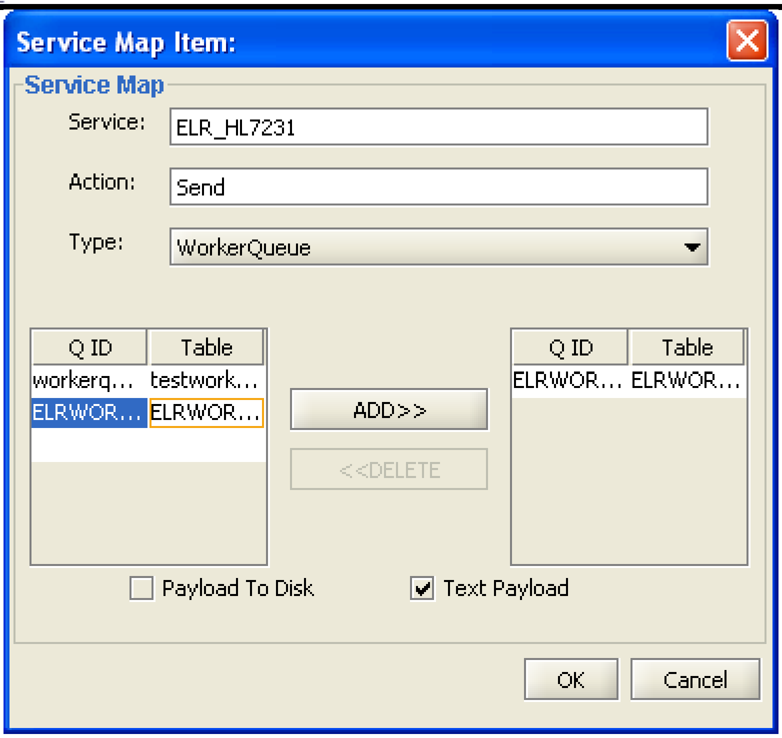


Service Map

Service	Action
defaultservice	defaultaction
ELR_HL7231	Send

Figure 7.12. Service Map Receiver Configuration

3. click **Add**, displaying Figure 7.13,



Service: ELR_HL7231

Action: Send

Type: WorkerQueue

Q ID	Table
workerq...	testwork...
ELRWOR...	ELRWOR...

Q ID	Table
ELRWOR...	ELRWOR...

□ Payload To Disk ☑ Text Payload

Figure 7.13. Service Map Item

4. enter the following parameters:
   - Service: **ELR_HL7231**,
   - Action: **Send**,
   - Type: **WorkerQueue** opening the service map item,

Note: The Service and Type displayed in Figure 7.13 could use different terms depending on the program used.

5. highlight **ELRWORKERQUEUE QID**, click **Add** moving the Q ID to the right,
6. check **Text Payload**,

Note: When Payload to Disk is checked the incoming payload is written to disk instead of to the database field. In this case the name of the local file on disk is stored in the WorkerQ table. When Text Payload is checked, the payload is written to the **payloadTextContent** field. When Text Payload is not checked, the payload is written to the **payloadBinaryContent** field in the WorkerQ.

7. click **OK**, and
8. click **Save** returning to the PHINMS 2.7.00 SP1 Console.

Send a dummy message to test the setup. Verify the TransportQ and WorkerQ data fields are correct.

8.0 RECOMMENDED PHINMS PORTS

Table 2 and Table 3 list the recommended ports for the PHINMS Sender and Receiver respectively. Table 4 displays the recommended Receiver ports for Web Logic. Table 5 lists the ports recommended for Stunnel. The ports for IPSec are shown in Table 6.

Note: When the port is used from Table 4, the port shown in Table 5 is not required and vice versa.

PORT	INBOUND/OUTBOUND	TYPE	REQUIRED	DESCRIPTION
443	Outbound	TCP	Yes	Makes a SSL connection to Receiver at CDC or other public health organizations.
5088	Outbound	TCP	No	Makes a connection to the CDC Ping Server. This connection is not required to make the PHINMS application work. It allows the user to test the application.
389	Outbound	TCP	No	Makes a LDAP call to the Verisign LDAP Server allowing the user to download Public Key. When using the CDC to download the Public Key, it is not necessary to open port 389.

Table 2. Sender Ports

PORT	INBOUND/OUTBOUND	TYPE	REQUIRED	DESCRIPTION
443	Inbound	TCP	Yes	Makes a SSL connection to receive traffic from the internet to the DMZ Proxy Server.

Table 3. IIS Proxy Server Port

PORT	INBOUND/OUTBOUND	TYPE	REQUIRED	DESCRIPTION
7002	Inbound	TCP	Yes	Makes a SSL connection from proxy server to Receiver running on Web Logic server using ISAPI Plug-in. (Assuming Web Logic is configured to run SSL on 7002.)

Table 4. Web Logic Server Receiver Port

PORT	INBOUND/OUTBOUND	TYPE	REQUIRED	DESCRIPTION
8009	Inbound	TCP	Yes	Makes a connection on the Proxy Server and the PHINMS Receiver Server to receive AJP13 traffic from the Proxy Server.

Table 5. Receiver Using Stunnel Ports

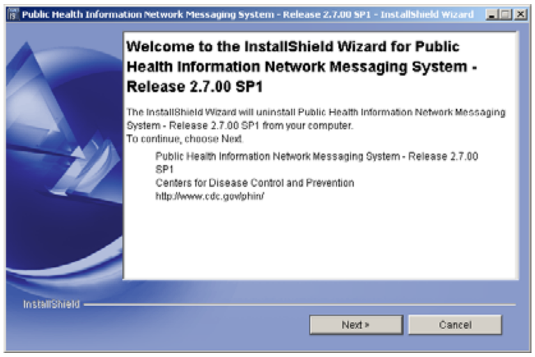
PORT	INBOUND/OUTBOUND	TYPE	REQUIRED	DESCRIPTION
500	Inbound/Outbound	UDP	Yes	Makes a connection between the Proxy Server and the PHINMS Receiver Server to allow ISAKMP traffic to be forwarded.
50	Inbound/Outbound	IP	Yes	Makes a connection between the Proxy Server and the PHINMS Receiver Server to allow Encapsulating Security Protocol (ESP) traffic to be forwarded to setup IPSEC.
51	Inbound/Outbound	IP	Yes	Makes a connection between the Proxy Server and the PHINMS Receiver Server to allow Authentication Header (AH) traffic to be forwarded to setup IPSEC.
8009	Inbound	TCP	Yes	Makes a connection on the PHINMS Receiver Server to receive AJP13 traffic from the Proxy Server.

Table 6. Receiver Using IPSEC

9.0 UNINSTALL PHINMS 2.7.00 SP1

Complete the following steps to uninstall PHINMS 2.7.00 SP1:

1. select **Start** > **Programs** > **PHINMS** > **Uninstall PHINMS** displaying Figure 8.1,


Public Health Information Network Messaging System - Release 2.7.00 SP1 - InstallShield Wizard
InstallShield
Next >
Cancel

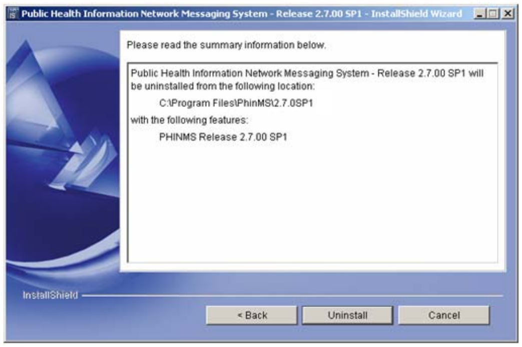
Welcome to the InstallShield Wizard for Public Health Information Network Messaging System - Release 2.7.00 SP1

The InstallShield Wizard will uninstall Public Health Information Network Messaging System - Release 2.7.00 SP1 from your computer.
To continue, choose Next.

Public Health Information Network Messaging System - Release 2.7.00 SP1
Centers for Disease Control and Prevention
http://www.cdc.gov/phin/

Figure 8.1. Uninstall Welcome

2. click **Next** displaying Figure 8.2,


Public Health Information Network Messaging System - Release 2.7.00 SP1 - InstallShield Wizard
InstallShield
< Back
Uninstall
Cancel

Please read the summary information below.

Public Health Information Network Messaging System - Release 2.7.00 SP1 will be uninstalled from the following location:

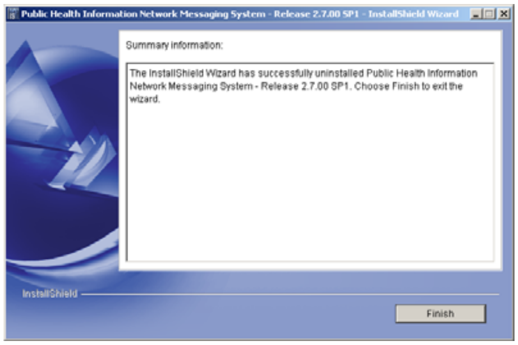
C:\Program Files\PhinMS\2.7.0SP1

with the following features:

PHINMS Release 2.7.00 SP1

Figure 8.2. Uninstalled Summary

3. click **Uninstall** displaying Figure 8.3, and


Public Health Information Network Messaging System - Release 2.7.00 SP1 - InstallShield Wizard
InstallShield
Finish

Summary information:

The InstallShield Wizard has successfully uninstalled Public Health Information Network Messaging System - Release 2.7.00 SP1. Choose Finish to exit the wizard.

Figure 8.3. Successful Uninstall

4. click **Finish**.

10.0ADDITIONAL FEATURES

10.1 Export CPA

PHINMS 2.7.00 SP1 allows the user to export the Collaboration Protocol Agreement (CPA) directly from the PHINMS 2.7.00 SP1 Console. Complete the following steps to export the CPA:

1. open the **PHINMS 2.7.00 SP1 Console**, select **Tools**, **CPA**, **Export CPA**,
2. select the **Route(s)** to export, click **Export Selected Routes**,
3. select a **folder** to store the exported CPA, and
4. select **Open** and
5. a message will indicate a successful export, click **OK**.

10.2 Import CPA

PHINMS 2.7.00 SP1 allows the user to import the CPA directly from the PHINMS 2.7.00 SP1 Console. Complete the following steps to import the CPA:

1. open the **PHINMS 2.7.00 SP1 Console**, select **Tools**, **CPA**, **Import CPA**,
2. select the **CPA** to import,
3. select **Open**, and
4. a message will indicate a successful import click **OK**.

10.3 View Receiver Logs

The Receiver Logs stores information on the status of received messages and can be viewed directly from the PHINMS 2.7.00 SP1 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 2.7.00 SP1 Console**, select **Tools**, **Logs**, **View Receiver Logs**,
2. select a specific **Date/Time** log, select **View**, and
3. the log will display in a text format allowing the user to view the status.

10.4 View Sender Logs

The Sender Logs stores information on the status of send messages and can be viewed directly from the PHINMS 2.7.00 SP1 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 2.7.00 SP1 Console**, select **Tools, Logs**, **View Sender Logs**,
2. select a specific **Date/Time** log, select **View**, and
3. the log will display in a text format allowing the user to view the status.

10.5 Import Configuration

When an identical configuration is required for another computer, the application is able to import the configuration files eliminating the need to configure the other computer. Complete the following steps to import the PHINMS 2.7.00 SP1 configuration files:

Note: Before a configuration can be imported, the configuration must be exported to a disk or shared drive. Section 9.6 explains the export steps.

1. select **Tools**, **Configuration**, **Import Configuration**,
2. confirm overwrite current settings by clicking **OK** to proceed,
3. complete the following fields,
   - **Backup Location** - required

Note: The backup location is the place the zip file was stored when the configuration files were exported.

   - **Domain Name** - required,
   - **Party ID** - required,
   - **Key Store**,
   - **Key Store Password**,
   - **Re Enter Key Store Password**,
4. click **OK**, and
5. a message will indicate a successful configuration import, click **OK**.

Note: Setting for various resources (e.g., database), database connection parameters, and JDBS files will still need to be reviewed and/or modified.

10.6 Export Configuration

When a configuration is required for another computer, the application is capable of exporting the configuration files eliminating the need to manually configure the settings. Complete the following steps to export the PHINMS 2.7.00 SP1 configuration files:

1. select **Tools**, **Configuration**, **Export Configuration**,
2. navigate to a location to store the exported configuration zip file, enter a **File Name**,
3. select **Open**, and
4. a message will indicate a successful export, click **OK**.

10.7 Import Trusted Certificate

A Trusted Certificate consists of a public key and a private key. The public key is used to encrypt information and the private key is used to decipher it. When a browser points to a secured domain, a secure sockets layer handshake authenticates the server and the client. It establishes an encryption method and a unique session key. Then a secure session guarantying message privacy and message integrity can begin.

The user can now import the Trusted Certificate directly from the PHINMS 2.7.00 SP1 Console. Complete the following steps to import the Trusted Certificate:

1. open the **PHINMS 2.7.00 SP1 Console**, select **Tools**, **Import Trusted Cert**,
2. navigate to the location the Trusted Certificate is stored,
3. select the **Trusted Certificate** (.cer or .pem file) to import, and
4. click **Open**, successfully importing the Trusted Certificate into the Sender's trusted CA certificate store.

10.8 Import JDBC JAR Files

JDBC Jar Files are able to be imported directly from the PHINMS 2.7.00 SP1 Console. Complete the following steps to import the three (3) JDBC Jar Files:

1. open the **PHINMS 2.7.00 SP1 Console**, select **Tools**, **Import JDBC Jar Files**,
2. locate and select **msbase.jar**, **mssqlserver.jar**, **msutil.jar**,

Note: The JDBC Jar files referenced in Step 2 above are for a SQL server, for other types of servers the JDBC Jar file names may vary.

3. click **Open**,
4. a message will indicate a successful import, click **OK**, and
5. restart **PHINMS 2.7 Apache Tomcat** service.

10.9 Change Login Password

PHINMS 2.7.00 SP1 allows the user to change the Console login password. Complete the following steps to successfully change the login password:

1. open the **PHINMS 2.7.00 SP1 Console**, select **Tools**, **Change Login Password**,
2. enter the **Old Console Password**, **New Console Password**, **Re-Enter New Console Password**, click **Change Password**,
3. click **OK**, and
4. restart **PHINMS 2.7 Apache Tomcat** service.

10.10 System Alarms

PHINMS 2.7.00 SP1 contains system alarms for the Sender and Receiver. This feature allows the user to acknowledge and enter a resolution for each alarm. View and resolve the alarms by completing the following steps:

1. open the **PHINMS 2.7.00 SP1 Console**, select **Alarms**, **Sender Alarms** or **Receiver Alarms**,

2. click the **Message** to view the associated information,
3. click **Enter Resolution**,
4. enter **Your Name** and **Your Comments** once the error has been resolved which stores the resolution, and
5. click **Save**.

10.11 Sender Alarms Configuration

Sender can receive and email alarm notifications. Configure the Sender alarms by completing the following steps:

1. open the **PHINMS 2.7.00 SP1 Console**, select **Configuration Alarms**, **Sender Alarms Configuration**,
2. check **Report Alarms**,
3. check **E-Mail Alarms** if required, proceed to step 4, if not required, proceed to step 7,
4. complete the following fields,
    - **SMTP Server -** required,
    - **User Name**,
    - **User Password**,
    - **Re Enter User Password**,
    - **From Address** - required,
5. enter an **email address**,
6. click **Add** placing the email address in the E-Mail Notification List,
7. click **OK**,
8. a message will indicate a successful save, click **OK**, and
9. click the SP1 2.7.00 SP1 Console **Restart** button.

10.12 Receiver Alarms Configuration

Receivers can receive and email alarm notifications. Configure the Receiver alarms by completing the following steps:

1. open the **PHINMS 2.7.00 SP1 Console**, select **Configuration Alarms**, **Sender Alarms Configuration**,
2. check **Report Alarms**,
3. check **E-Mail Alarms** if required, proceed to step 4, if not required, proceed to step 7,
4. complete the following fields,
    - **SMTP Server** - required,
    - **User Name**,

- **User Password**,
- **Re Enter User Password**,
- **From Address** - required,

5. enter an **email address**,
6. click **Add** placing the email address in the E-Mail Notification List,
7. click **OK**,
8. a message will indicate a successful save, click **OK**, and
9. click the 2.7.00 SP1 Console **Restart** button.

10.13 Folder Based Polling

This feature makes it much easier to applications to interface with PHINMS 2.7.00 SP1. Senders can now configure the Console for Folder Based Polling. Folder Based Polling 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 2.7.00 SP1 Console**, select **Snd Cfg**, select the **Sender Info tab**,
2. check **Folder Based Polling**,
3. click **Save**,
4. click **OK**,
5. click the PHINMS 2.7.00 SP1 Console **Restart** button,
6. create the following three (3) folders in any directory:
    - **Outgoing** - used to store messages to be sent,
    - **Processed** - regional file which messages have been processed, and
    - **Acknowledgement** - stores the message receipt from the Receiver.