PHINMS
Alarms

Version: 1.0.0

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

Date: January 11, 2008

VERSION HISTORY

VERSION #	IMPLEMENTER	DATE	EXPLANATION
1.0.0	Chris Childs	01/11/08	Create version 1.0.0.

EXECUTIVE SUMMARY

The Public Health Information Network Messaging System (PHINMS) is a secure and reliable data transport system built to open standards. PHINMS is the primary data transport mechanism for the Centers for Disease Control and Prevention (CDC) Public Health Information Network (PHIN).

This document provides an analysis of the alarms that PHINMS 2.7 SP1 will alert when there is any error during transport of a message or receiving of a message.

TABLE OF CONTENTS

1.0 PHINMS 2.7SP1 ALARMS

1.1 Database Errors

The table below displays the database errors PHINMS 2.7SP1 flags under the Alarms.

TYPE	DESCRIPTION
DBError01	JDBC Driver class was not found, missing JDBC Driver. The class definition is correct., Copy JDBC Driver Jar files for [1] to [2] and restart PHINMS service.
DBError02	JDBC Driver class [1] was not found, incorrect JDBC Driver class definition. Please correct the JDBC Driver class definition based on the database type. Select the Restart button on the PHINMS console.
DBError03	JDBC URL is not correct. An example of correct JDBC URL: [1] for [2] database.
DBError04	Invalid database host name or unreachable host machine [1] specified by JDBC URL, Contact the administrator for the correct database host name.;
DBError05	PHINMS could not connect to database server at [1]:[2]. Either the database server is not running or an incorrect database host name and/or port number exists.
DBError06	Invalid database user name and/or password. Contact the database administrator for the correct JDBC user name and password.
DBError07	Table does not exist or an invalid table name. Create a table or change the table name in the database.
DBError08	Insert is taking longer than five (5) minutes or a failure has occurred. Detect any table and/or row locking.
DBError09	A generic database error has occurred. The Java exception message is provided as: [1]. Please contact the database administrator to ensure: (1) the user connecting to the database server has the following permissions: select, delete, and insert, and (2) the table name and schema are correct.
DBError10	ODBC data source name: [1] was not found. Enter the correct ODBC data source name.

1.2 Network Error

The table below displays the network errors PHINMS 2.7SP1 flags under the Alarms.

TYPE	DESCRIPTION
NetError01	The Receiver is not up at [1]:[2] or the firewall is blocking outgoing requests. (1) Correct the receiver host and/or port. (2) Unblock the firewall which is preventing outgoing requests.
NetError02	Incorrect protocol. Use HTTP or HTTPS.
NetError03	Authentication failed. Receiver requires client certificate. Acquire a client certificate to authenticate against the Receiver.
NetError04	Authentication failed. Receiver side: [1]'s SSL certificate was not trusted. Import Receiver’s root CA certificate into the Sender’s trusted Keystore file.

NetError05	Authentication failed. Form based authentication: incorrect user name and/or password. Set the correct user name and/or password for form-based authentication (used in custom authentication).
NetError06	Authentication failed. Incorrect Web proxy user name and/or password for proxy server [1]:[2]. Set the correct user name and/or password for web proxy."};
NetError07	Connection failed. Incorrect Web proxy host and port: [1]:[2] or the web proxy is down. Set the correct host:port for web proxy and verify the web proxy is up and running.
NetError08	Access was denied by [1]://[2]:[3]. HTTP Error 403 – Forbidden (1) SDN activity is not assigned. (2) Client certificate was not trusted by Receiver proxy server.
NetError099	Access was denied by [1]://[2]:[3]. (1) Passphrase is incorrect. (2) The certificate (.pfx file) was not exported correctly. Check the checkbox \"Include all certificates in the certification path if possible\ when exporting certificate from IE browser.
NetError10	Client certificate Keystore (.pfx file) was not found at location: [1] Client Keystore (.pfx) path is incorrect or doesn't exist. Copy the .pfx file into the correct location.
NetError11	Can not load the client certificate Keystore ([1]). (1) Correct the Keystore password. (2) Use pfx format for the Keystore.
NetError12	"Trusted Keystore was not found at: [1]", "Correct the Trusted Keystore path."}
NetError13	Invalid Trusted Keystore (cacerts file) password. Correct the Trusted Keystore password.
NetError14	Access was denied by [1]://[2]:[3]. (1) Client certificate was not trusted by the Receiver. (2) The certificate (.pfx file) was not exported correctly. Check the checkbox \"Include all certificates in the certification path if possible\" when exporting certificate from IE browser.
NetError15	Sender can not send a message: [1] in the last [2] seconds. Contact the Receiver administrator to resolve the problem.
NetError16	Receiver certificate Keystore (.pfx file) was not found at location: [1] Certificate Keystore path (.pfx) is incorrect or doesn't exist. Copy the .pfx file into the correct location.
NetError17	Receiver returns a HTTP 500 error. Receiver is having problem serving your message request.Contact the Receiver administrator to resolve the problem.

1.3 Messaging Error

The table below displays the messaging errors PHINMS 2.7SP1 flags under the Alarms.

TYPE	DESCRIPTION
MSGError01	Invalid service: [1] action: [2] used in the outgoing message. Correct service/action pair for the outgoing message.
MSGError02	Inconsistent error. Import Sender’s CPA file into the PHINMS Receiver.
MSGError03	Insert failure. Message was received, but was not inserted into database.
MSGError04	Security failure: Encryption certificate for ([1]) expired at [2] 1) Renew the Receiver's decryption certificate or (2) when using \"CertificateURL\", get the renewed encryption certificate from the Receiver. (3) Use LDAP search.
MSGError05	Security failure: certificate was not found using LDAP proxy, route [1] doesn't exist.

	Set the LDAP proxy to use the correct route.
MSGError06	Security failure: certificate was not found using LDAP proxy, service/action: [1]/[2] are incorrect. Set the LDAP proxy search service/action pair correctly. Default is LDAP/search.
MSGError07	Security failure: certificate was not found using LDAP proxy (1) Three LDAP search related attributes are incorrect. Server address: [1] Base DN, [2] Common Name, [3] or (2) LDAP server is down.
MSGError08	Security failure: certificate was not found LDAP lookup without using LDAP proxy. Incorrect LDAP server: [1]:[2] or outbound port [3] was blocked. Unblocked the outbound LDAP port or start using LDAP proxy.
MSGError09	Security failure: certificate was not found at certificate URL: [1] Correct the certificate URL to point to the encryption certificate.
MSGError10	Security failure: certificate was not found LDAP search attributes or certificate URL are not set.
MSGError11	Invalid route: [1] "\"RouteInfo\" for this message is not a valid route.
MSGError12	Payload file [1] was not found", "Correct the local payload file name.
MSGError13	Receiver is taking too much time ([1] seconds) to process a message, which is more than 600 seconds (StuckThreadMaxTime) causing the message to abort. Contact the Receiver administrator.
MSGError14	SecurityFailure/cert not found using LDAP proxy, service/action: [1]/[2] are incorrect. Set the LDAP proxy search service/action pair correctly. Default is LDAP/search.

1.4 System Error

The table below displays the system errors PHINMS 2.7SP1 flags under the Alarms.

TYPE	DESCRIPTION
SYSError01	OutofMemory. System is running out of memory", "Need bump up the heap size.
SYSError02	Out of disk space. Need more disk space for save payload or logs.