GE PulseNET Standard
Administration Guide
Version 4.5.0
# Table of Contents

## Introduction
- What is GE PulseNET? 4
- Understanding GE PulseNET Roles 4
- GE PulseNET Documentation 5
  - Release Notes 5
  - Installation Guide 5
  - User Guide 5
  - Administration Guide 6

## Getting Started
- Starting GE PulseNET 7
- Stopping GE PulseNET 7
- Using the Administration Dashboard 8

## Working with Licenses
- Requesting Licenses 9
- Adding Licenses 10
- Managing Licenses 10
- Requesting Replacement Licenses 11

## System Configuration
- Email Configurations 12

## Working with Users
- Creating Users 14
- Managing Users 15
- Configuring Password Policy 15
- Setting User Session Timeout 16

## Working with Rules
- Predefined Rules 17
- Enabling and Disabling Rules 19
- Configuring Rule Thresholds 20
  - Fire Strategy Values 20
  - Enabling Email for Rules 21

## Collection Schedules
- 22
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduling Device Data Collection</td>
<td>22</td>
</tr>
<tr>
<td>Monitoring Configuration</td>
<td>25</td>
</tr>
<tr>
<td>Defining SNMP Properties</td>
<td>25</td>
</tr>
<tr>
<td>Configure SNMP Setting</td>
<td>25</td>
</tr>
<tr>
<td>Managing SNMP Credentials</td>
<td>25</td>
</tr>
<tr>
<td>Managing SNMP v1 or v2c Community Strings</td>
<td>25</td>
</tr>
<tr>
<td>Managing SNMP v3 Credentials</td>
<td>27</td>
</tr>
<tr>
<td>Migrating Devices to New SNMP Credentials</td>
<td>28</td>
</tr>
<tr>
<td>Managing ICMP Settings</td>
<td>29</td>
</tr>
<tr>
<td>Managing DLINK Settings</td>
<td>30</td>
</tr>
<tr>
<td>Configuring DLINK Properties</td>
<td>30</td>
</tr>
<tr>
<td>General DLINK Properties</td>
<td>31</td>
</tr>
<tr>
<td>Adding DLINK Master Seeds</td>
<td>33</td>
</tr>
<tr>
<td>Planning Data Collection on DLINK Networks</td>
<td>34</td>
</tr>
<tr>
<td>Device Discovery</td>
<td>37</td>
</tr>
<tr>
<td>Discovering SNMP Devices</td>
<td>37</td>
</tr>
<tr>
<td>Discovered Devices</td>
<td>39</td>
</tr>
<tr>
<td>Ineligible Devices</td>
<td>39</td>
</tr>
<tr>
<td>Discovering DLINK Devices</td>
<td>40</td>
</tr>
<tr>
<td>Active Discovery</td>
<td>40</td>
</tr>
<tr>
<td>Passive Discovery</td>
<td>40</td>
</tr>
<tr>
<td>Defining the Discovery Method for a Master</td>
<td>40</td>
</tr>
<tr>
<td>Running DLINK Discovery</td>
<td>41</td>
</tr>
<tr>
<td>Discovered Devices</td>
<td>42</td>
</tr>
<tr>
<td>Continuous Passive Auto-discovery</td>
<td>43</td>
</tr>
<tr>
<td>Authorizing Devices</td>
<td>43</td>
</tr>
<tr>
<td>Managing Device Settings</td>
<td>44</td>
</tr>
<tr>
<td>Device Administration</td>
<td>44</td>
</tr>
<tr>
<td>Decommissioning Individual Devices</td>
<td>44</td>
</tr>
<tr>
<td>Decommissioning SNMP devices - Authorized Device List</td>
<td>45</td>
</tr>
<tr>
<td>Configuring data collection on DLINK master devices</td>
<td>45</td>
</tr>
<tr>
<td>Managing System Schedules</td>
<td>48</td>
</tr>
<tr>
<td>Getting Support</td>
<td>50</td>
</tr>
<tr>
<td>Generating a Support Bundle</td>
<td>50</td>
</tr>
<tr>
<td>Enabling Debug Mode</td>
<td>50</td>
</tr>
</tbody>
</table>
Introduction

The Administration Guide is intended to help you configure and manage GE PulseNET and contains information related to configuring the system settings and monitoring devices.

This section describes the Operator and Administrator roles, provides instructions for starting, stopping, and logging in to GE PulseNET, and describes the Administration Home dashboard that you see when you log in with the GE PulseNET Administrator role.

What is GE PulseNET?

GE PulseNET is a software application used for monitoring devices in Industrial Communications networks. Each device that GE PulseNET monitors serves a specific function in the network. These functions may include acting as a bridge, router, access point/base station, or remote/subscriber. The devices can be widely dispersed geographically and are able to operate with different bandwidths, depending on radio type and frequency. For additional information on specific Industrial Communications products, refer to the GE MDS website.

GE PulseNET Standard edition is intended for small-scale operations with a need to monitor less than 500 devices. GE PulseNET Enterprise edition is intended for large-scale operations with a need to monitor 25,000+ devices.

Understanding GE PulseNET Roles

There are two GE PulseNET roles to which permissions can be assigned:

**Operator** — An operator is primarily responsible for tracking the status of the devices that the system is monitoring. Operators have access to a restricted set of dashboards. The User Guide primarily explains the tasks that operators can accomplish.

**Administrator** — An administrator installs, configures, and controls the overall functionality of the GE PulseNET system, and provides support for all of the operators. An administrator has a number of responsibilities including creating users, requesting and installing licenses, configuring email settings, setting the frequency of data collection, and discovering/authorizing devices for monitoring.

This Administration Guide outlines the advanced responsibilities granted to administrators. Since the User Guide contains basic information for operations that will be employed by all users, it is recommended that administrators read that guide as well.
GE PulseNET Documentation

Release Notes

The Release Notes provide:

- A list of new and updated features
- Workarounds for any known issues
- Late-breaking news about the software

Consult this document first, because it may contain updates to information and procedures described in the other GE PulseNET documents.

Installation Guide

The Installation Guide includes:

- Installation prerequisites, system recommendations, and planning guidelines
- Instructions for installing and configuring GE PulseNET on all supported platforms

User Guide

The User Guide provides basic navigation and operation information that all users, especially those with the Operator role, will need in order to effectively use GE PulseNET.

- An overview of GE PulseNET, describing its purpose, explaining key concepts, and providing instructions for basic navigation
- Basic navigation and dashboard overview
- Working with time ranges, charts, and tables
- Managing and monitoring devices, including information on device detail views
- Creating and scheduling reports and dealing with alerts

Because the information contained in the User Guide is vital for the normal operation of GE PulseNET, we recommend that both Operators and Administrators read this guide.
The Administration Guide is intended to help those with the administrator role configure and manage the GE PulseNET system. This guide provides instructions on how to perform administrative tasks such as:

- Creating users
- Requesting and installing licenses
- Configuring email settings
- Creating report schedules and setting rule thresholds
- Setting the parameters and frequency for data collection
- Discovering and authorizing devices
- Requesting GE support
Getting Started

Starting GE PulseNET

Windows

Open a command window and navigate to the directory `<pulsenet_home>` and execute the following command: `start.bat`

When GE PulseNET starts successfully, the following message appears in the command window: PulseNET startup completed.

Linux

Open a terminal window and navigate to `<pulsenet_home>` and execute the following command: `start.sh`

Stopping GE PulseNET

Windows—Choose one of the methods listed below.

- If GE PulseNET is running in a command window, type `Ctrl-C` to stop GE PulseNET.
- Navigate to the directory `<pulsenet_home>` and execute the following command: `stop.bat`

Linux—Choose one of the methods listed below.

- If GE PulseNET is running in a terminal window, type `Ctrl-C` to stop GE PulseNET.
- Open a terminal window and navigate to `<pulsenet_home>` and execute the following command: `stop.sh`
Using the Administration Dashboard

The Administration dashboard is the default home page for an administrator. It provides links to other dashboards where you can complete administrative tasks.

This dashboard provides the following links:

**Monitoring Configuration** — for setting SNMP, ICMP, and DLINK parameters

**Collection Schedules** — for configuring how often GE PulseNET collects metrics from different types of devices

**Device Discovery** — for discovering SNMP and DLINK devices, and setting up passive auto-discovery of DLINK remotes

**Email Configuration** — for configuring the email server and account GE PulseNET will use to send email notifications

**Rules** — for managing threshold settings and notification rules

**Report Management** — for generating, scheduling, and managing reports and viewing audit logs. See the GE PulseNET User Guide for details.

**User Management** — for creating, configuring, and maintaining GE PulseNET users

**Schedules** — for adding, changing, or deleting default system schedules

**Licensing** — for requesting, installing, and managing licenses

**Support** — for generating and downloading support bundles and requesting support
Working with Licenses

One of the first administrative tasks you should accomplish is to request and install a valid GE PulseNET license. A license provides GE PulseNET with the capacity to authorize and monitor devices. Each device connected with GE PulseNET will be assigned a license during the authorization process.

Requesting Licenses

To request a license:

1. Navigate to Administration > Licensing > Request a License. A dialog box will appear.
2. Select your product from the dropdown list of Available Products.
3. In the Contact Name field, type the name of the person at your company who will be the contact.
4. In the Access Code field, type your access code. You can obtain your access code from your GE Sales team.
5. In the Desired Capacity field, type the total number of licenses required. For example, if you want to monitor 100 access points and 300 remote devices, enter 400.
6. In the Comment field, enter any comments that you have which would help the Licensing team fulfill your license request.
7. Click Save Request to a File in order to send this license request to the GE Licensing team. You may also open this licenseRequest.txt file and copy/paste the hardware ID directly into an email if desired.

When the request is approved, the new license is sent by GE to you via email.
Adding Licenses

After you receive new licenses, you must add them so that you can monitor your devices.

To add a license:

1. Navigate to Administration > Licensing > Add a License.
2. In the dialog box that appears, click Import License from File to locate the license file on your computer (the file must be on the machine where the browser is running). You may also copy the license key from the file and paste it directly into the License Key field.
3. Click ➕ Add License.

If the license is valid, it is added to GE PulseNET. Otherwise, you will receive a message stating that the license key is invalid. Contact the GE PulseNET Licensing team if this occurs.

Managing Licenses

Installed licenses appear under Administration > Licensing > Manage Licenses. Here you can delete expired licenses, migrate devices to new licenses, or request a replacement license.

Click on any license row to view the details for a specific license. Here you can view the Hardware ID that identifies the server to GE PulseNET. You can click the checkbox on a row to select it, and selected rows may also be deleted from the system. Click on the License Key field to view the GE PulseNET license key associated to this license.
In the Used column you also have the option to migrate devices that have been associated to this license. Click the migrate link to view the list of devices and select them for migration. Once selected, you may choose another GE PulseNET license to which the selected devices should be migrated.

Requesting Replacement Licenses

If a GE device is removed from service and replaced with a new device, you will need to request that GE send a replacement PulseNET license for the new device. Existing licenses are bound to the serial numbers of GE devices, so they cannot be reused once they have been assigned to a specific device during the authorization process.
System Configuration

Email Configuration

Another administrative task that must be accomplished is to configure email settings. This will allow PulseNET to notify users about system issues.

To define email settings:

1. Navigate to Administration > Email Configuration.
2. In the Email Configuration dialog box, fill in each property and define the required values so that you can be notified about system issues (see the table below for information about these values).
3. When you are finished editing the properties, click Test Configuration to ensure that emails can be sent.
4. In the Recipient Addresses box, type your email address.
5. Click Send Test Email.

PulseNET will send a test email to your email address. Check your mailbox to ensure that it contains the test email message. If the configuration settings are valid, click Save.

Below are explanations of the values you must define in order to receive email notifications about system issues:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail Server</td>
<td>The host name or IP address of the mail server to be used for sending email.</td>
</tr>
<tr>
<td>Sender Address</td>
<td>The email address that will appear in the From portion of the sent email.</td>
</tr>
<tr>
<td>Recipient Addresses</td>
<td>The list of destination email addresses that should receive PulseNET email notifications. Separate multiple email addresses with a comma.</td>
</tr>
<tr>
<td>Mail Server Port</td>
<td>The port number that PulseNET uses to communicate with the mail server.</td>
</tr>
<tr>
<td>Mail Protocol</td>
<td>The transport protocol used for sending emails. The supported protocols are SMTP and SMTPS.</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>EnableSTARTTLS?</td>
<td>Indicates whether you want to enable the START-TLS protocol and use encryption when sending emails from PulseNET.</td>
</tr>
<tr>
<td>EnableSSL?</td>
<td>Indicated whether you want to enable the SSL protocol and use encryption when sending emails from PulseNET.</td>
</tr>
<tr>
<td>MailServerLogin</td>
<td>The user name of the email account required by the mail server in order to send email.</td>
</tr>
<tr>
<td>UserPassword</td>
<td>The password for the above user account.</td>
</tr>
</tbody>
</table>
Working with Users

PulseNET controls user access to the web interface using the concept of users and roles. When administrators create new users, a role is assigned to the user. The assigned role determines the dashboards and views that users can access when they log in to PulseNET.

Users assigned to the PulseNET Administrator role have access to all available dashboards. Users assigned to the PulseNET Operator role have access to a restricted set of dashboards.

Creating Users

As a PulseNET Administrator, you can create new PulseNET users.

To create a new user:

1. Navigate to Administration > User Management > Users.
2. Click the Add button.
3. In the New User wizard, type a name for the new user.
4. Assign the new user a role. A user can be an administrator or an operator, but not both. Administrators still have access to all operator functionality. See Understanding PulseNET Roles.
5. Select Change Password to assign a password to the new user. In the Password fields, type the same password.
6. Click Save.

The new user now appears in the User Management list located at Administration > User Management > Users.
Managing Users

All users are listed in the Users table. For each user, you can lock the account, edit the settings, or delete the user account.

- Click the **🔒 Lock** icon to lock or unlock a user account
- Click the **📋 Edit** icon to change account details (name, role, password)
- Click the **⛔ Delete** icon to remove the account from GE PulseNET
- Click the **Audit Trail** icon to view the GE PulseNET activity by this user

Configuring Password Policy

As an administrator, you can configure the global password policy for user accounts. Click the **Edit** button to change any of the global defaults.
Setting User Session Timeout

As an administrator you can set the user session timeout. Enter the new value and click **Save**. You may also check the box which disables session timeout, if desired.
Working with Rules

GE PulseNET provides several types of notifications so that you can efficiently monitor your GE devices.

**System event emails** — System events such as expiring licenses will trigger automatic email notifications. These alerts are embedded in GE PulseNET and cannot be disabled. To direct such emails to the proper recipients, add the user email addresses to the list of email recipients. See Configuring Email Settings.

**Alerts based on GE PulseNET rules** — Alerts are triggered when problems arise in your monitored environment. Once a performance rule has been enabled, GE PulseNET will send an alert (fatal, critical, or warning) when it determines that one or more devices have met that rule’s predefined conditions. This alert appears as an icon beside the device name in the web interface and a generic icon on the device type. See Enabling and Disabling Rules.

**Email notifications based on GE PulseNET rules** — You can also receive email notifications if problems arise in your monitored environment. These notifications can be enabled by checking the Enable Email checkbox for the desired severity levels within each rule. See Enabling Email for Rules.

Predefined Rules

GE PulseNET contains a number of predefined rules for device monitoring. You can enable any of these rules and configure the thresholds you require so that you are notified if your system encounters problems. Users are notified when rule thresholds are exceeded if their email addresses are correctly configured in the email recipients list. See Configuring Email Settings.

The following table provides a description of each of GE PulseNET’s predefined rules.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP Change for Remote</td>
<td>Monitors remote devices for migration to different access points.</td>
<td>N/A</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Severity</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Bad Access Point Health</td>
<td>Monitors the percentage of remote devices for an access point that are in a particular alert state or worse. Beyond that percentage, the access point may be the root cause of the problem.</td>
<td>Warning, Critical, Fatal</td>
</tr>
<tr>
<td>Bad Remote Health</td>
<td>Monitors the percentage of remote devices that are in a particular alert state or worse.</td>
<td>Warning, Critical, Fatal</td>
</tr>
<tr>
<td>Bad Repeater Health</td>
<td>Monitors TransNET devices that are acting as Store and Forward (SAF) or master devices. This rule fires if a defined number of downstream devices are unavailable.</td>
<td>Warning, Critical, Fatal</td>
</tr>
<tr>
<td>Device Unavailable</td>
<td>Monitors the availability of the device.</td>
<td>Fatal</td>
</tr>
<tr>
<td>DLINK Alert Notification</td>
<td>Monitors whether a DLINK alarm has been received from a narrowband radio.</td>
<td>N/A</td>
</tr>
<tr>
<td>PA Temperature</td>
<td>Generates alerts for DLINK devices when Power Amplifier temperatures reach defined limits.</td>
<td>Warning, Critical, Fatal</td>
</tr>
<tr>
<td>Poor Response Time</td>
<td>Monitors the ICMP round trip time for a device.</td>
<td>Warning, Critical, Fatal</td>
</tr>
<tr>
<td>RSSI Change</td>
<td>Monitors values of RSSI that are outside the two-day moving average.</td>
<td>Warning, Critical, Fatal</td>
</tr>
<tr>
<td>RSSI Level</td>
<td>Monitors the levels of Received Signal for devices.</td>
<td>Warning, Critical, Fatal</td>
</tr>
<tr>
<td>SD Master Station Failover</td>
<td>Monitors whether a radio failover has occurred between redundant radio modules.</td>
<td>N/A</td>
</tr>
<tr>
<td>Serial Number Unrecognizable</td>
<td>Generates an alert when the serial number of a DLINK access point is unrecognizable</td>
<td>Fatal</td>
</tr>
<tr>
<td>SNR Change</td>
<td>Monitors for values of SNR that are outside the two-day moving average.</td>
<td>Warning, Critical, Fatal</td>
</tr>
</tbody>
</table>
SNR Level | Monitors the ratio of Signal to Noise for devices. | Warning, Critical, Fatal

**NOTE:** Some of the predefined rules are disabled by default, allowing you to enable the ones you need for your environment.

### Enabling and Disabling Rules

Enable rules so that alerts are triggered when problems arise in your monitoring environment. The alert appears as an icon beside the device name in the Summary table and, if configured, an email is sent to the addresses configured under Email Settings.

To enable a rule:

1. Navigate to Administration > Rules.
2. On the Rules dashboard, find the row for the rule that you want to enable.
3. In the Enabled column for the desired rule, click the checkbox to toggle the rule on.

Multiple severity rules can have different conditions defined so that you are notified when increasing or decreasing thresholds are met. Once a rule is enabled, define the required threshold values (see **Configuring Rule Thresholds** below) and enable email notifications if desired.

To disable a rule:

In the Enabled column for a rule, uncheck the checkbox to toggle the rule off.
Configuring Rule Thresholds

Most GE PulseNET Multiple Severity Rules have four thresholds: ☠ fatal, 🔴 critical, ⚠ warning, and ✅ normal. You can define the threshold values for the rule so that GE PulseNET sends alerts when your required condition is met on the devices you are monitoring.

To configure the thresholds for a rule:

1. Navigate to Administration > Rules.
2. Click the ☑️ Edit icon for the rule you want to modify.
3. In the table provided, click the ☑️ Edit icon for the value that you want to edit.
4. Type the new value and click 📡 Save.

Fire Strategy Values

A fire strategy defines the number of consecutive times a certain threshold must be met to cause a rule to raise the corresponding alert ☠ fatal, 🔴 critical, ⚠ warning).
**Example**

For an iNET-900 remote the RSSI threshold for the warning alert is set to -82 dBm with a fire strategy value of 1. This means that the first time this threshold is exceeded during the polling cycle for that device, a warning alert is raised. In order to smooth out any “flapping” conditions for a device on the borderline of this threshold, you can set the strategy to fire an alert only if GE PulseNET detects the threshold has been breached on three consecutive polls. You can also set the strategy to fire an alert if GE PulseNET detects the threshold has been breached on three of the last five consecutive polls.

**Enabling Email for Rules**

Predefined GE PulseNET rules are configured by default not to send notifications when a threshold is breached. Email notifications can be enabled for any desired severity level while you are editing a specific rule, as shown in the image above. Simply check the box to **Enable Email**.
Collection Schedules

Scheduling Device Data Collection

Administrators can schedule the frequency of data collection by device type. The Collection Schedules dashboard lists the devices that GE PulseNET can monitor.

To configure the data collection schedule for monitored devices:

1. Navigate to Administration > Collection Schedules.
2. On the Collection Schedules view, each row in the table shows the current schedule for each type of device. To edit the collection schedule for any row, click the Edit icon.

On the Update Collection Schedule display, you may change the values for each of the three types of data collection done by GE PulseNET (Configuration schedule, Performance interval, and Availability interval).
To edit the Configuration Schedule:

1. Choose whether you want GE PulseNET to collect device configuration information on selected days of the week or whether you only want selected days of the month. Click the radio button for weekdays or dates of the month as desired.
2. Check the week days or days of the month that you want GE PulseNET to use for configuration collection.
3. In the Run Times box, select one or more times of day (hours) that you want GE PulseNET to use for configuration collections. You can also enter a specific time during each hour that you want GE PulseNET to use when it collects
configuration data from each device.
4. You can also update the description text for this Configuration Schedule, if desired.

**To edit the Performance Interval:**
- Enter a new value (minutes) in the field.

**To edit the Availability Interval:**
- Enter a new value (minutes) in the field.

Click **Save** to apply your changes to GE PulseNET’s collection schedules.
Monitoring Configuration

The Monitoring Configuration dashboard allows you to configure GE PulseNET settings for using several network protocols to communicate with devices (SNMP, DLINK, and ICMP).

Defining SNMP Properties

To configure SNMP settings:

- Navigate to Administration > Monitoring Configuration > SNMP Configuration.
- Click SNMP Properties.

The SNMP Properties display allows you to configure the SNMP versions that GE PulseNET will support, the default SNMP port, and the timeout value after which GE PulseNET will consider a device unreachable during polling. You may also set the number of parallel threads GE PulseNET uses during SNMP polling, as well as the gap between successive SNMP queries and the number of retries allowed after a timeout. If the SNMP query is being made on the GE PulseNET server itself, the Same Host Request Interval applies. Also, during SNMP discovery, the Discovery Request Timeout setting will be used rather than the timeout for regular data collection.

Managing SNMP Credentials

Managing SNMP v1 or v2c Community Strings

To monitor SNMP devices, credentials and protocol settings must be defined. There are two default community strings: public (read-only) and private (write). Custom community strings can be added or edited as needed. Although GE PulseNET allows you to select more than one Community String, it is general practice to run discovery with just one
SNMP read-only selected at a time. This prevents the discovery action from being flagged by your internal IT systems as a security risk (i.e. port scan).

To add an SNMP community string:
- Click the➕ Add button and enter the community string, along with selecting whether this credential is allowed to Read, Write, or both.
- Click💾 Save to save the new community string to GE PulseNET.

NOTE: The Add button is dimmed if neither SNMP v1 nor SNMP v2c are selected for use in the SNMP properties. See Defining SNMP Properties.

To edit an SNMP community string:
- Click the📋 Edit icon on the row displaying the credential you wish to edit.
- Change the values as desired, and click💾 Save to save your changed.

To delete an SNMP community string:
- Click the🗑 Delete icon on the row displaying the credential you wish to delete.
- Click the🗑 Delete button to confirm that you want to delete the selected community string. Community strings cannot be deleted if they are being used to manage devices.
Managing SNMP v3 Credentials

To add SNMP v3 credentials:

- Navigate to Administration > Monitoring Configuration > SNMP Configuration.
- On the SNMP Credentials table, click 📘 Add in the SNMP v3 Credentials section.

The 📘 Add button is disabled if SNMP v3 is not selected for use in the advanced SNMP settings (see Defining Advanced SNMP Settings).

1. Type the username that will be used for authentication.
2. Select Read Permission, Write Permission, or both.

To discover GE MDS entraNET devices, you must have at least one Write credential defined so that remote devices can be discovered from the access point.

To change the permission on an existing credential, click the value in the Permission column. In the dialog box, select the permission.

3. Select a Security Level:

   - No authentication and no privacy — the identity of the sender is not verified
   - Authentication and no privacy — the identity of the sender is verified, but the information is not encrypted
   - Authentication and privacy — the identity of the sender is verified and the information is encrypted

4. If the Security Level that you selected requires authentication, specify an authentication protocol and passphrase (i.e., the password for the specified user name).
5. If the Security Level that you selected requires privacy, specify a privacy protocol and passphrase. The passphrase is the encryption key.
6. Click 📡 Save.
To edit SNMP v3 credentials:

- In the **SNMP v3 Credentials** table, click the 📒 Edit icon for the SNMP v3 credential that you want to edit.
- Edit the settings for the credential as desired.
- Click 📡 Save.

To delete SNMP v3 credentials:

- Click the ⚠️ Delete icon on the row displaying the credential you wish to delete.
- Click the ⚠️ Delete button to confirm that you want to delete the selected community string. Community strings cannot be deleted if they are being used to manage devices.

### Migrating Devices to New SNMP Credentials

Navigate to **Administration > Monitoring Configuration > SNMP Configuration > SNMP Credentials**.

To migrate devices from one community string or set of credentials to another:

- Find the community string or credential from which you want to migrate devices, and click the number in the **Managed Devices** column.
• In the **Migrate Credential** wizard, choose the type of SNMP credential to which you want to migrate the selected devices (v1/v2c or v3), then select the specific SNMP credential that will be used to communicate with these devices in the future.

• Check the specific devices that you want to migrate to the new credential.

• Click **Save** to tell GE PulseNET to use the new credential when communicating with the selected devices.

**Managing ICMP Settings**

The Internet Control Message Protocol (ICMP) is used when pinging Ethernet devices to determine whether they are reachable on the network.

**To configure ICMP settings:**

Navigate to **Administration > Monitoring Configuration > ICMP Configuration**. Enter or modify any settings as desired.

- **Worker Threads** sets the number of simultaneous parallel ICMP queries that GE PulseNET will be capable of generating.

- **Ping Delay** sets the amount of time between successive ICMP requests.

- **Timeout** sets the amount of time that GE PulseNET will wait before marking a device as unreachable on the network.

- **Retry Count** sets the number of retries allowed after a timeout is reached.

- **Retry Interval** sets the number of milliseconds to wait before sending a retry query.

- **Retry Timeout** sets the timeout for retries separately from the timeout used on the initial query.
Managing DLINK Settings

Configuring DLINK Properties

DLINK settings can be applied on a global level or to individual authorized masters. The global settings contain the default values that are used when masters are first authorized, or until the settings are changed for an individual master. For more information about changing the settings for individual masters, see Defining Data Collection on DLINK Networks. For additional explanations on features of the GE MDS Diagnostic Link Protocol, see GE MDS publication 05-3467A01, “Network-wide Diagnostics Handbook.”

To change DLINK properties:

- Navigate to Administration > Monitoring Configuration > DLINK Configuration.
- Click DLINK Properties.

In the DLINK Properties display there are four separate sections which can be modified. Click the Update button above each section in order to make changes to the settings.
General DLINK Properties

- **Worker Threads** sets the maximum number of simultaneous DLINK queries GE PulseNET is allowed to make. This value needs to be increased as the number of monitored devices increases. Additional threads consume CPU and memory, so use caution when you increase this value.

- **Default Connection Type** defines whether GE PulseNET will use a Telnet or Raw TCP message format between the server and the Ethernet-to-Serial converter or terminal server.

- **Port** sets the default port which GE PulseNET will connect to on the Ethernet-to-Serial converter or terminal server. This sets a global default, but this value can also be customized for each DLINK Master radio being monitored.

- **Default Discovery Type** sets whether Active or Passive diagnostic messages will be used during device discovery.

- **Default Collection Type** sets whether Active or Passive diagnostic messages will be used during regular performance and configuration polling.

- **Collection Size** sets whether GE PulseNET will collect a limited or extended set of device configuration parameters during a configuration poll.

- **Discovery Request Timeout** sets the time after which GE PulseNET will consider the device unresponsive during the discovery process.

- **Enable Configuration Schedule** tells GE PulseNET whether or not to collect configuration information from the radios.

Active Mode Properties

These properties can be configured separately for Discovery polling vs. regular monitoring collections after the device has been authorized.

- **Request Timeout** sets the time GE PulseNET waits for a response to an active DLINK request.

- **Request Gap** sets the length of time GE PulseNET waits between making active requests for data.

- **Max Attempts** sets the maximum number of DLINK retries before timing out.

- **Max Connection Attempts** sets the maximum number of connection attempts before timing out.

- **Min Unit Address** sets the lowest diagnostic unit ID of a range of IDs to be queried.

- **Max Unit Address** sets the highest diagnostic unit ID of a range of IDs to be queried.
Sleep Mode Properties

These properties can be configured separately for Discovery polling vs. regular monitoring collections after the device has been authorized.

- **Request Timeout** sets the time GE PulseNET waits for a response on a DLINK request to a sleeping device.
- **Wake Gap** sets the length of time GE PulseNET waits between sending wake up messages to a device in sleep mode.
- **Wake Iteration** sets the number of wake up messages GE PulseNET can send to a DLINK device in sleep mode.
- **Sleep Inhibit Interval** sets the maximum length of time GE PulseNET keeps a sleep-mode device awake to collect data. The system wakes the device again if the collection has not finished in this amount of time.
- **RSSI Timeout** sets the amount of time GE PulseNET waits before requesting an RSSI register after the device has been awakened.

Passive Mode Properties

These properties can be configured separately for Discovery polling vs. regular monitoring collections after the device has been authorized.

- **Request Timeout** sets the time GE PulseNET waits for a response to an passive DLINK re- quest.
- **Response Gap** sets the minimum time between collecting one metric and querying for the next metric.
- **Repeats** sets the maximum number of DLINK retries.
- **Repeat Interval** sets the time GE PulseNET must wait before requesting the next metric from the list of devices.
- **Forgive Missed Polls** sets the number of times a device can fail to respond to consecutive requests before it is marked as unavailable.
- **Poll Timeout** comes into play when GE PulseNET has not received a response from any of the devices on the Master. This usually indicates that the Master itself is unresponsive.
- **Auto-Discovery Timeout** sets the amount of time GE PulseNET waits for device information during auto-discovery.
Adding DLINK Master Seeds

To monitor DLINK devices, master seed settings must be defined so that GE PulseNET knows how to send DLINK protocol queries to the diagnostic interface on the Master device.

Navigate to Administration > Monitoring Configuration > DLINK Configuration > Master Seeds. On the Master Seeds table, click + Add for manual configuration or click Import to have GE PulseNET read a list of Master Seeds from a file.

To add a DLINK Master Seed:

- Enter one or more IP addresses which have common settings.
- Enter the port on the terminal server which connects to the diagnostic interface on the Master.
- If you want passive discovery to be the default method, leave the Passive Discovery checkbox selected. Clear the checkbox if you want active discovery to be the default.

Be aware that the choice between active and passive discovery can significantly affect the length of time that the discovery process takes and the impact that the discovery process has on your network. For more information about passive and active discovery, see Device Discovery.

- In the Collection Repeat Interval
field, enter the default value you would like to set for the Master devices using this/these IP addresses. See Configuring DLINK Properties above.

- Check the Sleep Mode Network box if the radio network is in sleep mode. Clear the checkbox if the radio network is not in sleep mode.
- Select the default type of DLINK connection (Raw TCP or Telnet format).
- Click ✨ Save.

Each Master Seed row in the table can be copied, edited, or deleted individually.

Copying a Master Seed Setting

- In the Master Seeds table, click the 📄 Copy icon on the row which you want to copy.
- Change any settings as required and click ✨ Save.

Editing a Master Seed Setting

- In the Master Seeds table, click the ☑️ Edit icon on the row which you want to edit.
- Change any settings as required and click ✨ Save.

Deleting a Master Seed Setting

- In the Master Seeds table, click the ⚠️ Delete icon on the row which you want to remove.
- Click Yes to confirm deletion.

Planning Data Collection on DLINK Networks

There are a number of factors that you should consider when planning data collections for monitored DLINK networks. You must understand the physical arrangement of the devices in your environment and their relationships to each other. Identify the way in which the applications are operating and polling over the network in order to determine how GE PulseNET should collect diagnostic data. The following network types are defined below: Rarely Polled, Frequently Polled, and Sleep Mode networks.

Rarely Polled Networks

Rarely polled networks typically have very little traffic most of the day with the exception of increased traffic at specific times. These networks are good candidates for active data collection. To collect actively, GE PulseNET requests data from each device directly and
puts extra traffic on the network. Active data collection is fast and reliable, but it can impact other traffic that may be flowing through the device at the same time.

Key Considerations:

- **Schedule** — Use careful scheduling to control collection times and avoid impacting critical network operations. You can independently schedule performance and configuration data collection to occur either on a frequency (for example, every 20 minutes), or on a pre-defined schedule.

- **Request Timeout** — The length of time that GE PulseNET waits for a response from the device. Remember to consider latency within your network because of the distances between devices, and also the number of gateways or repeaters that may be deployed.

- **Request Gap** — The length of time that GE PulseNET waits between data requests. A larger request gap means that it will take longer to retrieve all the data for the devices. However, a larger gap also reduces the intrusiveness of the data collection, relieving network performance. If you need to configure data collection using the frequency technique, you may need to select a larger request gap.

**Frequently Polled Networks**

Frequently polled networks typically carry large amounts of SCADA traffic. Finding opportunities to schedule active collection may be difficult because active collection can be intrusive regardless of when it occurs. In frequently polled networks, passive data collection is recommended. When you use passive data collection, GE PulseNET’s data requests are appended to existing application traffic. As a result, GE PulseNET only receives responses when there is traffic on the monitored network and each radio has an application response to send.

Key Considerations:

- **Data Freshness** — GE PulseNET requests information from DLINK devices one item at a time. Responses are received only when application data is flowing on the network. If GE PulseNET needs to collect four data points at a time, and your application polls twice a day, it may take two days before a specific data value is refreshed.

- **Timeouts** — GE PulseNET uses a round-robin style of data collection. Timeouts should be configured to reasonably reflect the amount of delay expected between responses from different devices on your network. Timeouts that are too short results in incomplete data collection and the devices may be marked as unavailable. If you have a layered gateway or repeater devices, multiple SCADA data collection cycles may be required before all the devices send back the requested performance data to GE PulseNET. With these
configurations, the timeout value may need to be set as a multiple of your application polling frequency.

- **Forgive Missed Polls** — The value of this parameter determines how quickly a device is marked as unavailable. If a device misses the specified number of consecutive data collection requests, it is considered unavailable.

### Sleep Mode Networks

Sleep mode networks typically have limited access to power. These networks are often configured to operate in a low-power mode most of the time and are awakened periodically for scheduled activities. These networks require special handling in GE PulseNET and should be monitored with care. Active data collection must be used for these networks.

Passive collection can be used if the sleep mode network is awake at regular intervals, for example if devices are scheduled to be awake for 10 seconds and then sleep for 20 seconds. If you use passive collection, the Passive Collection Repeat Interval value should be low so that the request frequency is high and can catch the devices when they are awake.

**Key Considerations:**

- **Scheduling** — Allow sufficient time between your application polling and the schedule for GE PulseNET data collection. Also, consider how the power is consumed for monitoring your devices. Ensure that you leave enough power available for normal application polling.

- **Sleep Inhibit Timeout** — This parameter determines how long the devices stay awake when GE PulseNET attempts to collect monitoring data. If this parameter is too short, some devices will go back to sleep before they have an opportunity to respond; these devices may then reported as unavailable. If the parameter value is too long, you may be consuming more power than necessary when monitoring data.
Device Discovery

This section describes how to:

- Discover SNMP devices
- Discover DLINK devices and allow passive auto-discovery
- Authorize devices
- Decommission devices

Discovering SNMP Devices

To discover devices:

1. Navigate to Administration > Device Discovery > SNMP Discovery.
2. Click the Discover SNMP Devices button.
3. On the SNMP Discovery Request display, specify the SNMP community strings and/or credentials to be used to discover devices. At least one READ credential or community string must be selected. If you are discovering EntraNet devices, at least one WRITE credential must be selected.

The more credentials you specify, the longer the discovery typically runs. If you do not see the SNMP community strings or credentials you need, click the SNMP Properties link at the upper right corner of the display to add them (see Managing SNMP Credentials).

4. Specify the IP addresses to be included in the left panel.

   - To specify a single IP address to be included in the discovery, click Add. Enter the IP address and click Save. The IP address is added to the discovery list.

   **NOTE:** Community strings are disabled if neither SNMP v1 nor SNMP v2c are selected for use in the SNMP Properties section. Credentials are disabled if SNMP v3 is not selected for use in the advanced SNMP settings. For detailed information, see Defining SNMP Properties.
5. Specify any IP addresses to be excluded using the right panel.
6. Repeat, adding as many IP addresses and ranges as necessary, and then click **Start**.

Your discovery request is processed and a list of eligible devices will be displayed in the left panel of the as described below.
Discovered Devices

Discovered devices that can be authorized appear in the list in the left pane of the SNMP Device Selection view (see Authorizing Devices). Discovered devices that are ineligible appear in the Ineligible Devices pane at the right (see Ineligible Devices).

During discovery, in the Discovery Notice Message pane, you are notified about any decommissioned devices that you may want to re-authorize, as well as notifications about any monitored devices that have significant configuration changes. If there are decommissioned devices you want to re-authorize, you can perform discovery to re-authorize them. Also, if you become aware that the configuration for a device has changed and you do not have the information you require to manually edit the configuration, you can perform discovery to acquire the new configuration information.

Ineligible Devices

SNMP devices may be deemed ineligible either because the device is a model that GE PulseNET does not monitor or because GE PulseNET successfully made contact with the device but could not connect to it with the provided SNMP credentials.
Discovering DLINK Devices

There are two on-demand methods for finding DLINK devices: Active discovery and Passive discovery. The difference in these methods is the way the data is retrieved. The discovery method can be defined separately for each master device or globally for all master devices. Review the methods to decide which method is most appropriate for discovering unauthorized devices on your network.

Active Discovery

During active discovery the master device will immediately return information from the remote devices in the network. This discovery method is intrusive because it places addition traffic on the network.

If you have devices that are kept in sleep mode, use active discovery to ensure that the devices require the least amount of wake time. When a device is discovered, it wakes up, sends information, and then quickly returns to sleep mode.

Passive Discovery

Passive discovery sends a broadcast message to all remote devices asking them to return data the next time they have a response to send back to a SCADA application poll. This means that discovery can take longer, but data retrieval is less intrusive to the network.

**NOTE:** After a master is authorized and configured for passive collection continuous auto-discovery is available for all remote devices connected to that master. For more information, see [Continuous Passive Auto-Discovery](#).

Defining the Discovery Method for a Master

To change the global default discovery method, update the DLINK properties. For more information, see [Defining DLINK Properties](#). To define the discovery method for an individual master, check or uncheck the Passive Discovery checkbox when you add the Master Seed for the master radio. For more information, see [Adding DLINK Master Seeds](#). The discovery method can also be changed in the discovery wizard.
Running DLINK Discovery

When the DLINK discovery process starts, GE PulseNET suspends its own scheduled collections for previously authorized DLINK devices. The collections resume automatically when DLINK discovery completes.

To review the radio settings that must be in place before DLINK can be used, see GE MDS publication 05-3467A01, “Network-wide Diagnostics Handbook.” DLINK must be enabled on the radio, and the DTYPE must be ROOT for the master or NODE for the downstream devices.

To discover DLINK devices:

1. Navigate to Administration > Device Discovery > DLINK Discovery.
2. Click the Discover DLINK Devices button. You may select Master devices for discovery using either a Master Seed definition or by specifying the IP address of an SD Master radio.
3. **DLINK Master Seed:** check one or more of the checkboxes for the DLINK master seeds that will be used to discover devices. The more master seeds you specify, the longer the discovery process is likely to take.

   **NOTE:** If you do not see the DLINK Master Seed(s) you need, click the DLINK Properties link at the upper right of the Discovery display to add, copy, or edit a new seed definition. For more information, see Managing DLINK Settings.

4. **SD Radio via IP:** Click the Add button to enter one or more IP addresses for discovery. GE PulseNET will use default values for the additional discovery parameters that are required, which include active polling to port 9999 on the SD radio at that IP address.

   Repeat, adding as many IP addresses and ranges as necessary. You may also specify IP addresses or ranges to be excluded from discovery.

5. If you are using Active Discovery, you can indicate the specific Unit IDs or a range of target Unit IDs for the set of radios you wish to discover. Valid Unit IDs can be in the range of 1 to 65000. If specifying multiple Unit IDs, please separate each Unit ID or ID range with a comma.

5. Click Start to begin the discovery process.
Your discovery request is processed and a list of eligible devices will be displayed in the left panel of the as described below.

**Discovered Devices**

Discovered devices that can be authorized appear in the list in the left pane. For instructions on how to authorize devices, see Authorizing Devices.

During discovery, in the Discovery Progress pane at the top right, you are notified about any decommissioned devices that you might want to re-authorize, as well as about any monitored devices that have significant configuration changes.

If there are decommissioned devices that you want re-authorized, run a discovery
to re-authorize them. Also, if you become aware that the configuration for a device has changed and you do not have the information you require to manually edit the configuration, you can run a discovery to acquire the new configuration information.

Continuous Passive Auto-discovery

Continuous discovery occurs during passive data collection on DLINK master radios that are authorized and configured for this discovery method. To configure passive auto-discovery, see Configuring Data Collection on DLINK Master Devices.

When data is collected passively, new remote devices that have not yet been discovered will be noticed by GE PulseNET as normal data traffic passes across the network. If continuous passive discovery is enabled, the information about new remote devices will be listed. Administrators can view and authorize the newly discovered remote devices by navigating to Administration > Device Discovery > Auto-Discovery. Eligible devices will be displayed in the left panel, where they can be selected and authorized for monitoring.

Authorizing Devices

After discovering the devices in your network, you must authorize them before GE PulseNET can begin monitoring them.

To authorize devices:

1. On the list of discovered devices, select the checkbox for individual devices or click the checkbox in the table header to select all of the devices in the list.
2. Click the Authorize button.
3. Confirm your selections and click Authorize.

A full configuration collection will be automatically started on the newly authorized devices.
Managing Device Settings

Device Administration

GE PulseNET Administrators can decommission a monitored device and configure collections for DLINK masters.

Decommissioning Individual Devices

If you know that a monitored device has been removed from service, you can decommission the device. Decommissioning is also used if you want to swap devices located at the same IP address. The new device must have the same credentials as the monitored device that you are decommissioning. After you decommission the monitored device, the GE PulseNET Administrator needs to discover and authorize the new device at the same IP address. If devices are swapped without first decommissioning the monitored device, GE PulseNET detects the changed MAC address and stops reporting all metrics, except for availability and response time.

To decommission a monitored DLINK device:

1. Navigate to Administration > Device Discovery > DLINK Discovery. Perform a discovery against the device or range of devices that you wish to decommission. This will populate the Already Authorized tab on the discovery menu. Click this tab to access the authorized device list for that range, and use the Decommission icon to remove the desired devices.
   Associated downstream device(s) will also be removed for any decommissioned master.
2. Click Yes to confirm that you want the device(s) decommissioned.

The device will be immediately decommissioned and removed from monitoring.

To re-authorize a decommissioned device, the GE PulseNET Administrator must perform a discovery (see Discovering SNMP Devices or Discovering DLINK Devices.)
Decommissioning SNMP devices from the Authorized Device List

For SNMP devices, navigate to Administration > Device Discovery > SNMP Discovery

Run discovery against the desired device or range, then click the link above the table header which says Already Authorized for Discovery Range.

Click the 🚫 Delete icon and confirm that you want to decommission the device by clicking the Yes button.

Configuring data collection on DLINK master devices

Use the Configure Collection menu option to define the collection type and scope of data collected on an individual DLINK master and its downstream devices. Global default settings are defined in the DLINK Properties section (see Configuring DLINK Properties).

To define the settings for an individual master device:

1. On the Detail view for the master, click the 🗝 Administration menu icon and select Configure Collection from the list.
2. In the Configure Collection display you may edit the current IP address and port number being used to connect to the diagnostic interface on this master radio.
3. Select the appropriate Collection Type (Active or Passive).

**Active Collection Settings**

Changes to these settings will be applied to this Master and all of its downstream devices.
Based on the radio performance and frequency of SCADA polling, you may need to adjust the DLINK Request Timeout, Request Gap, Max Attempts, or Max Connection Attempts, as well as whether the network has been configured in Sleep Mode.

**Passive Collection Settings**

Changes to these settings will be applied to this Master and all of its downstream devices.

Based on the radio performance and frequency of SCADA polling, you may need to adjust the DLINK Response Gap, Repeat Count, Repeat Interval, Forgive Missed Polls, and Poll Timeout.

You can also select the option for Continuous Passive Auto-discovery on this Master and any of its downstream devices. When GE PulseNET broadcasts the passive data collection request, all of the remote devices in the network receive the request, even remote devices that are not yet authorized for monitoring in GE PulseNET. If an unauthorized remote device returns data, the information about that device is collected and stored. Administrators can view and authorize these discovered remote devices at any time by navigating to **Administration > Device Discovery > Auto-Discovery** (see Continuous Passive Auto-Discovery).
4. Choose the Collection Size for configuration data. To minimize the impact of GE configuration collection, you can limit the number of parameters that will be updated during the configuration collection.
   - **Limited**—a smaller selection of configuration parameters is requested and returned for masters and remote devices. The total time to complete a limited collection will be less than for an extended collection.
   - **Extended**—all available configuration parameters are requested and returned for masters and remote devices. The total time to complete an extended collection will be greater than for a limited collection.

5. Next you can specify whether GE PulseNET should ask the devices for their configuration information. If Enable is checked, then you can enter the collection schedule that you want GE PulseNET to use for obtaining configuration data. For more information about using the scheduling tool, see Scheduling Device Data Collection.

6. Finally, set the collection interval on which GE PulseNET will ask devices for their Performance information.

7. Click **Save** to save the updated Collection Configuration for this Master.
Managing System Schedules

GE PulseNET contains a number of predefined schedules which can be used during the process of scheduling reports. These schedules are different than the ones previously discussed for configuring GE PulseNET’s collection schedules, and they include useful definitions such as the beginning of a day, first day of the month, weekends, hourly, and daily during business hours. The timezone for these schedules is inherited from the GE PulseNET server time.

Adding a new System Schedule Definition

You can add to the list of predefined system schedules by clicking the + Add button.

To define the settings for a new system schedule:

1. Select the Schedule Type (Trigger or Window). These are identical except for the addition of a time duration field for a Window schedule.
2. Enter a Name for the new schedule.
3. Provide a description for this schedule.
4. Select a Recurrence Pattern from the dropdown list. The scheduling options will change based on the type of pattern you choose.
   - Once: This option allows you to set the start day/time for a single occurrence.
• **Periodical:** You can set the start and stop day/times, as well as configuring the time at which the event will recur (HH:MM).

• **Daily:** Specify the start and stop day/times, then configure the number of days when the event will recur, or the specific day(s) of the week on which the event will recur, or the days of the month when the daily event will recur. You also can limit the daily event to a specific hour of the day.

• **Weekly:** Set the start and stop day/times, then select how many weeks between occurrences, the specific day(s) of the week, and the exact time of day when the weekly event will recur.

• **Monthly:** Set the start and stop day/times, then select either the day of the month or the day of a week during that month, and finally set the exact time of day when the monthly event will recur.

• **Yearly:** Set the start and stop day/times, then select either the day of the month or the day of a week during that month, and finally set the exact time of day when the yearly event will recur.

5. If a Window schedule is being defined, enter a time duration during which the event is allowed to run (minutes, hours, days, weeks, months, or years).

6. Click 📄 Save to save the new schedule.

**Editing a System Schedule Definition**

Predefined schedules can be edited by clicking the ☑️ Edit icon on the row you want to update. Even though you are not allowed to change the schedule name, you may need to change the description depending on the type of modification you make to the existing schedule.

**Deleting a System Schedule Definition**

You may delete a schedule by clicking the ⚠️ Delete icon for the row you want to remove. Click Yes to confirm that you want to delete the row.
Getting Support

If problems arise, diagnostic data can be gathered and saved as a collection of files called a support bundle. These support bundles can then be forwarded to the GE MDS Technical Support team to aid in determining and correcting the problem. Each support bundle contains a diagnostic snapshot of the GE PulseNET Management Server and log files.

Generating a Support Bundle

It is not difficult to generate a support bundle, but it does take time. The time it takes to generate a support bundle depends on the number of monitored devices and the length of time the system has been monitoring those devices.

To generate a support bundle:

1. Navigate to Administration > Support.
2. On the Support view, click Generate Support Bundle.
3. When prompted, you may either view the support bundle using a local archive manager or download it.

Enabling Debug Mode

Click on the red “on” hyperlink to enable Debug Mode. In the dialogue box that appears, select a maximum runtime for Debug Mode from the drop-down menu. Click OK. Please keep in mind that Debug Mode may cause slowdowns in your system’s performance.
About GE MDS

Over two decades ago GE MDS began building radios for business-critical applications. Since then we have installed millions of radios in countries across the globe. We overcame impassable terrain, brutal operating conditions, and complex network configurations to succeed. We also became experts in wireless communication standards and applications worldwide. The result of our efforts is that today thousands of organizations around the world rely on GE MDS wireless networks to manage their 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 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 applications. GE MDS is also at the forefront of wireless communications for private and public infrastructure and online transaction processing. 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.

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 engage in a relationship that is forthright and ethical, one that builds confidence and trust. Data sheets, frequently asked questions, application notes, firmware upgrades and other updated information is available on the GE MDS Web site.

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 using. 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 below. In addition, manual updates can often be found on the GE MDS Web site.

About End 2 End Technologies

End 2 End (E2E) Technologies offers a unique combination of wireless communications and information technology expertise. We improve efficiency, reduce risk and lower the cost of industrial field operations via modernization and management of our customer’s wireless communications networks. From initial planning through lifecycle support we assist your team in adopting a wireless solution that keeps communication costs low while maximizing network reliability and performance. For more information visit us at www.e2etechninc.com.

Customer Support

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

Phone: 585-241-5510  
Email: gemds.techsupport@ge.com  
Fax: 585-242-8369

License Credits

GE PulseNET contains several third party components. Please refer to the complete list of these components at www.e2etechninc.com/index.php/about/legal.