

MDS PulseNET

Network Management System

Version 2.2

Enterprise

***An Enterprise Management Tool for GE MDS Products
and other IP-Connected Devices***

MDS 05-6567A01, Rev. A
FEBRUARY 2011



Digital Energy
MDS

Quest Copyright Notice

© 2011 Quest Software, Inc.
ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software, Inc.

The information in this document is provided in connection with Quest products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest products. EXCEPT AS SET FORTH IN QUEST'S TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software World Headquarters
LEGAL Dept
5 Polaris Way
Aliso Viejo, CA 92656
www.quest.com
email: legal@quest.com

Refer to our Web site for regional and international office information.

Patents

This product includes patent pending technology.

Trademarks

Quest, Quest Software, the Quest Software logo, Foglight, IntelliProfile, PerformaSure, Spotlight, StealthCollect, TOAD, Tag and Follow, Vintela Single Sign-on for Java, and vFoglight are trademarks and registered trademarks of Quest Software, Inc in the United States of America and other countries. For a complete list of Quest Software's trademarks, please see <http://www.quest.com/legal/trademark-information.aspx>. Other trademarks and registered trademarks are property of their respective owners.

Third Party Contributions

MDS PulseNET contains some third party components. For a complete list, see the License Credits page in `<INSTALLDIR>\docs\core\pdf`.

About Quest Software, Inc.

Quest Software simplifies and reduces the cost of managing IT for more than 100,000 customers worldwide. Our innovative solutions make solving the toughest IT management problems easier, enabling customers to save time and money across physical, virtual and cloud environments. For more information about Quest go to www.quest.com.

About GE MDS

Over two decades ago, GE MDS began building radios for business-critical applications. Since then, we have installed thousands of radios in over 110 countries. To succeed, we overcame impassable terrain, brutal operating conditions and disparate, complex network configurations. We also became experts in wireless communication standards and system applications worldwide. The result of our efforts is that today, thousands of utilities around the world rely on GE MDS-based wireless networks to manage their most critical assets.

The majority of GE MDS radios deployed since 1985 are still installed and performing within our customers' wireless networks. That's because we design and manufacture our products in-house, according to ISO 9001 which allows us to control and meet stringent global quality standards.

Thanks to our durable products and comprehensive solutions, GE MDS is the wireless leader in industrial automation—including oil and gas production and transportation, water/wastewater treatment, supply and transportation, electric transmission and distribution and many other utility applications. GE MDS is also at the forefront of wireless communications for private and public infrastructure and online transaction processing. Now is an exciting time for GE MDS and our customers as we look forward to further demonstrating our abilities in new and emerging markets.

As your wireless needs change you can continue to expect more from GE MDS. We'll always put the performance of your network above all. Visit us at www.gemds.com for more information.

GE MDS ISO 9001 Registration

GE MDS adheres to the internationally-accepted ISO 9001 quality system standard.

To GE Customers

We appreciate your patronage. You are our business. We promise to serve and anticipate your needs. We will strive to give you solutions that are cost effective, innovative, reliable and of the highest quality possible. We promise to build a relationship that is forthright and ethical, one that builds confidence and trust.

Related Materials on the Internet—Data sheets, frequently asked questions, application notes, firmware upgrades and other updated information is available on the GE MDS Web site at www.gemds.com.

Manual Revision and Accuracy

This manual was prepared to cover a specific version of our product. Accordingly, some screens and features may differ from the actual version you are working with. While every reasonable effort has been made to ensure the accuracy of this guide, product improvements may also result in minor differences between the manual and the product shipped to you. If you have additional questions or need an exact specification for a product, please contact our Customer Service Team using the information at the back of this guide. In addition, manual updates can often be found on the GE MDS Web site at www.gemds.com.

Installation and Setup Guide

February 2011

Version 2.2

Table of Contents

Before Installing MDS PulseNET Enterprise	7
What Is MDS PulseNET Enterprise?.....	7
Planning Your Installation.....	8
High Availability Mode	8
Using the Embedded Database.....	9
Using an External Databases	10
Hardware Requirements and Guidelines	10
Installing PulseNET.....	11
Preparing to Install	11
Installing PulseNET	12
<i>To Install PulseNET.....</i>	<i>12</i>
PulseNET Server Start Up Page	24
To Install PulseNET in HA Mode.....	25
Next Steps	27
External Database Access for Remote Users	27
Manual Database Configuration	28
Importing a Network Security Certificate	31
Uninstalling PulseNET.....	33
Installing PulseNET FAQ.....	34
Running PulseNET.....	35
Initializing the Database	35
Tuning an External MySQL Database for PulseNET	35
Starting and Stopping PulseNET.....	38
Starting PulseNET	38
Running PulseNET as a Windows Service.....	40

6 | PulseNET
Installation and Setup Guide

Stopping PulseNET	41
Starting and Stopping the Server in High Availability Mode.....	41
Remote Monitor	43
Logging in to PulseNET	44
Running PulseNET FAQ.....	44
Index	49

Before Installing MDS PulseNET Enterprise

This guide provides instructions for installing and starting MDS PulseNET Enterprise.

This chapter provides you with setup information.

Important Before you begin, consult the *PulseNET Enterprise Release Notes*. That document contains important information about any late-breaking changes, as well as known and resolved issues.

What Is MDS PulseNET Enterprise?

MDS PulseNET Enterprise (PulseNET) is a software application used for monitoring devices in Industrial Communications (IC) networks. Each device PulseNET monitors serves a specific function in the network. These functions include acting as a bridge, router, access point, remote, etc. The devices are widely dispersed geographically and operate with very limited bandwidth restrictions.

PulseNET is intended for large-scale operations with a need to monitor up to 25,000 devices.

Planning Your Installation

Before you install PulseNET, ensure that you have the information you need, such as port numbers and the server name.

The following are the main stages involved in installing and configuring PulseNET:

Stage 1: Install the PulseNET server and configure the server and database.

Stage 2: If you are using the embedded database, start the PulseNET server and log in. If you are using an external database, install, configure, and initialize the database, and then start the PulseNET server and log in.

Note If you are using the embedded database, initialization is performed when you start the PulseNET server. If you are using an external database, the database must be initialized successfully before you can run the PulseNET server.

High Availability Mode

Before you install PulseNET, you need to determine if you are going to set up and run the PulseNET server in High Availability (HA) mode or as a standalone server. High Availability mode enables you to install multiple servers where one server is the primary server and the others are standby servers. If the primary server stops responding, then the responsibility is taken over by one of the standby servers in the HA cluster.

Configuring multiple servers using HA mode offers the following benefits:

- **Automatic restart:** The restart process (PulseNET HA Daemon) runs on the same host as the PulseNET server it is monitoring and monitors the state of the server. If the server stops responding or has a fatal error, then the restart process stops and restarts the server automatically. The process can also send out email notifications about various conditions of the server.
Note The default value for the restart process is five minutes (300 seconds). Machines with a slower processing speed take longer to reboot.
- **Standby Server:** To reduce outage times, a standby server instance is created (for a particular PulseNET server), and forms a partition. One server becomes the primary server and communicates with the agents, receives and processes data, and processes rules. All other servers are standby servers. If a primary server stops responding, one of the standby servers resumes service and becomes the primary server.

Considerations for running the PulseNET Management Server in HA mode

If you plan to run the PulseNET server in HA mode, there are certain considerations:

- Specific ports are required for the HA setup to work. These are:
 - Cluster Mcast Port
 - HA JNDI RMI Port
 - HA JNDI JNP Port
 - HA JRMP Invoker Port
 - HA Pooled Invoker Port
 - HA JNDI UDP Group Port

All of these ports must be set to the same values for all Servers in the HA cluster.

- Any system on which you are going to install a PulseNET component must be able to resolve itself and, if necessary, forward and reverse resolve all peers.
- By default, HA mode works only within the local subnet and uses UDP (User Datagram Protocol) for communication.
- In both High Availability Mode and Single Server Mode, the database must be running for PulseNET to operate. You may have to implement a combined database-backup and High Availability solution to achieve true failover of all components.
- A server running in HA mode can only use an external database.
- The PulseNET Agent Manager must be installed on a different machine than either of the PulseNET server instances.

Note In standalone mode, PulseNET uses a PulseNET Agent Manager that is embedded in PulseNET. In HA mode, the PulseNET Agent Manager must be remote in case the primary PulseNET server goes down.

Using the Embedded Database

PulseNET offers the option to use MySQL as an embedded database. The lifecycle of the embedded database matches that of the PulseNET server. If the server is stopped or started, the embedded database is automatically stopped or started.

Using an External Databases

An external instance of an Oracle database, a Microsoft SQL Server database, or MySQL with an InnoDB storage engine, can be used if your DBA has installed one. Please see the *Release Notes* for more information on the supported external databases.

Note The PulseNET server supports connection to the Microsoft SQL Server database only by means of SQL Server Authentication. Windows Authentication is not supported.

A setup with an external database has the advantage of using existing infrastructure. For setup, a remote administrator user/password is required that has rights to create users and tables in the user/temp tablespace. Remote administrator access must be granted.

Note Oracle databases must be configured to support Unicode characters. For example, you can use UTF-8 or UTF-16 to support Unicode.

Hardware Requirements and Guidelines

The hardware requirements to run PulseNET can vary, depending on the number of devices being monitored.

For the current hardware requirements, consult the *Release Notes*.

Running PulseNET requires:

- The PulseNET server
- The PulseNET database repository

Installing PulseNET

This chapter provides the instructions for installing PulseNET 2.2.

Note PulseNET should be installed on a dedicated machine.

Preparing to Install

The requirements for installing PulseNET are:

- A machine to host PulseNET. PulseNET should run on a dedicated machine because it must process and store large volumes of data.
 - Note** Ensure that a host name resolution and reverse lookup are confirmed prior to installing PulseNET.
- Administrator or root access to the machine.
- An administrator password for PulseNET. The user name and the default password (admin/admin) for the account can initially be used to log in to the browser interface and to use command-line interface options with root or administrator privileges. It is strongly recommended that you change the default password for this account.
- On Linux platforms, a user account on the machine where you are installing PulseNET.
- The IATEMPDIR or TEMP environment variable must be set to a location with sufficient space for installer self-extraction to meet the requirements described in the document available at:
<http://support.installshield.com/kb/view.asp?articleid=Q000054>
- If you are installing PulseNET with the embedded MySQL database on Linux, the PulseNET installer and PulseNET server must be able to write to the directory

where the MySQL socket is installed. By default, the MySQL socket is installed in the */tmp* directory (which is world-writable on Linux).

- If you are installing PulseNET with the embedded MySQL database on Linux, you must define the IPv4 entry for *localhost* in the */etc/hosts* file prior to installing PulseNET. If you do not do so, the installer cannot start the embedded database and the installation fails.

To prevent the installation from failing, add the following IPv4 entry for *localhost* in the */etc/hosts* file prior to installing PulseNET:

```
127.0.0.1 localhost.localdomain localhost
```

- If you are installing PulseNET on 64-bit Linux platforms, the 32-bit version of *libgcc*.rpm* must be installed for the PulseNET installer to run.
- Flexera Software, makers of the InstallAnywhere tool, recommend that you install as Administrator or use an account that is part of the Administrator group.

Installing PulseNET

Once all system requirements are in place, you are ready to install PulseNET. The installer prompts you to input data, and provides you with progress feedback during the installation process.

The PulseNET installation process offers two installation options:

- **Standard** — This option accepts all of the installer defaults, and installs a standalone instance of PulseNET and an embedded MySQL database.
- **Custom** — This option allows you to modify installer defaults, choose an external database type, and configure PulseNET to run in HA mode.

If you want to install PulseNET in HA mode, see “[To Install PulseNET in HA Mode](#)” on page 25. Otherwise, proceed to “[To Install PulseNET](#)” below.

The PulseNET installation process consists of the same basic steps for all supported platforms.

To Install PulseNET

Start the installation process by initiating the executable included on the PulseNET install media. Each installation screen includes a **Previous** button, allowing you to go back and adjust the information you have specified.

Step 1: Introduction

The Introduction screen provides an overview of the mechanics of the installation interface. Click **Next** after reading the contents of the Introduction screen.

Step 2: Transaction Product Agreement

- 1 Read the Transaction Product Agreement statement, and accept or decline the terms of the agreement.
- 2 If you select **I accept the terms of the License Agreement**, click **Next**.

Step 3: Select Installation

- 1 Choose **Standard Install** or **Custom Install**.

The standard option accepts all of the installer defaults, and installs a standalone instance of PulseNET and an embedded MySQL database. The custom option allows you to modify installer defaults, choose an external database type, and configure PulseNET to run in HA mode.

Note If PulseNET will be monitoring 2500 or more devices, it is strongly recommended that you use the 64-bit version of PulseNET with an external database.

- 2 Click **Next**.

Step 4: Choose Install Folder

- 1 Choose the location where you want to install PulseNET. You can accept the default location or click the **Browse** button to navigate to another location.
- 2 Click **Next**.

Step 5: Choose Shortcut Location

- 1 Choose the location where you want to create product icons. There are several options displayed:
 - **In a new Program Group:** Type the name of the group in the field.
 - **In an existing Program Group:** Use the menu to select an existing program group.
 - **In the Start Menu**
 - **On the Desktop**
 - **In the Quick Launch Bar**
 - **Other** (default): Browse your system for a shortcut location. Click the **Choose** button to enable the browser.
 - **Don't create icons**

Select the **Create Icons for all Users** check box to create shortcuts for all PulseNET users.

The screenshot shows the 'Choose Shortcut Location' dialog box. On the left is a navigation pane with the following items: Introduction, License Agreement, Choose Install Folder, Choose Shortcut Location (highlighted), Pre-Installation Summary, Installing..., Secure Server, Server Settings, Database Settings, Port Settings, and Install Complete. The main area is titled 'Where would you like to create product icons?' and contains the following options:

- In a new Program Group: PulseNET
- In an existing Program Group: Accessories
- In the Start Menu
- On the Desktop
- In the Quick Launch Bar
- Other: programs\GE MDS\PulseNET
- Don't create icons

At the bottom of the main area is a checkbox labeled 'Create Icons for All Users' which is currently unchecked. A 'Choose...' button is located next to the 'Other' text box. At the bottom of the dialog are three buttons: 'Cancel', 'Previous', and 'Next'.

- 2 Click **Next**.

Step 6: PulseNET Service

- 1 If you want to have PulseNET run as a Windows service (recommended), select **Enable PulseNET as a Service**.
Note This is not an option if you are installing PulseNET on Linux.
- 2 Click **Next**.

Step 7: Pre-Installation Summary

- 1 Review the installation information.
- 2 If you are satisfied with the parameters of your installation, click **Install**.
To make changes to the installation parameters, click **Previous**.

Step 8: Installing PulseNET 2.2

PulseNET installs files into the specified directory.

Step 9: Secure Server (HTTPS Only)

- 1 To run PulseNET in secure mode (HTTPS) only, select the **Secure Server (HTTPS Only)** check box.

Note To set up PulseNET to use HTTPS, you must also generate a key pair (security certificate) into the PulseNET keystore. For information about how to do this, see ["Importing a Network Security Certificate"](#) on page 31.

- 2 Click **Next**.

Switching to Secure Mode (HTTPS) After the PulseNET Installation

If you choose not to run PulseNET in secure mode and then at some point after the PulseNET installation you want to run PulseNET in secure mode, follow the steps below.

Note You must have the administrator role to perform the following steps.

To toggle HTTPS mode on or off after the PulseNET installation:

- 1 Ensure that the PulseNET Server is installed and running.
- 2 In the Command Prompt window (Windows) or the terminal window (Linux), switch to HTTPS mode using the following command:

```
fglcmd.bat -usr admin -pwd <adminpassword> -cmd HTTPS:Toggle  
-Mode enable
```

or

Switch out of HTTPS mode using the following command:

```
fglcmd.bat -usr admin -pwd <adminpassword> -cmd HTTPS:Toggle  
-Mode disable
```

- 3 Stop and then restart the PulseNET server. For instructions on how to stop and start the PulseNET Server, see ["Starting and Stopping PulseNET"](#) on page 38.

Note When in HTTPS mode, the user must access the server using port 8443. When not in HTTPS mode, the user can access the server using either port 8080 (HTTP) or port 8443 (HTTPS).

Step 10: PulseNET Mode

- 1 Choose the server startup mode. The options are **Standalone** or **HA (High Availability)**.

Important You cannot switch to High Availability mode after installing the PulseNET server.

Note A server running in HA mode can only use an external database.

- 2 If you choose **HA (High Availability)**:
 - In the **HA Partition** field, type the partition name. All servers set up in **HA (High Availability)** mode that you want to act as either primary or secondary servers for failover have to be configured with the same partition name.

Caution Servers with different partition names do not participate in the high availability setup.

- 3 Click **Next**.

Step 11: PulseNET Database Configuration

This step allows you configure the PulseNET database.

Note If you are configuring PulseNET to use an external database, the database must exist before you complete this step.

After you click **Next**, the installer creates the user (*pulsenet* is the default user ID) in the database and sets the appropriate permissions.

Important If the PulseNET server you are installing is configured to be part of an HA cluster, you must set **User ID**, **Password**, and **PulseNET Database** to the same values as those used for the other PulseNET servers that share the same HA partition name.

- 1 In the PulseNET Database Account **User ID** field, accept the default user ID (*pulsenet*) or type an alternate one. This is the name for the PulseNET user that you are creating. PulseNET uses this account to store data in the database.
With an external Oracle database, the **User ID** is used for the database name.
- 2 In the PulseNET Database Account **Password** field, accept the default password (*pulsenet*) or type an alternate one.
- 3 In the PulseNET Database Account **Retype Password** field, accept the default (*pulsenet*) or, if you have provided an alternate password in [step 2](#), retype the password for verification.
- 4 From the **DB Configuration** list, choose **Embedded** or **External**. For the embedded database instructions, see [Embedded Database](#) below. For the external database instructions, see [External Database](#) below.

Note If PulseNET will be monitoring 2500 or more devices, it is strongly recommended that you use the 64-bit version of PulseNET with an external database.

Note Because an external database is required for an HA configuration, the **DB Configuration** list is disabled if you selected HA as the server startup mode in “[Step 10: PulseNET Mode](#)” on page 17.

Embedded Database

Database Configuration

Introduction
License Agreement
Choose Install Folder
Choose Shortcut Location
Pre-Installation Summary
Installing...
Secure Server
Server Settings
Database Settings
Port Settings
Install Complete

Database Account:
User ID: pulsenet
Password: ****
Retype Password: ****

DB Configuration: Embedded

Database Port: 13306
DB Administrator Password: ****
Retype DB Administrator Password: ****

InstallAnywhere

Cancel Previous Next

- 1 Accept the default port (13306) or type an alternate **Database Port**.
- 2 In the **DB Administrator Password** field, accept the default password provided (*pulsenet*) or type an alternate one.
- 3 In the **Retype DB Administrator Password** field, accept the default (*pulsenet*) or, if you have provided an alternate password, retype the password for verification.
- 4 Click **Next**. A progress box appears as the embedded database is installed.

External Database

Note For information about granting remote users access to an external MySQL or Oracle database, see [“External Database Access for Remote Users”](#) on page 27.

Important If you are installing a secondary PulseNET instance to be part of an HA cluster, you already configured the database when you installed the primary PulseNET instance. Do not configure the database again; it could cause the installation to fail. Select the **Setup DB: Later (manually)** option and click **Next**.

Important If you select the **Setup DB: Later (manually)** option, database initialization scripts are placed in the `<pulsenet_home>\scripts\sql` directory. These scripts contain sensitive information and should be deleted.

If the PulseNET server you are installing is configured to be part of an HA cluster, you must also configure it to connect to the same database instance as all other members of the cluster. This typically means that you set **DB Type**, **DB Host**, **DB Port** or **Instance** and **DB Name** or **SID** to the same values as those used for the other members. In some rare cases, certain settings might be different. For example, the value for **DB Host** might be different if there is a firewall between the database and certain members of the cluster in your environment.

- 1 Choose a database type from the **DB Type** list.
 - Note** If you install and configure a MySQL database instance as an external database and this instance is to run on a different machine than the one hosting the server, choose the **MySQL** option to make the database accessible remotely.
- 2 In the **DB Host** field, type the database host name or IP address (*localhost* is the default name).
- 3 In the **DB Port** or **Instance** field, specify a port number or accept the default. This is the TCP/IP port on which the database communicates with the PulseNET server. The external database needs to be configured to communicate on this port.
 - Note** If you are configuring a Microsoft SQL Server, you can enter the database instance name here instead of the port number. This is name of the SQL Server instance to which you want the PulseNET server to connect.
- 4 In the **DB Name** or **SID** field, type the name of the database (*pulsenet* is the default name) if you are configuring a MySQL or SQL Server database. Type the service ID for the database if you are configuring an Oracle database.
- 5 Select one of the following **Setup DB** options:
 - **Now**
 - **Later (manually)**
 - Note** If you select **Later (manually)**, you must manually configure the database after the installation is complete and prior to starting the PulseNET server. See "[Manual Database Configuration](#)" on page 28 for information. This is not recommended.
- 6 If you selected **Now** in step 5, type the **Database Administrator Account User ID** and **Password**.
 - Caution** The Database Administrator Account User ID cannot be the same as the PulseNET Database Account User ID.
 - Caution** If the PulseNET server you are installing is configured to be part of an HA cluster, you must set the **Database Administrator Account User ID** and **Password** to the same values as those used for the other PulseNET servers that share the same HA partition name.
- 7 **Optional.** If you are configuring an Oracle database, you can click the **Advanced** button to configure Oracle tablespace information at this time. The values you specify in this dialog are referenced in the *storage-config.xml* file. See the Oracle documentation for more information about Oracle tablespaces.

Oracle Tablespace Configuration

Configuration Tablespaces

Data: [USERS] Index: [USERS] Lob: [USERS]

Observation Tablespaces

Data	Index	Lob

Add Edit Delete Done

Note Check with your database administrator for information on how to correctly assign tablespace names.

It is recommended that you create a PulseNET label for Data, Index, and Objects.

8 Click **Next**.

If a database schema already exists, the PulseNET Database Found screen appears. This screen allows you to keep your existing data, create a new database, or select a different database.

Step 12: PulseNET Ports Configuration

- 1 Configure the server ports. The PulseNET Ports Configuration screen displays default ports that you can assign.
- 2 If you want to revert to the default values, click **Defaults**.
- 3 Click **Next**.

Note If there are any port assignment conflicts, an error message dialog box appears. You can either click **Review Ports** if you want to return to the PulseNET Ports Configuration screen to configure the conflicting port(s), or choose **Ignore and Continue** to continue with the installation without resolving the port conflicts. Choose one of these options to continue.

Please enter the port assignments.	
Cluster Multi-cast Port:	45566
HTTP Port:	8080
HTTPS Port:	8443
JNDI RMI Port:	1098
JNDI JNP Port:	1099
JRMP Invoker Port:	4444
Pooled Invoker Port:	4445
Unified Invoker Port:	4448
Corba ORB Port:	3528

Defaults

InstallAnywhere

Cancel Previous Next

Step 13: Install Complete

Click **Done** to complete the installation process.

PulseNET Server Start Up Page

If you installed PulseNET as a service, on startup PulseNET launches the PulseNET Server Start Up page in a Web browser.

If you don't see the status below or status hasn't been updated in a while, please click [here](#) to refresh.

MDS PulseNET Server Start Up

Status: Cartridges enabled: Core-Compatibility-5_5_9

Services started: 173
Cartridges enabled: 9

Main Services	Other Services
<input checked="" type="checkbox"/> Action	<input type="checkbox"/> Cartridge StartUp Spring Bootstrap
<input checked="" type="checkbox"/> Agent Manager	<input type="checkbox"/> Nitro Dyn Data Source Deployer
<input checked="" type="checkbox"/> Alarm	<input checked="" type="checkbox"/> (action=migrate_agent)
<input checked="" type="checkbox"/> Cartridge	<input checked="" type="checkbox"/> (action=migrate_data)
<input checked="" type="checkbox"/> Cartridge StartUp	<input checked="" type="checkbox"/> (action=migrate_dcim)
<input checked="" type="checkbox"/> Database Lifecycle	<input checked="" type="checkbox"/> (deployer=CDIDeployer)
<input checked="" type="checkbox"/> Denotation	<input checked="" type="checkbox"/> (handler=AdapterExtension)
<input checked="" type="checkbox"/> Diagnostic	<input checked="" type="checkbox"/> (handler=AgentAdapter)
<input checked="" type="checkbox"/> Federation Connection Manager	<input checked="" type="checkbox"/> (handler=Branding)
<input checked="" type="checkbox"/> Incident	<input checked="" type="checkbox"/> (handler=Cartridge)
<input checked="" type="checkbox"/> Licensing	<input checked="" type="checkbox"/> (handler=CcdRecording)
<input checked="" type="checkbox"/> Query	<input checked="" type="checkbox"/> (handler=CommandLine)
<input checked="" type="checkbox"/> Registry	<input checked="" type="checkbox"/> (handler=F4MigrationBaseline)
<input type="checkbox"/> Remote Access	<input checked="" type="checkbox"/> (handler=Installer)
<input checked="" type="checkbox"/> Rule	<input checked="" type="checkbox"/> (handler=JBoss)
<input checked="" type="checkbox"/> Schedule	<input checked="" type="checkbox"/> (handler=Jar)
<input checked="" type="checkbox"/> Scripting	<input checked="" type="checkbox"/> (handler=Localization)
<input checked="" type="checkbox"/> Security	<input checked="" type="checkbox"/> (handler=MonitoringPolicy)
<input checked="" type="checkbox"/> Topology Loader	<input checked="" type="checkbox"/> (handler=OnlineHelp)
<input checked="" type="checkbox"/> Topology Persistence	<input checked="" type="checkbox"/> (handler=PersistentCartridgeLifecycle)
<input checked="" type="checkbox"/> Web Server	<input checked="" type="checkbox"/> (handler=SpringJar)
	<input checked="" type="checkbox"/> (handler=TestError)
	<input checked="" type="checkbox"/> (handler=TopologyTypes)
	<input checked="" type="checkbox"/> (handler=WCF)
	<input checked="" type="checkbox"/> (handler=WcfJar)
	<input checked="" type="checkbox"/> Action Thread Pool
	<input checked="" type="checkbox"/> Adapter Config Provider
	<input checked="" type="checkbox"/> Adapter Registry
	<input checked="" type="checkbox"/> Agent Adapter Tasks Quartz Scheduler
	<input checked="" type="checkbox"/> Agent Aware Credential Client Manager
	<input checked="" type="checkbox"/> Agent Config Diagnostic Service
	<input checked="" type="checkbox"/> Agent Config Provider
	<input checked="" type="checkbox"/> Agent Event Producer
	<input checked="" type="checkbox"/> Agent Framework Monitor
	<input checked="" type="checkbox"/> Agent Lifecycle Manager
	<input checked="" type="checkbox"/> Agent Management Quartz Scheduler
	<input checked="" type="checkbox"/> Aggregate Alarm Notification Monitor
	<input checked="" type="checkbox"/> Distributed Persistence Cache
	<input checked="" type="checkbox"/> Dynamic Model
	<input checked="" type="checkbox"/> Dynamic Model Quartz Scheduler
	<input checked="" type="checkbox"/> Dynamic Property Monitor
	<input checked="" type="checkbox"/> Email Alarm Notifier
	<input checked="" type="checkbox"/> Email Sender
	<input checked="" type="checkbox"/> Env Complexity Estimator
	<input checked="" type="checkbox"/> Event
	<input checked="" type="checkbox"/> Extension Registry
	<input checked="" type="checkbox"/> FSM Alarm Filter
	<input checked="" type="checkbox"/> Federation Config
	<input checked="" type="checkbox"/> Federation MBean Monitor
	<input checked="" type="checkbox"/> Foglight4XML Config AgentTransformer
	<input checked="" type="checkbox"/> Foglight4Migration
	<input checked="" type="checkbox"/> Groovy Data Source Manager
	<input checked="" type="checkbox"/> HA Membership
	<input checked="" type="checkbox"/> Health Check
	<input checked="" type="checkbox"/> High Freq Internal JVM Monitor
	<input checked="" type="checkbox"/> High Freq MBean Monitor
	<input checked="" type="checkbox"/> Historic Data Cache
	<input checked="" type="checkbox"/> Installer Repository
	<input checked="" type="checkbox"/> Load Estimator
	<input checked="" type="checkbox"/> Localization
	<input checked="" type="checkbox"/> Log Monitor
	<input checked="" type="checkbox"/> Low Freq Internal JVM Monitor
	<input checked="" type="checkbox"/> Low Freq MBean Monitor
	<input checked="" type="checkbox"/> Memory Load Sensor
	<input checked="" type="checkbox"/> Metric Export
	<input checked="" type="checkbox"/> Metric Handler
	<input checked="" type="checkbox"/> Monitor Quartz Scheduler
	<input checked="" type="checkbox"/> Nitrogen Data Transform Factory
	<input checked="" type="checkbox"/> Observation Index Cache
	<input checked="" type="checkbox"/> Observation Imbalancer
	<input checked="" type="checkbox"/> Oracle Database Monitor
	<input checked="" type="checkbox"/> Persistence
	<input checked="" type="checkbox"/> Persistence Config
	<input checked="" type="checkbox"/> Persistence Policy Quartz Scheduler

This page provides information about the status of PulseNET as it starts up, such as:

- The number of services that have started and internal cartridges that are enabled.
- The latest status of PulseNET as it starts.
- A list of the PulseNET services that are starting. As shown in the image above, services listed in grey have not yet started, services listed next to a blue circle are starting, and services listed next to a green square with a check mark have started.
- A link to the PulseNET login page (once startup is complete). Click the link to access the PulseNET login page. For instructions on how to log in to PulseNET, see the *PulseNET Quick Start Guide*.

The information on the page is updated as PulseNET starts. The page also includes a link that allows you to refresh the page.

To Install PulseNET in HA Mode

This section describes how to install PulseNET in HA mode.

Note If you intend to have a firewall between the primary and secondary PulseNET HA servers, the firewall must be configured to allow the following PulseNET-required ports: For TCP, 45566, 8080, 8443, 1098, 1099, 4444, 4445, 4448, 3528, 3529, 1101, 1100, 4447, 4446, 8448, and for UDP, 1102.

Important In a PulseNET HA environment, a firewall can have an adverse affect on system performance and stability. If you have a firewall between your PulseNET HA servers, we do not support issues related to the firewall. For the support team to assist in debugging server issues, any such firewall must be disabled.

To install PulseNET in HA mode:

- 1 Select a host machine to be the primary PulseNET server.
- 2 Select a different host machine to be a secondary PulseNET server.
- 3 Select a third host machine for the database.

Important To run PulseNET in HA mode, the database must be external.

- 4 Select a host machine for the PulseNET Agent Manager.

In standalone mode, PulseNET uses a PulseNET Agent Manager that is embedded in PulseNET. In HA mode, the PulseNET Agent Manager must be remote in order to provide failover functionality.

Note The PulseNET Agent Manager can be installed on the same machine as the database, but not on the same machine as either instance of the PulseNET server.

- 5 Install the primary PulseNET instance.

For instructions on how to install PulseNET, see [“To Install PulseNET”](#) on page 12.

- 6 Start the primary PulseNET instance.

For instructions on how to start the primary PulseNET instance, see [“Starting and Stopping the Server in High Availability Mode”](#) on page 41.

- 7 Log in to the primary PulseNET instance.

For instructions on how to log in to PulseNET, see [“Logging in to PulseNET”](#) on page 44.

- 8 Obtain a PulseNET license from GE and install it on the primary PulseNET instance.

For instructions on how to obtain and install a PulseNET license, see the *PulseNET Administrator's Guide*.

- 9 Install the secondary PulseNET instance.

For instructions on how to install PulseNET, see “[To Install PulseNET](#)” on page 12.

- 10 Start the secondary PulseNET instance.

For instructions on how to start the secondary PulseNET instance, see “[Starting and Stopping the Server in High Availability Mode](#)” on page 41.

- 11 Install the PulseNET Agent Manager on a remote machine.

Initiate the PulseNET Agent Manager installer file included on the PulseNET install media, and follow the instructions provided.

Now data collection is possible.

Now PulseNET is in HA mode (that is, failover protection is available).

Performance and Stability Considerations

By default, PulseNET HA uses UDP. If your PulseNET HA configuration encounters performance or stability issues, you can reconfigure PulseNET HA to use TCP instead of UDP using the following instructions.

To manually reconfigure PulseNET HA to use TCP:

Note You must make the following changes to each server in the cluster.

- 1 Shutdown the servers.
- 2 Edit *server/default/deploy/cluster-service.xml*.

- a Comment out the following element:

```
<config>
  <udp . . .
  . . .
</config>
```

- b Uncomment the following element:

```
<config>
    <tcp ...
    ...
</config>
```

- c Find ... `thathost[7800]` ..., and change “`thathost`” to the host name of the secondary server in the cluster.
- 3 Save your changes.
- 4 Start the primary server.
- 5 Wait for the primary server to completely start up, and then restart the secondary server.

Next Steps

Start the PulseNET Management Server by following the instructions in “[Starting and Stopping PulseNET](#)” on page 38.

To log in to PulseNET, refer to “[Logging in to PulseNET](#)” on page 44.

External Database Access for Remote Users

Oracle and SQL Server support remote administration access by default.

When running PulseNET with an external MySQL database, the `GRANT ALL ON` query needs to be executed once in order to give users remote access to the database.

To provide users with remote access to the database:

- 1 From the **MySQL Server Instance Configuration** dialog box, select the **Modify Security Settings** check box.
- 2 Type a **new root password** (this password is used when executing the `GRANT ALL ON` query as described below).
- 3 Select the **Enable root access from remote machines** check box.

Executing the Grant All On Query Script

When running PulseNET with an external MySQL database, the `GRANT ALL ON` query needs to be executed once in order to give users remote access to the database.

Option 1

For better security, employ this option when the MySQL instance is being used as more than one database.

To grant remote access to the MySQL Administrator account, create the PulseNET database, and grant remote access to the PulseNET database:

- From the `mysql` prompt, type:

```
GRANT ALL ON mysql.* to 'root'@'%' identified by '<password>'
with grant option;
```

```
CREATE DATABASE pulsenet DEFAULT CHARACTER SET utf8 COLLATE
utf8_bin;
```

```
GRANT ALL ON pulsenet.* to 'root'@'%' identified by
'<password>' with grant option;
```

Where `<password>` is the `root` password you specified in [To provide users with remote access to the database](#): above.

This gives the `root` user (with username `root` and password `password`) remote access with all privileges.

Option 2

Use this option only when the MySQL instance is dedicated entirely to PulseNET.

To grant remote access to the entire MySQL instance:

- From the `mysql` prompt, type:

```
GRANT ALL ON *.* to 'root'@'%' identified by '<password>' with
grant option;
```

Where `<password>` is the `root` password you specified in [To provide users with remote access to the database](#): above.

Caution In some cases, following one of these options might not give `grant_priv` to the `root` user. If `grant_priv` is missing for `root@%` after executing the `GRANT ALL ON` query, see [“Installing PulseNET FAQ”](#) on page 34 for more information.

Manual Database Configuration

If you chose the option **Setup DB Later (manually)** while installing the PulseNET server for use with an external database, you must manually configure the database prior

to starting the PulseNET server by following the steps under the appropriate heading below.

Manually Configuring the External MySQL Database

Manually configure the external MySQL database by running the scripts in the `<pulsenet_home>/scripts/sql` directory in the order shown below.

Note The external database must exist before you run the scripts.

To perform manual database configuration:

- Run the *sql* scripts in the following order:
 - a `mysql_drop_db.sql`

This script must be run under an account with root or administrator privileges (for example, `sys`) since you require system access to execute it.
 - b `mysql_create_db.sql`

This script must be run under an account with root or administrator privileges (for example, `sys`) since you require system access to execute it.
 - c `mysql_create_schema.sql`

This script must be run as the PulseNET Database Account User ID that you set in [step 1](#) of “[Step 11: PulseNET Database Configuration](#)” on page 18. The default PulseNET Database Account User ID is *pulsenet*.
 - d `mysql_populate_db.sql`

This script must be run as the PulseNET Database Account User ID that you set in [step 1](#) of “[Step 11: PulseNET Database Configuration](#)” on page 18. The default PulseNET Database Account User ID is *pulsenet*.

Examples:

```
mysql -uroot -ppassword < mysql_drop_db.sql
mysql -uroot -ppassword < mysql_create_db.sql
mysql -upulsenet -ppulsenet < mysql_create_schema.sql
mysql -upulsenet -ppulsenet < mysql_populate_db.sql
```

Manually Configuring the External SQL Server Database

Manually configure the external SQL Server database by running the scripts in the `<pulsenet_home>/scripts/sql` directory in the order shown below.

Note The external database must exist before you run the scripts.

To perform manual database configuration:

- 1 Launch a command window.
- 2 Run the `.sql` scripts by issuing the following commands from the prompt in the order shown below.

Note In the commands shown below, replace `<admin username>` and `<admin password>` with the user name and password for the user account of the Microsoft SQL Server administrator.

a `sqlcmd -U <admin username> -P <admin password> -i <pulsenet_home>\scripts\sql\sqlsvr_drop_db.sql`

b `sqlcmd -U <admin username> -P <admin password> -i <pulsenet_home>\scripts\sql\sqlsvr_create_db.sql`

Note The script `sqlsvr_create_db.sql` does not drop the existing schema.

c `sqlcmd -U <pulsenet db username> -P <pulsenet db password> -i <pulsenet_home>\scripts\sql\sqlsvr_create_schema.sql`

Note Warnings related to the maximum length of index keys appear. These warnings are safe to ignore.

d `sqlcmd -U <pulsenet db username> -P <pulsenet db password> -i <pulsenet_home>\scripts\sql\sqlsvr_populate_db.sql`

Manually Configuring the External Oracle Database

Manually configure the external Oracle database by running the scripts in the `<pulsenet_home>/scripts/sql` directory in the order shown below.

Note The external database must exist before you run the scripts.

When you manually configure an Oracle database using the scripts described below, a new user is created in your database. The scripts create the required permissions for this user.

The scripts described below do not create tablespaces. If you need to create new tablespaces, you must do so manually first, before running the scripts. See the Oracle documentation for more information about Oracle tablespaces.

Note Check with your database administrator to correctly assign tablespace names. It is recommended that you create a PulseNET label for Data, Index, and Objects.

- 1 Run SQL*Plus by specifying the following from the command line:

```
sqlplus <username>/<password>
```

The SQL prompt appears.

- 2 Run the `.sql` scripts by issuing the following commands in the order shown below:

- a SQL> START <pulsenet_home>/scripts/sql/oracle_drop_db.sql

If you are using an Oracle database, this script must be run under an account with root or administrator privileges (for example, `sys`) since you require system access to execute it.

- b SQL> START <pulsenet_home>/scripts/sql/oracle_create_db.sql

This script must be run under an account with root or administrator privileges (for example, `sys`) since you require system access to execute it.

- c SQL> START <pulsenet_home>/scripts/sql/oracle_create_schema.sql

This script must be run using the PulseNET Database Account User ID that you set in [step 1 of Step 11: PulseNET Database Configuration](#). The default PulseNET Database Account User ID is `pulsenet`.

- d SQL> START <pulsenet_home>/scripts/sql/oracle_populate_db.sql

This script must be run using the PulseNET Database Account User ID that you set in [step 1 of Step 11: PulseNET Database Configuration](#). The default PulseNET Database Account User ID is `pulsenet`.

Importing a Network Security Certificate

To set up PulseNET to use HTTPS, you must generate a key pair (security certificate) into the PulseNET keystore. This allows PulseNET to communicate through the HTTPS protocol. You need to delete the existing certificate shipped with PulseNET

before generating a new key pair. Use the `keytool` utility shipped with PulseNET to create, import, and export certificates. This utility can be found in:

```
<pulsenet_home>\jre\bin\keytool
```

There are two keystores used by PulseNET:

- The built-in Tomcat keystore located at:
`<pulsenet_home>\server\default\conf\tomcat.keystore` (default password: nitrogen)
- The PulseNET keystore located at:
`<pulsenet_home>\jre\lib\security\cacerts` (default password: changeit)

To import a certificate:

- 1 Delete the existing `tomcat` key from the `tomcat.keystore` directory using the following command:

```
<pulsenet_home>\jre\bin\keytool -keystore <pulsenet_home>\server\default\conf\tomcat.keystore -storepass nitrogen -delete -alias tomcat
```

- 2 Create a new key under the `tomcat` alias using the following command:

```
<pulsenet_home>\jre\bin\keytool -keystore <pulsenet_home>\server\default\conf\tomcat.keystore -storepass nitrogen -genkey -alias tomcat
```

- 3 Generate a Certificate Signing Request (CSR) using the following command:

```
<pulsenet_home>\jre\bin\keytool -keystore <pulsenet_home>\server\default\conf\tomcat.keystore -storepass nitrogen -certreq -alias tomcat -file <your_request_file.csr>
```

This file must be signed by Certification Authority (CA).

- 4 Once you have the certificate signed, import it back to the `tomcat.keystore` using the following command:

```
<pulsenet_home>\jre\bin\keytool -keystore <pulsenet_home>\server\default\conf\tomcat.keystore -storepass nitrogen -import -trustcacerts -alias tomcat -file <your_converted_certificate>
```

You are prompted to specify the keystore password.

- 5 Type `nitrogen`.

Uninstalling PulseNET

You can uninstall PulseNET using the uninstaller utility for your platform. The uninstaller can be found in `<pulsenet_home>/forge-uninstaller`.

The default mode for the uninstaller is the graphical user interface (GUI) mode. The PulseNET uninstaller can be run from the command line by using console mode. Console mode is only available for Linux.

To uninstall PulseNET:

- 1 Stop the PulseNET Server using the appropriate method:
 - To stop a standalone PulseNET Server that is not running as a Windows service, follow the instructions in “[Stopping PulseNET](#)” on page 41.
 - To stop a standalone PulseNET Server that is running as a Windows service, follow the instructions in “[Running PulseNET as a Windows Service](#)” on page 40.
 - To stop a server that is running in High Availability (HA) mode, follow the instructions in “[Starting and Stopping the Server in High Availability Mode](#)” on page 41.
- 2 If PulseNET is installed as a Windows service, remove the service by navigating to `<pulsenet_home>\bin` and executing the following command:

```
fms.exe -r
```

or

```
fms.exe --remove-service
```

Alternatively, you can navigate to and click the **Remove Service For PulseNET Enterprise** shortcut.

- 3 Navigate to the `<pulsenet_home>/forge-uninstaller` directory of your PulseNET installation and run the uninstall script that is appropriate for your platform.

Follow the instructions in the console to uninstall PulseNET.

Alternatively, you can navigate to and click the **Uninstall PulseNET** shortcut.

Note Uninstalling does not affect the registry, shortcuts, or services.

- 4 After uninstalling, you can safely delete the `<pulsenet_home>` directory. It is recommended that you do so, since certain directories within it are not removed by the uninstaller.
- 5 After uninstalling, you should manually remove the PulseNET shortcuts. Then, if you re-install PulseNET, you will have just one set of shortcuts.

Installing PulseNET FAQ

PulseNET generated the following error during installation: “Embedded DB Error: Failed to startup embedded database”. Why does this error appear?

If you are installing PulseNET with the embedded MySQL database on Linux, the installer cannot start the embedded database and the installation fails if you do not define the IPv4 entry for *localhost* in the */etc/hosts* file prior to installing PulseNET.

To prevent the installation from failing, add the following IPv4 entry for *localhost* to */etc/hosts* prior to installing PulseNET:

```
127.0.0.1 localhost.localdomain localhost
```

If it was not set by executing the GRANT ALL ON query, is there a way to manually set grant_priv to give users remote access to an external MySQL database running with PulseNET?

Yes. In some cases, executing the `GRANT ALL ON` query may not set `grant_priv` to `y` for the *root* user in the `user` table.

If `grant_priv` is missing for `root@%` after running the `GRANT ALL` query as described in [“When running PulseNET with an external MySQL database, the GRANT ALL ON query needs to be executed once in order to give users remote access to the database.”](#) on page 27, follow the instructions below to manually set the required permission.

To update the user table to set grant_priv to the required value for the root user:

- 1 Log in to MySQL as *root*:

```
mysql -u root -p <password>
```

In this command, replace `<password>` with the *root* password you specified in [“To provide users with remote access to the database:”](#) on page 27.

- 2 From the `mysql` prompt, execute the `Grant All On query script` to give `grant_priv` to *root* for your database. See [“Executing the Grant All On Query Script”](#) on page 27 for information.

Running PulseNET

The instructions in this chapter assume that you have already installed PulseNET. If you have not, see “[Installing PulseNET](#)” on page 11 for installation instructions.

Note On 64-bit Linux platforms, the 32-bit version of *libgcc*.rpm* must be installed for PulseNET to run.

Initializing the Database

If you are using the embedded database, the initialization is performed when you start PulseNET.

For external databases, once the database has been successfully initialized, you can run PulseNET.

Caution On Linux, do not make the MySQL database file *my.cnf* world-writable, for example by issuing the command `chmod a+w <pulsenet_home>/mysql/my.cnf`. PulseNET and the database cannot start if there is world access to the configuration file *my.cnf*.

Tuning an External MySQL Database for PulseNET

If you are running the PulseNET server with an external MySQL database in a production environment, you may want to tune your database to ensure that it is not

under-resourced. Please refer to the table below for the tunable settings in the `<mysql_install_path>/my.ini` file.

Caution Database tuning is an advanced-user activity. Changing settings for your MySQL database incorrectly can result in problems with your PulseNET installation, such as serious performance problems with the PulseNET server.

my.ini setting	Recommended Value	Comments
<code>innodb_additional_mem_pool_size</code>	20M	Additional memory pool used by InnoDB to store metadata information.
<code>innodb_buffer_pool_size</code>	512M	InnoDB uses a buffer pool to cache both indexes and row data. The larger you set this, the less disk I/O is needed to access data in tables. Note: On 32-bit systems you might be limited to 2 - 3.5G of user level memory per process, so do not set it too high. Also, ensure that the host has enough real memory free for the specified buffer pool size. Performance will degrade substantially if the buffer pool uses virtual memory.

my.ini setting	Recommended Value	Comments
innodb_flush_log_at_trx_commit	2	Value 2 means that the transaction log is only flushed to the OS cache rather than to disk at each commit. The log file is still flushed to disk approximately once per second.
innodb_log_buffer_size	8M	The size of the buffer InnoDB uses for buffering log data.
innodb_log_file_size	128M	Size of each log file in a log group. You should set the combined size of log files to about 25 to 100% of your buffer pool size to avoid unneeded buffer pool flush activity on log file overwrite. Note: A larger log file size will increase the time required for the recovery process.
max_connections	341	The maximum number of concurrent sessions the MySQL server will allow.

my.ini setting	Recommended Value	Comments
<code>query_cache_size</code>	16M	Query cache is used to cache SELECT results and later return them without executing the same query again.
<code>sort_buffer_size</code>	256K	This buffer is allocated when MySQL needs to rebuild the index in REPAIR, OPTIMIZE, ALTER table statements as well as in LOAD DATA INFILE into an empty table.
<code>tmp_table_size</code>	32M	Maximum size for internal (in-memory) temporary tables.

Starting and Stopping PulseNET

The following sections describe how to start and stop PulseNET.

Starting PulseNET

The following section describes how to start the PulseNET from the command line or from a Windows shortcut and lists additional commands for use when starting or running PulseNET.

To start PulseNET from the command line:

- Navigate to the directory `<pulsenet_home>\bin` and execute the following command:

```
fms
```

To start PulseNET from a Windows shortcut:

- Depending on where you installed the startup icon, choose **Start > Programs > GE MDS > PulseNET 2.2 > Start PulseNET** or double-click the **Start PulseNET** icon on the desktop.

When PulseNET starts successfully, the following message appears in the command window:

```
PulseNET startup completed.
```

Additional Commands:

Command	Represents	Description
-s	start	Starts PulseNET (this is assumed if no command is specified).
-n	name	Provides a unique name for this instance of PulseNET.
-j	jvm-argument	Sets an option to be passed directly to the Java VM. Can be used to set more than one VM option.
-v	version	Displays the version number for this program and exits.
-h	help	Shows this information and exits.

Note The PulseNET Agent Manager starts automatically with the Server. When that happens, WARN messages like the following are expected to appear in the PulseNET Agent Manager's log file:

- Could not find an acceptable JRE in
 <pulsenet_home>\fglam\jre
- The path <pulsenet_home>\fglam\jre does not exist or is
 not a directory

These WARN messages can safely be ignored.

Running PulseNET as a Windows Service

After the installation is completed, you can install PulseNET as a Windows service either from the **Start** menu or the command line.

Note The procedures below assume that you have installed the program shortcuts in the default location.

Using the Start Menu Options

To install or remove PulseNET service from the Start menu:

- Choose **Start > Programs > GE MDS > PulseNET 2.2 > Windows Service > Install Service For PulseNET** (or **Remove Service For PulseNET**).

To start or stop PulseNET service from the Start menu:

- Choose **Start > Programs > GE MDS > PulseNET 2.2 > Windows Service > Start Service For PulseNET** (or **Stop Service For PulseNET**).

Using the Command Line

From the command line, navigate to `<pulsenet_home>\bin` and execute the following command to install PulseNET as a Windows service:

```
fms.exe -i
```

or

```
fms.exe --install-service
```

Additional Commands:

In addition to the additional commands listed in “[Starting and Stopping PulseNET](#)” on page 38, the following commands are available for the PulseNET Windows service.

Command	Represents	Description
-b	start-service	Start the PulseNET Windows service
-r	remove-service	Stop and remove the PulseNET Windows service

Stopping PulseNET

The following section describes how to stop PulseNET.

To stop PulseNET:

Do one of the following:

- Type **Ctrl-C** on the command window in which PulseNET started.
- Navigate to the directory `<pulsenet_home>\bin` and execute the following command:
`fms -q`
- Depending on where you installed the startup icon (Windows), choose **Start > Programs > GE MDS > PulseNET 2.2 > Stop PulseNET** or double-click the **Stop PulseNET** icon on the desktop.

When the server has stopped successfully, the **Start PulseNET** command window closes.

Starting and Stopping the Server in High Availability Mode

Configuring your server in High Availability (HA) mode allows you to run multiple servers in a JBoss partition offering HA.

Note To run the HA server, you must use an external database. The database has to be running before you start the PulseNET HA server.

To start the High Availability Server:

Do one of the following:

- Choose **Start > Programs > Quest Software > PulseNET 2.2 > High Availability > Start PulseNET In HA Mode**.
- Enter the following from the command line:
`fms ha`

When the server has started successfully, the following message appears in the window:

High Availability Server startup completed.

To stop the High Availability Server:

Do one of the following:

- Choose **Start > Programs > Quest Software > PulseNET 2.2 > High Availability > Stop PulseNET In HA Server.**
- Type **Ctrl-C** in the window in which the PulseNET HA server started.
- Open a second window, navigate to the directory `<pulsenet_home>/bin`, and execute the following command:

```
fmsha -q
```

When the server has stopped successfully, the window closes.

Redirecting Secondary Servers to the Correct URL

When PulseNET servers are configured as an HA cluster, the browser interface for each of the secondary servers redirects to the primary server. By default, the URL for the browser interface to which the secondary servers are redirected is generated automatically by PulseNET based on the primary server machine's host name.

You can override this URL and cause PulseNET to point to a different URL by starting the secondary servers from the command line with the following option, where `<host_name>` is the desired host name or FQDN (Fully Qualified Domain Name):

```
-Dquest.host.name=<host_name>
```

Use this option in cases where a single machine hosts multiple applications—including PulseNET—and is configured with multiple host names and IP addresses. In such cases:

- Each Web server is bound to a single IP address and responds to a unique FQDN or alias.
- The default URL used by PulseNET to redirect the secondary servers is based on the primary server machine's host name and so might not present the correct URL since PulseNET could be bound to a different alias.

You can cause the URL to be based on this alias by using the `-D` option described above.

Example:

You have two machines, whose host names are `server1` and `server2`. You have an HA cluster running on these machines. The primary server runs on `server1` and the secondary server runs on `server2`.

Both machines have two IP addresses: one internal and the other external. The external IP addresses are bound to the DNS (Domain Name System) names `pulsenet1.example.com` and `pulsenet2.example.com`. PulseNET has been bound to the

external IP addresses and is not listening on the internal IP addresses. In this case, the PulseNET browser interface is available at *http://pulsenet1.example.com:8080*.

However, the default URL to which the secondary server redirects is *http://server1:8080*, which in this case fails to display the browser interface. Overriding the URL with `-Dquest.host.name=pulsenet1.example.com` solves the problem.

Remote Monitor

The Remote Monitor is a Java program that regularly communicates with a set of High Availability (HA) servers. If there is no reply after it attempts to contact the server, then it logs the event and can optionally send out e-mail notifications to an administrator.

The Remote Monitor takes a list of host names or host name/port pairs as parameters. When invoked without parameters, Remote Monitor takes the list of host names or host name/port pairs from the file `<pulsenet_home>/config/remote_monitor.config` under the entry `server.urls`.

Each parameter in the entry `server.urls` points to a specific HA server. If a port is not specified as part of this entry, the default port 51231 is used. The default port can be configured in `<pulsenet_home>/config/remote_monitor.config`, under the entry `health.monitor.port`. This entry should match the `health.monitor.port` entry in the file `<pulsenet_home>/config/restart_monitor.config` on your servers.

Note To use the Remote Monitor, JRE 1.5 must be installed on the machine hosting the Remote Monitor and the `JAVA_HOME` environment variable must be set to point to the installation directory.

To install the Remote Monitor:

- Copy the `<pulsenet_home>/tools/remote_monitor.zip` file to your target machine and unzip the contents to a directory.

To start the Remote Monitor:

Note The PulseNET server must be running before you can start the Remote Monitor.

Enter the command:

- `<pulsenet_home>/bin/remotemonitor <hostname[:port]>>`

or:

- Choose **Start > Programs > Quest Software > PulseNET 2.2 > High Availability > Start Remote Monitor**.

To stop the Remote Monitor:

- Enter **Ctrl-C** from the command window where the Remote Monitor started.

or:

- Choose **Start > Programs > Quest Software > PulseNET 2.2 > High Availability > Stop Remote Monitor**.

Logging in to PulseNET

Note PulseNET must be running before you can log in.

To log in to PulseNET from the GUI:

- 1 Depending on where you installed the program icons, choose **Start > Programs > GE MDS > PulseNET 2.2 > PulseNET Console**.
- 2 Enter a valid username and password and click **Login**.

To log in to PulseNET using a Web browser:

- 1 Open a Web browser and type the following:

```
http://<hostname>:<port>
```

Where <hostname> is the name of the machine where PulseNET is installed and <port> is the http port specified during installation (the default is 8080).

- 2 Enter a valid user name and password and click **Login**.

Running PulseNET FAQ

Why do I see an extra process named Quest Process Runner when I run PulseNET?

On Linux, PulseNET uses the Quest Common Process Runner to run processes such as the embedded MySQL database and command actions.

On Windows, PulseNET starts the Quest Common Process Runner (*qcn_runner.exe*) but does not use it to launch new processes.

Why does the error message “cannot restore segment prot after reloc: Permission denied” appear when I start PulseNET?

Newer Linux distributions have enabled new kernel security extensions from the SELinux project at the NSA (National Security Agency). SE Linux is an NSA project to improve the security of Linux through Mandatory Access Control (MAC). These extensions allow finer-grained control over system security. However, SELinux also changes some default system behaviors, such as shared library loading, which can be problematic to third-party programs.

If you see the error message “cannot restore segment prot after reloc: Permission denied” when you start PulseNET, your SELinux configuration is preventing IDL from launching.

To rectify this issue, you can perform one of the following workarounds:

- Change the default security context for PulseNET by issuing the command:

```
chcon -t texrel_shlib_t <pulsenet_home>/jre/lib/i386/*.so
chcon -t texrel_shlib_t <pulsenet_home>/jre/lib/i386/server/
*.so
```
- Disable SELinux altogether by setting it to disabled in your `/etc/sysconfig/selinux` file:

```
SELINUX=disabled
```

For more information about SELinux, consult your Linux distribution vendor.

Can a live PulseNET server be excluded from a High Availability (HA) cluster?

Primary and standby PulseNET servers in an HA cluster periodically ping each other to check if they are still active. If a server fails to respond several times in a row to the ping message (within a configurable timeout period), it is suspected to be down and excluded from the cluster.

This mechanism can lead to a live server being removed from the cluster in certain situations, such as when:

- The server host’s CPU is overloaded for an extended period of time, so that it cannot process the ping message in time.
- The server is suspended in a debugger.
- A temporary network disruption has occurred.

To reduce the chances of this swap happening, you can increase the timeout or number of retries for failure detections, as described below.

- 1 Open `<pulsenet_home>/server/default/deploy/cluster-service.xml` in an editor.
Note You must edit this file for each server in the cluster.
- 2 Find the line starting with the following:
`<FD shun="true"`
- 3 Set the `timeout` attribute or the `max_tries` attribute to a larger number.
Note The unit for the `timeout` attribute is milliseconds.
- 4 Save `cluster-service.xml`.
- 5 Restart the PulseNET server.

I am running PulseNET with a MySQL database. When I try to start PulseNET, it fails to start and a SQL exception appears in the logs. Why does this happen?

If you encounter this problem, the cause might be that the MySQL database file `my.cnf` has been made world-writable.

Do not make the MySQL database file `my.cnf` world-writable, for example by issuing the command `chmod a+w <pulsenet_home>/mysql/my.cnf`. PulseNET and the database cannot start if there is world access to the configuration file `my.cnf`.

I am running PulseNET in High Availability (HA) mode. When I start my PulseNET servers, "UDP mcast receiver" errors appear in the logs for the primary and secondary servers. How can I resolve these errors?

If servers that are not part of a particular HA partition are configured to multicast using the same port on the same subnet as those within the HA partition, errors like the following appear in the logs for the servers that are configured in this way:

```
ERROR [UDP mcast receiver] org.jgroups.protocols.UDP - message
does not have a UDP header
```

or

```
ERROR [UDP mcast receiver] org.jgroups.protocols.UDP - discarded
message from different group
```

If you see this type of message, change the cluster multicast port of the servers that are reporting the error. In addition, if you plan to have multiple High Availability (HA)

partitions on the same subnet, configure a different cluster multicast port for each HA partition. If necessary, contact technical support for assistance.

Important In both cases described above (resolving errors and planning to have multiple HA partitions on the same subnet), the primary server and secondary servers within each HA partition must be configured to use the same cluster multicast port.

If I stop PulseNET by closing the Command Prompt window, an error appears when I start it up again. How do I restart PulseNET?

It is recommended that you do not use this method to stop PulseNET. However, if you do use this method, follow the workaround listed below.

- 1 If you are running the embedded MySQL database, stop the database manually before restarting PulseNET.
- 2 Remove the stale *.pid* file that is located in the *state* directory. The logs or the console output inform you which *.pid* file to remove when you restart PulseNET.

Index

A

administration

default user name and password 11

administrator

access 11

D

database

external

configuration 18

external access for remote users 27

initializing 35

devices

limit 7

H

high availability 8

installing 25

performance 26

stability 26

TCP 26

UDP 26

High Availability Server 41

I

industrial communications 7

installation

requirements 11

L

logging in

to PulseNET 44

N

network security certificate

importing 31

P

password

administrator 11

PulseNET

uninstalling 33

What is it? 7

R

remote monitor

installing 43

starting 43

running

PulseNET 35

S

server

starting 38

stopping 41

U**uninstalling**

PulseNET 33

user account

administrator 11

W**Windows**

service, from the command line 40

service, installing PulseNET as a 40

IN CASE OF DIFFICULTY...

If you have problems, comments or questions pertaining to the MDS PulseNET application, please contact GE MDS using one of the methods listed below:

Phone: 585 241-5510

E-mail: gemds.techsupport@ge.com

FAX: 585 242-8369

Web: www.gemds.com