# TABLE OF CONTENTS

## INTRODUCTION
- What is GE PulseNET? ......................................................... 8
- Understanding GE PulseNET Roles ....................................... 8
- GE PulseNET Documentation
  - Release Notes .......................................................... 9
  - Installation Guide ....................................................... 9
  - User Guide .................................................................. 9
  - Administration Guide ..................................................... 10

## GETTING STARTED
- Starting GE PulseNET ....................................................... 11
- Stopping GE PulseNET ...................................................... 11
- Using the Administration Dashboard .................................... 12

## WORKING WITH LICENSES
- Requesting Licenses ......................................................... 14
- Adding Licenses ............................................................. 15
- Managing Licenses .......................................................... 15
  - Requesting Replacement Licenses .................................. 16

## SYSTEM CONFIGURATION
- Email Configuration .......................................................... 17
  - Define Email Settings .................................................. 17
- Managing System Schedules .............................................. 18
  - Adding a New System Schedule Definition ..................... 19
    - Define settings for new system schedule .................... 19
  - Editing a System Schedule Definition .......................... 20
  - Deleting a System Schedule Definition ........................ 21
- Google Maps API Configuration ........................................ 21
- Service Monitoring .......................................................... 21
- Custom Data Configuration ............................................... 22
Create a Custom Data Field
Edit a Custom Data Field
Delete a Custom Data field
SNMP Trap Configuration
  Outgoing Tab
  Incoming Tab
Certificate Management
Complementary Database
API Tokens
System Configuration Summary
Syslog Configuration
Syslog Rules

WORKING WITH USERS
Managing User Roles
Managing User Groups
Creating Users
  Create a New User
Managing Users
Configuring Password Policy
Setting User Session Timeout
Configuring LDAP
  Configure LDAP Server Information
  Find LDAP User Groups
  Assign Permissions (Roles) to LDAP Groups
  Finding LDAP Users
LDAP User Groups
Enabling RADIUS Authentication
  Enable RADIUS Authentication
  Define User Roles

WORKING WITH RULES
Predefined Rules
Bulk Enable/Disable/Delete
  To enable rules
  To disable rules
  To delete rules
Quick Update for Rule Settings
  Configure thresholds for a rule
Fire Strategy Values 50
Enabling Email for Rules 50
Full Update for Rule Settings 51
Editing Rule Defaults 53
Editing Severity Conditions and Thresholds 54
Action Icons for Rules 56
Reprioritize Rule Evaluation Order 56
Copy Rule Definitions 56
Edit Rule Definitions 56
Delete a Rule 56
Enable/Disable a Rule 57
Show Device Selector List 57

COLLECTION SCHEDULES 58
Scheduling Device Data Collection 58
Configure a Data Collection Schedule 58

MONITORING CONFIGURATION 61
Defining SNMP Properties 61
Configure SNMP Settings 61
Managing SNMP Credentials 62
Managing SNMP v1 or v2c Community Strings 62
Add an SNMP Community String 62
Edit an SNMP Community String 63
Delete an SNMP Community String 63
Managing SNMP v3 Credentials 63
Add SNMP v3 Credentials 63
Edit SNMP v3 Credentials 64
Delete SNMP v3 Credentials 64
Migrating Devices to New SNMP Credentials 65
Managing ICMP Settings 66
Configure ICMP Settings 66
Managing NETCONF Settings 67
Configure NETCONF Settings 67
Managing DLINK Settings 67
Configuring DLINK Properties 67
Change DLINK Properties 68
General DLINK Properties 68
Active Mode Properties 69
Sleep Mode Properties 70
Passive Mode Properties 71
Adding DLINK Master Seeds 71
Add a DLINK Master Seed 72
Copying a Master Seed Setting 73
Editing a Master Seed Setting 73
Deleting a Master Seed Setting 73
Planning Data Collection on DLINK Networks 73
Rarely Polled Networks 73
Frequently Polled Networks 74
Sleep Mode Networks 75

MANAGING DEVICE FILTERS 76
View Device List for a Filter 76
Copy an Existing Filter 76
View a Filter Definition 76
Edit a Custom Filter Definition 76
Delete a Custom Filter Definition 76
Adding Device Filters 77

MANAGING DEVICE BACKUP 80
Add a Device Configuration Backup 81

MANAGING DEVICE GROUPS 82
View Device List for a Group 82
Edit Device Group Definition 82
Delete Device Group 82
Adding Device Groups 83

CHANGE MANAGEMENT 84
Configuring Change Management 84
Managing Firmware Servers 86
Manage Firmware Servers 86
Managing Change Templates 88
Add a Configuration Change Template 88
Add a Password Change Template 91
Add a Firmware Change Template 91
Add a Certificate Import Change Template 92
Managing Change Requests 93
Adding a Configuration Change Request 93
Adding a Password Change Request 95
Adding a Firmware Change Request 96
Adding a Restart Device Change Request 97
Managing Change Requests 98
Editing SD Devices from the Device Details Page 100
   Make Changes to Individual SD Device 100

ACCESS CONTROL 101
   View Access Control Properties 101
   Delete Access Control Records 101
   Edit Access Control Records 102
   Add Access Control Records 102
   Adding an Access Control Record 102

DEVICE DISCOVERY 104
   Discovering SNMP Devices 104
      Discover SNMP Devices 104
      Discovered Devices 105
      Ineligible Devices 106
   Discovering DLINK Devices 106
      Active Discovery 106
      Passive Discovery 107
      Defining Discovery Method for a Master 107
      Running DLINK Discovery 107
         Discover DLINK Devices 108
         Discovered Devices 108
   Discovering DLINK Redundant Clusters 110
      Continuous Passive Auto-Discovery 111
      Trigger Force Compliance 112
   Authorizing Devices 113
      Authorize Devices 113
   Working with Redundant Clusters 113
      Creating a New Hot Redundant Cluster 114
      Triggering Config Collection for Redundant Cluster 117
      Triggering Performance Collection for Redundant Cluster 118
      Editing Collection Configuration 118
      Editing Redundant Clusters 118
         Edit a Redundant Cluster 118
      Moving Redundant Clusters to Staging or Production 119
Creating Maintenance Windows for Redundant Clusters 119
Decommissioning Redundant Clusters 119

MANAGING DEVICE SETTINGS 120
Device Actions 120
Decommissioning Individual Devices 120
  Decommission a Monitored Device 120
Decommissioning SNMP devices from the Authorized Device List 121
Configuring data collection on DLINK master devices 121
Define Settings for an Individual Master Device 121
  Active Collection Settings 121
  Passive Collection Settings 122
Triggering Data Collections 123
  Trigger an On-demand Configuration Collection 123
  Trigger an On-demand Performance Collection 123
Trigger Compliance Checks 123
  Trigger a Compliance Check for a Device 123

GETTING SUPPORT 124
  Generating a Support Bundle 124
  Generate a Support Bundle 124
  Enabling Debug Mode 124

APPENDIX 124
  Traps Format 125
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. The User Guide includes:
- 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.
Administration 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 a GE PulseNET administrator. It provides links to other dashboards where you can accomplish administrative tasks.

This dashboard provides the following links:

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

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

**Device Groups** — for defining GE PulseNET device groups

**Filters** — for creating and saving filter definitions

**Access Control** — for granting users access to specific dashboards and features

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

**Report Management** — for creating, generating, scheduling, and managing reports and viewing audit logs. See the [GE PulseNET User Guide](#) for additional details.

**User Management** — for creating, configuring, and maintaining GE PulseNET users, roles, groups, and policy settings
System Configuration — for configuring email settings, managing system schedules, installing and managing system services, entering Google Map premier client ID, and viewing a summary of the GE PulseNET system configuration

Change Management — for viewing and managing device change requests and settings

Licensing — for requesting, installing, and managing GE PulseNET 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 sends a replacement GE 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 device during the authorization process.
SYSTEM CONFIGURATION

Email Configuration

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

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.

GE 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>Mail Server</th>
<th>The host name or IP address of the mail server to be used for sending email.</th>
</tr>
</thead>
<tbody>
<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 GE PulseNET email notifications. Separate multiple email addresses with a comma.</td>
</tr>
<tr>
<td>Mail Server Port</td>
<td>The port number that GE PulseNET uses to communicate with the mail server.</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------------------------------------------</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>Enable STARTTLS?</td>
<td>Indicates whether you want to enable the START-TLS protocol and use encryption when sending emails from GE PulseNET.</td>
</tr>
<tr>
<td>Enable SSL?</td>
<td>Indicates whether you want to enable the SSL protocol and use encryption when sending emails from GE PulseNET.</td>
</tr>
<tr>
<td>Mail Server Login</td>
<td>The user name of the email account required by the mail server in order to send email.</td>
</tr>
<tr>
<td>User Password</td>
<td>The password for the above user account.</td>
</tr>
</tbody>
</table>

**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, the 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.

Define settings for 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.
   a. **Once**: This option allows you to set the start day/time for a single occurrence.
   b. **Periodical**: You can set the start and stop day/times, as well as configuring the time at which the event will recur (HH:MM).
   c. **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.
   d. **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.
   e. **Monthly**: Set the start and stop days/times, then select either the day of the month or the day of the week during that month, and finally set the exact time of day when the monthly event will recur.
   f. **Yearly**: Set the start and stop days/times, then select either the day of the month or the day of the 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.

Google Maps API Configuration

To enable enhanced Google Maps API functionality and acquire access to additional support, you must obtain and add a Premier Client ID.

For more information about Google Maps API options, see the Google maps website: developers.google.com/maps/documentation/javascript/usage#usage_limits

Service Monitoring

When GE PulseNET is installed, the software creates many services which are required for it to operate. These services each have responsibilities such as collecting, storing, and processing data. Services are configured to start automatically on installation and when the system reboots. If a service stops running, it may cause disruption to the operation of other services and the data that is available in the user interface.

To monitor the installed services, navigate to Administration > System Configuration > Service Monitoring. This view allows for the state of all services to be displayed.

If a service is in a Failed or Not Running state, it can be restarted manually using the Windows Services tool or on Linux using the System V 'service start/stop' commands.
Services which are in a bad state will also show in the Notification Area window. To navigate to this window, look for the red bubble icon in the top-right of your screen. The Notification Area icon is displayed on all views and dashboards.

Click the red bubble Notification Area icon to show the System Notifications window. This window will display the services that are not currently running.

**Custom Data Configuration**

You may want to store device information that GE PulseNET does not collect. For that purpose, you can create up to ten device Custom Data Fields in the Custom Data Configuration window.

Navigate to Administration > System Configuration > Custom Data Configuration.
Create a Custom Data Field

1. In the Custom Data Configuration menu, click Add.
2. In the Add Custom Data Field dialog box that opens, type a label for the field in the Field Label field.
3. If you want the field to be visible in the Summary View for applicable devices, select the Visible in Summary View checkbox. For more information on the Summary view, see the Working with GE PulseNET section of the GE PulseNET User Guide.
4. Click Save.

The new field is added to the Custom Data Field tab on the Device Detail View for every monitored device and, if you select the Visible in Summary View check box, as a column in the Summary view for applicable devices.
Edit a Custom Data Field

1. In the **Custom Data Configuration** menu, click the **Edit** icon for the data field you want to edit.
2. In the **Edit Data Fields** dialog box that opens, edit the label for a field by clicking the present label and typing over it.
3. If you want the field to be visible in the **Summary View** for applicable devices, select the **Visible in Summary View** checkbox. If not, clear that check box. For more information on the Summary view, see the **Working with GE PulseNET** section of the **GE PulseNET User Guide**.
4. Click **Save**.

Fields that were created by the Administrator will become available for Operators to edit on the **Custom Data Field** tab on the **Device Detail View** for every device in the network (see the **GE PulseNET User Guide** for details).
Delete a Custom Data field

1. In the **Custom Data Configuration** menu, click the **Delete** icon in the data field you would like to delete.

2. In the **Delete Item** dialogue box that appears, confirm that you want to continue to delete the data field by clicking the **Delete** button. Click the **Cancel** button to abort deletion of the data field.

3. The data field will now be deleted from the GE PulseNET browser interface.

4. Click **Save** 📄.
SNMP Trap Configuration

The SNMP Trap Configuration dialog provides information about incoming and outgoing alert messages from remote Simple Network Management Protocol (SNMP) enabled systems. SNMP is one possible protocol that devices can use to communicate. Navigate to Administration > System Configuration > SNMP Trap Configuration. NOTE: Refer to Appendix A for the traps format.

Outgoing Tab

In the Outgoing Tab, you can enable and define where you send your outgoing alerts, including the destination and credentials for your messages. When the Forward External Alerts checkbox is not selected, trap messages are sent only when PulseNET Enterprise rules generate alerts. When the Forward External Alerts checkbox is selected, PulseNET Enterprise will also send alerts received from the external devices.

Click the Send Test Trap button to test the trap message. To confirm your trap messages are being sent, verify the test message has been received.

Incoming Tab

In the Incoming Tab, you can enable and define how you receive incoming traps as device alerts, including the incoming trap port and credentials.

NOTE: GE PulseNET can receive traps from any device and generate a general alert but only the following devices support open/close alerts and more details: iNET, Mercury, EntraNET and TD220X access points.
Certificate Management

The Certificate Management window allows for the management of Simple Certificate Enrollment Protocol (SCEP) security certificates and firmware certificates on the GE MDS Orbit devices. To manage your certificates, navigate to Administration > System Configuration > Certificate Management.

The Certificate Renewal checkbox tells GE PulseNET that security certificates should be automatically renewed if they are within a few days of expiration. The period of renewal can be defined in the Security Certificate Pre-expiration Window (days) field.

The remaining fields in the Security Certificates Panel allow you to modify the individual security certificate attributes, if needed.

The Certificate Retrieval checkbox tells GE PulseNET that firmware certificates should be retrieved automatically from devices.

Select when you would like the security and firmware certificates to be retrieved from the Retrieval Schedule dropdown menu.
Complementary Database

To connect and populate a complementary database, navigate to Administration > System Configuration > Complementary Database. GE PulseNET supports a complementary database for carrying alert history, device configuration and performance information only.

In the Complementary Database Configuration window, fill in the required fields. In the Database field, you can select to populate either an Oracle or MSSQL complementary database. In the following fields, enter the IP Address, Port, Username and Password.

**NOTE:** When you connect and populate an MSSQL server, PulseNET will connect to your default database. If you set the PulseNET database as your default database, then PulseNET will automatically connect to that database.

Click the Validate button to continue. GE PulseNET will now attempt to connect to the external Complementary Database and create the necessary tables in the database.

Once the connection is successful, the data will be inserted and updated in near real-time. GE PulseNET will not manage its own data. In order to control the size of the complementary database and to maintain optimal performance, a database administrator will need to routinely remove old data as needed.

**API Tokens**

An API token is a unique identifier created by GE PulseNET in order for other applications to request access to the software. If at any point you would like to integrate another piece of software with PulseNET, you will need to generate an API token and provide that token to the other application. To generate an API Token, navigate to Administration > System Configuration > API Tokens. The API Tokens dialog box automatically creates a random Token ID.
In the **API Tokens** dialog box, you can view your unique **Token ID** in the first field. The **Name** field allows you to add a descriptive name to your token ID to help you remember what it will be used for. The **Expires At** field allows you to set an expiry date for your token to determine at which point it will no longer work. In the **Permissions** drop-down menu, you can determine which privileges your token will provide.

**Readonly:** The software will only be allowed to view information. For example, it will be able to gather device information or view the current system debug level.

**Device:** The software will be able to perform modifications to devices. For example, it will be able to add a new device to the system or trigger a configuration poll.

**System:** The software will be able to perform modifications to the PulseNet system itself. For example, it will be able to change the system debug level or add a new license.

The **Token ID** table lists and describes all of your unique token IDs. The table contains all of the above information for each token and each column is sortable by clicking on the heading title. The **Last Used** category is useful when setting up an API token in order to ensure it is working properly. It will display the last date GE PulseNet received a call from that specific token ID and the status of the last call.
System Configuration Summary

The **System Configuration Summary** provides information about the machine(s) on which GE PulseNET was installed. This includes information on the operating system, filesystem path, and network address of the GE PulseNET system. To view the **System Configuration Summary** window, navigate to **Administration > System Configuration > System Configuration Summary**.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>WINDOWS</td>
</tr>
<tr>
<td>IP Address</td>
<td>10.1.0.57</td>
</tr>
<tr>
<td>Home Path</td>
<td>C:GE_MDS\pulseNET\</td>
</tr>
<tr>
<td>Home Name</td>
<td>PERFTEST\INSRV12</td>
</tr>
<tr>
<td>OS</td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>Windows Server 2012 R2</td>
</tr>
<tr>
<td>Patch</td>
<td>6.3</td>
</tr>
<tr>
<td>High Availability</td>
<td></td>
</tr>
<tr>
<td>Status</td>
<td>false</td>
</tr>
<tr>
<td>Peers</td>
<td>0</td>
</tr>
<tr>
<td>Database</td>
<td></td>
</tr>
<tr>
<td>Host</td>
<td>127.0.0.1</td>
</tr>
<tr>
<td>Port</td>
<td>27017</td>
</tr>
<tr>
<td>Database Name</td>
<td>stingray</td>
</tr>
<tr>
<td>User</td>
<td>stingray</td>
</tr>
<tr>
<td>Embedded</td>
<td>true</td>
</tr>
</tbody>
</table>
Syslog Configuration

Syslog Configuration provides information about where and how to send syslog messages and what to do with those messages once they are sent. This includes the endpoint or Port Number, the Thread Count, the Number of Days to Keep Logs, and the Purge Schedule. To view the Syslog Configuration window, navigate to Administration > System Configuration > Syslog.

NOTE: Consider the size of your database when setting your purge schedule and log records. A longer record-keeping period will use more disk space while a shorter record-keeping period will use less space.

Syslog Rules

The Syslog Rules summary allows you to create, view, and manage syslog rules. Syslog rules determine what action GE PulseNET takes when it receives a message, and which messages trigger that action. To view the Syslog Rules window, navigate to Administration > System Configuration > Syslog Rules.
To create a new syslog rule, click the Add button. In the Syslog Rule window, set the rule Name and Description and select the Device Group, Device Filter or Devices. Click the Add button.

In the Add Syslog Rule Filter and Action(s) window, set the parameters of your Syslog Rule. Syslog Rule Filters determine which messages trigger the actions, either a log message or an alert. Any messages that do not match the filters are discarded. Select Log to trigger a log message to the database and Alert to trigger an Alert. Click Save to create the rule.

**NOTE:** The syslog protocol version RFC3164 is recommended for Orbit devices.
WORKING WITH USERS

GE PulseNET controls user access to the web interface using the concept of users, groups, and roles. When administrators create new users, a role and/or group can be assigned to the user. The assigned role/group determines the features and views that users can access when they log in to GE PulseNET.

Managing User Roles

GE PulseNET has two default roles: Administrator and Operator. These roles allow each set of users to have the privileges they require in order to accomplish tasks related to GE PulseNET application administration, device management, and monitoring. Administrator users typically have full privileges to accomplish all tasks. Operator users typically have read-only access to view collected data and reports.

For most customers, the two default roles will be adequate to delineate the needs of their GE PulseNET users. However, GE PulseNET also provides Administrators with the ability to create custom roles as needed. To create a new role, click the Add button at the upper left corner of the user roles table to enter the unique name of the role and its description.

Managing User Groups

GE PulseNET user groups are defined based on the roles that have been created. GE PulseNET has two default user groups (Administrator and Operator) which correspond to the Administrator and Operator roles. These groups provide a higher level of abstraction for defining user privileges, since a single user group can consist of multiple user roles.

For most customers, the two default user groups will be adequate to delineate the needs of their GE PulseNET users. However, GE PulseNET also provides Administrators with the ability to create custom groups as needed. To create a new group, click the Add button at the upper left corner of the user groups table to enter the unique name of the group and its description. Then select the different user roles which will be members of
the group.

**Creating Users**

**Create a New User**

1. Navigate to Administration > User Management > Users
2. Click the *Add* button
3. Enter a unique name for the new user
4. Enter the user’s email address (if desired)
5. Enter a GE PulseNET password for this user, then confirm the password on the next line
6. Assign the new user one or more roles. Administrators also have access to all operator functionality.
7. You can optionally assign the new user to one or more user groups
8. Click *Save* 🛡️.

The new user now appears in the users table.

**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 **Copy** icon to make a duplicate of an existing user account
- Click the **Edit** 📝 icon to change account details (name, role, password)
- Click the **Delete** 🗑️ icon to remove an 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.
Configuring LDAP

Instead of duplicating your existing Lightweight Directory Access Protocol (LDAP) or Active Directory users in GE PulseNET, you can configure GE PulseNET to authenticate directly to your LDAP or Active Directory server. GE PulseNET supports Lightweight Directory Access Protocol (LDAP version 3) compatible directory services, including Active Directory, Sun Java Systems Directory Server, OpenLDAP, and Novell eDirectory.

You need to be familiar with the details of your LDAP directory service to set the appropriate configuration parameters in GE PulseNET. The following considerations are important when planning to integrate an external directory service with the GE PulseNET:

- Secure LDAP is supported, but not required
- LDAP with Transport Layer Security is not supported
- A persistent connection to the LDAP server is not required

LDAP groups can be imported into GE PulseNET and assigned GE PulseNET roles. This allows for users who have been granted special permissions within an organization to have associated permissions in GE PulseNET.

User credentials continue to be managed on the LDAP server. Any password changes in the LDAP directory service are transparent to GE PulseNET. After a password change in the directory service, that user can log into GE PulseNET with the new password, while any attempts to use the old password will fail. If a user account is removed from the directory service, any login requests with those credentials result in a login failure in GE PulseNET.

Similarly, if the LDAP authentication service is down, GE PulseNET cannot authenticate users whose accounts are defined there. At the same time, any internal GE PulseNET users, such as the built-in admin user or any accounts that you create manually using the Manage Users dashboard, are unaffected during LDAP authentication service interruptions.
Configure LDAP Server Information

The first window in the LDAP Configuration Wizard allows you to configure your connectivity and login with your LDAP server.

1. Navigate to Administration > User Management > LDAP Configuration.
2. In the LDAP Configuration Wizard window, select the Type of LDAP server, either Active directory or other.
3. In the Primary Host field, select Ldap or Ldap over SSL.
4. In the Primary Host Port field, your default port will appear.
5. If you have a failover server, enter the details in the Secondary Host and Secondary Host Port fields.
6. In the Base DN field, enter the distinguished name (DN) of the service account to fetch users and groups. In Active Directory, typically a common name (CN) is used instead of DN. For example: CN=John Smith, OU=Employees, DC=company, DC=com.
7. If you enable the Anonymous checkbox, GE PulseNET will use an anonymous service account to search for users in the extended directory. The default user name for anonymous service accounts is _anonymous_ and enabling this option sets the Distinguished Name of the service account to _anonymous_.
8. In the Username and Password fields, enter the username and password of the service account used for user searching in the external directory.
9. Click the Test button to test your system connection and login credentials for your LDAP server. If the Test is successful, proceed to the next step.
10. Click the Next > button.
Find LDAP User Groups

The second window in the LDAP Configuration Wizard allows you to grant Users proper permissions after login by querying for Groups and looking for their assigned permissions.

1. In the Group DN field, enter the search path for groups identified in your LDAP server. For example: OU=Groups, DC=2k3, DC=dom. The order in which the groups are searched is determined by the order of the groups listed in these settings. The Group Search DN 2 and 3 fields are optional.

2. In the Group Name Attribute-ID field, enter the Attribute-ID for finding Groups in the external directory. The default for Active Directory is “CN.”

3. In the Group Member Attribute-ID field, enter the Attribute-ID for finding Group Members in the external directory. The default for Active Directory is “member.”
4. In the **User Member Attribute-ID** field, enter the Attribute-ID for finding Users in the external directory. The default for Active Directory is “member.”

5. To ensure the paths are correct for finding Groups, in the **Group Name** field, enter the name of a Group to search. Click the **Search** button. If the search is successful, the **Test Search for Group** dialog box will indicate “Group found!” and list the Group Members including the Users and any Subgroups.

### Assign Permissions (Roles) to LDAP Groups

The third window in the **LDAP Configuration Wizard** allows you to assigned permissions (roles) to LDAP Groups.
1. Select the LDAP Groups to which you will assign roles by clicking the checkbox.
2. Click the **Assign** button.
3. In the **Select Role** window, select the role you will assign to the selected LDAP Groups by clicking the checkbox.
4. Click **Save**.
5. To remove a role from a Group, select the LDAP Group by clicking the checkbox. Then, click the **Unassign** button.
6. Click the **Next >** button.

**Finding LDAP Users**

The fourth window in the **LDAP Configuration Wizard** allows you to find LDAP Users.

1. In the **User Search DN** field, enter the search path for users identified in your LDAP server. For example, in Active Directory, if the CN user accounts are defined in the `sAMAccount=Users` group, and the Active Directory domain is `example.com`, apply the following: `CN=Users,DC=example,DC=com`
2. In the **Username Attribute-ID** field, enter the Attribute-ID which contains the Username. For example, in Active Directory, the default is `sAMAccountName`. 
3. In the **Group Membership Attribute-ID** field, enter the Attribute-ID which includes the Group Membership. For example, in Active Directory, the default is memberOf.

4. In the optional **Email Attribute-ID** field, enter the Attribute-ID which includes the User’s Email. For example, in Active Directory the default is mail.

5. To ensure the paths are correct for finding Users, in the **Username** field, enter the name of a User to search. Click the **Search** button. If the search is successful, the **Test Search for User** dialog box will indicate “User found!” and list the Username, User Roles, and Email Address.

6. In the **LDAP Configuration Wizard** window, click the **Finish** button.

**NOTE:** All credentials and permissions are controlled by the LDAP server. Each time a user logs in, GE PulseNET will check their credentials and the User Roles designated by LDAP, and update their permissions in PulseNET.

If you are configuring GE PulseNET to use secure LDAP, an additional step is required.

GE PulseNET makes use of the standard Java LDAP service provider using *Java Secure Socket Extension (JSSE)* software for SSL support. To configure secure communication between GE PulseNET and your LDAP server, you need to ensure that the GE PulseNET LDAP client trusts your LDAP server.

To do this, install the LDAP server’s root certificate (CA) in GE PulseNET’s database of trusted certificates.

1. Navigate to `<pulsenet_home>/jre/lib/security`
2. Obtain the CA certificate for your secure LDAP server and make sure it is accessible under `<pulsenet_home>`
3. Use the Java keytool program to import your LDAP server’s root CA certificate into the keystore. Refer to the documentation for the Java keytool command if you need additional information (docs.oracle.com/javase/6/docs/technotes/tools/solaris/keytool.html). If the `jssecacerts` keystore does not exist, the following commands will create it. If it already exists, be sure you have the existing keystore password to access it.
a. `<pulsenet_home>\jre\bin\keytool -import -file
<path_to_ldap_server_CA_file>\<root_CA_Cert_filename>.crt-keystore jssecacerts`
b. Enter the `jssecacerts` keystore password, or enter a new password if none previously existed.
c. Look at the files in the security folder to verify that the `jssecacerts` keystore exists.

4. Restart the GE PulseNET service and log in as an admin user to retest LDAPS connectivity.

GE PulseNET can now send requests to your secure LDAP server.

**LDAP User Groups**

To manage the roles assigned to LDAP User Groups navigate to Administration > User Management > LDAP User Groups.

1. Select the LDAP Groups to which you will assign roles by clicking the checkbox.
2. Click the **Assign** button.
3. In the **Select Role** window, select the role you will assign to the selected LDAP Groups by clicking the checkbox.
4. Click **Save** 🖊️.
5. To remove a role from a Group, select the LDAP Group by clicking the checkbox. Then, click the **Unassign** button.

**Enabling RADIUS Authentication**

If you use Remote Authentication Dial In User Service (RADIUS) to manage user access to your network, you can enable RADIUS server authentication in GE PulseNET. When the GE PulseNET server is configured to access the RADIUS server, it is able to authenticate GE PulseNET users, which enables you to manage user credentials using RADIUS.
Enable RADIUS Authentication

1. Navigate to Administration > User Management > RADIUS Configuration.
2. In the dialog box that appears, select the Enable check box.
3. In the Server Host Name box, type the hostname or IP address of the RADIUS server.
4. In the Authentication Port box, type the port number.
5. In the Shared Secret box, type the authentication key for the RADIUS server.
6. Select the Authentication Mode — PAP (Password Authentication Protocol) and CHAP (Challenge-Handshake Authentication Protocol) are both supported.
7. To ensure that all values are correct, click the Test button to test the connection to the RADIUS server. To check the credentials, enter the username and password before clicking the Test button. After the test connection is successful, close the dialog box.
8. In the Radio Configuration Wizard window, click the Next > button.

After the RADIUS server connectivity is configured, you now define the default roles for users.
Define User Roles

1. In the second **Radio Configuration Wizard** window, click the **Add** button to create a new user group. See **Managing User Groups** for more information on creating new groups.
2. If you’d rather select a default user group from the list of predefined options, select the “Administrators” or “Operators” group. Once a user logs onto GE PulseNET, they will be assigned this predefined group automatically. For instructions on changing that user group after the user logs in, visit **Managing User Groups > Managing Users**.
3. Click the **Finish** button.

**NOTE:** GE PulseNET only supports RADIUS usernames that have more than four characters.
WORKING WITH RULES

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

**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 when creating a user account. To configure the email service, see the System Configuration section.

**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 exist in their user profile.
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><strong>AP Change for Remote</strong></td>
<td>Monitors remote devices for migration to different access points.</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Bad Access Point Health</strong></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><strong>Bad Remote Health</strong></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><strong>Bad Repeater Health</strong></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><strong>Device Unavailable</strong></td>
<td>Monitors the availability of the device.</td>
<td>Fatal</td>
</tr>
<tr>
<td><strong>DLINK Alert Notification</strong></td>
<td>Monitors whether a DLINK alarm has been received from a narrowband radio.</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>PA Temperature</strong></td>
<td>Generates alerts for DLINK devices when Power Amplifier temperatures reach defined limits.</td>
<td>Warning, Critical, Fatal</td>
</tr>
<tr>
<td><strong>Poor Response Time</strong></td>
<td>Monitors the ICMP round trip time for a device.</td>
<td>Warning, Critical, Fatal</td>
</tr>
<tr>
<td><strong>RSSI Change</strong></td>
<td>Monitors values of RSSI that are outside the two-day moving average.</td>
<td>Warning, Critical, Fatal</td>
</tr>
<tr>
<td><strong>RSSI Level</strong></td>
<td>Monitors the levels of Received Signal for devices.</td>
<td>Warning, Critical, Fatal</td>
</tr>
<tr>
<td><strong>SD Master Station Failover</strong></td>
<td>Monitors whether a radio failover has occurred between redundant radio modules.</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Serial Number Unrecognizable | Generates an alert when the serial number of a DLINK access point is unrecognizable | Fatal
SNR Change | Monitors for values of SNR that are outside the two-day moving average. | Warning, Critical, Fatal
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.

**Bulk Enable/Disable/Delete**

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 rules

1. Navigate to Administration > Rules
2. On the Rules dashboard, find the row for the rule that you want to enable
3. On the row(s) for the desired rule, check the checkbox and then click the Enable button
4. Confirm your selection (Yes/Cancel)

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 and enable email notifications if desired.

To disable rules

On the row(s) for the desired rule, check the checkbox and then click the Disable button. Confirm your selection (Yes/Cancel)

To delete rules

On the row(s) for the desired rule, check the checkbox and then click the Delete button. Confirm your selection (Yes/Cancel)

This feature provides a way for several rules to be enabled/disabled/deleted in bulk.
Quick Update for Rule Settings

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.

Configure thresholds for a rule

1. Navigate to Administration > Rules.
2. Click the Edit icon for the rule you want to modify and select Quick Update.
3. Click the Edit icon for any 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:

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.
Full Update for Rule Settings

The Full Update display provides access to every setting available within a rule definition. You can open the Full Update window by clicking the Edit icon on a specific rule and selecting Full Update from the menu.

You may select the Rule Group to which this rule is assigned by choosing one from the dropdown menu. If you do not see an appropriate Rule Group, you can click the green Add icon to add a new Rule Group to the list. You can also change the rule Name and Description.

In the Device Selector section you can set the group of devices which this rule applies to by choosing either Device Group or Filter and selecting the appropriate entry from the dropdown menu. If you do not see an appropriate device group or filter, you can click the green Add icon to add a new group or filter to the list.

You may choose whether this rule is enabled by checking or unchecking the Enabled checkbox.
The Trigger Type section defines the method for triggering the rule based on the defined thresholds and fire strategies. There are three trigger types: By Data, By Schedules, and At a Fixed Time.

- **By Data:** triggers the rule based on metrics values that are collected by GE PulseNET
- **By Schedules:** triggers the rule on one or more predefined recurring time schedules
- **At a Fixed Time:** triggers the rule once at a specific time of day

The Blackout Schedules section allows you to set any time intervals during which you want the rule to be inactive.

In the Rule Default and Rule Severities table you can add, change, or delete any of the settings for triggering the rule. The settings for Warning, Critical, and Fatal severities can also be copied in order to create new intermediate severity levels for the rule if desired.

- **Rule Default:** The Rule Default is the foundation upon which the other severity levels can be built. It contains the default or baseline set of parameters which are inherited by the other severity levels (unless they are overridden in the severity level definitions). Rule Defaults do not have conditions or thresholds.

- **Fatal/Critical/Warning/Normal:** The severity level entries in the table show only the fields that will be overridden in the default by each severity. Severity level entries are where rule conditions and thresholds are defined.

In the example below, the Rule Default contains the event message and fire strategy, as well as the subject and content for the email alerts. The Fatal, Critical, and Warning severities will inherit all of those defaults, but each of them will trigger the rule on a slightly different condition or threshold value. The Normal severity overrides only the email subject which notifies users that the condition has returned to within normal limits. All other settings can be inherited from the Rule Default.
Editing Rule Defaults

The Event Message section allows you to create the alert message using a combination of text and GE PulseNET macros which will be replaced at runtime with the appropriate value for the device.

In the example below, the message includes #rssi which will be replaced with the actual RSSI value that triggered the alert. In addition, the @name and @modelNumber macros will be replaced with the actual device name and model on which the event occurred. These macros can be inserted into the text by selecting them from the dropdown list and then clicking the gray down arrow button to include them at the current cursor position.

Macro characters include the following:
- $ Variables defined in the rule itself ($MAX_RSSI)
- @ Configuration properties (name, model)
- # Metric values (#rssi, #snr, #voltage)
- % Hardcoded GE PulseNET variables (%severity and %deviceUrl)

The Fire Strategy works the same as described above in the Quick Update section.
In the Notification section you define the email recipient list, the Subject, and Message Content text. These messages can be constructed using the same method as described in the Event Message section.

**Editing Severity Conditions and Thresholds**

The main task for each severity level is to define the appropriate conditions and thresholds for triggering the alert. Conditions can be defined using a robust and powerful set of features that create complex condition filters.

Several types of operators are available: And, Or, Not, Compare. The Compare operator allows you to select devices that have a specific parameter that matches a chosen value. For example, you may compare to determine whether the IP address of a device starts with “10.0.0”.

Comparisons can include the following operators:

- **Equals**: The search string in the third field must exactly match the value of the chosen parameter. For example, if a device's IP address EQUALS “10.0.0.54” it will be listed.
- **Not Equals**: The comparison will return a match if the parameter’s value contains anything except the literal search string. For example, any device with a “Firmware Version” NOT EQUAL to “3.1.0” will be listed.
● **Contains:** The comparison will return a match if the search string is contained anywhere within the parameter’s value. For example, if the device’s model CONTAINS “MDS” then radios with any of the following models will be listed: GE MDS Orbit, MDS Orbit, GE Orbit by MDS.

● **Starts With:** The comparison will return a match if the parameter’s value begins with the literal search string. For example, if the device’s serial number STARTS WITH “250” then any radio with a serial number beginning with that sequence will be matched.

● **Ends With:** The comparison will return a match if the parameter’s value ends with the literal search string. For example, if the device’s serial number ENDS WITH “394” then any radio with a serial number ending with that sequence will be matched.

● **Matches:** Allows the use of regular expression wildcards to form the search string. For example, a search string of ^Orbit.* would match anything that starts with Orbit followed by zero or more characters. The search string of Orbit[0-9] would match the word Orbit immediately followed by any one of the digits within the brackets. See the **GE PulseNET User Guide Appendix** for a list of wildcards that are supported.

● **Is In:** The comparison will return a match if the parameter’s value matches any of the items in a comma separated list of values. For example, any device will be listed whose model is one of the following: “Orbit,MDS Orbit,Orbit-123,MyOrbit”.

The **AND** operator allows you to include devices which have all of the specific parameters and matching values that are included in the filter. For example, you may select devices whose IP address Starts With “10.10.” AND whose “Firmware Version” Equals “3.0.3”

The **OR** operator allows you to include devices which have any of the specific parameters and matching values that are included in the filter. For example, you may select devices whose IP address Starts With “10.10.” OR whose IP address Starts With “10.11.”

The **NOT** operator allows you to exclude devices which have the specific parameters and matching values in the filter. For example, you may select devices whose IP address does NOT Start With “10.20.”

Once you choose an operation (And/Or/Not/Compare) you need to specify a property that exists on the type of devices you selected in your **Device Selector**. If you want to see which properties are supported on your devices, click the green **Run** icon in the Device Selector section, which will display the list of devices that match your device filter or group. On that list, click any of the **Blue Information** icons to see a detailed list of device properties. As you define your severity condition you may choose any of the listed properties for your filter criteria.

When you are editing the rule severity conditions and thresholds you may also choose to edit some of the other values inherited from the Rule Default (if desired).
Action Icons for Rules

For each rule in the Rules Table there is a set of Action icons that allow you to re-prioritize, copy, edit, delete, and enable/disable rules one at a time.

Reprioritize Rule Evaluation Order

GE PulseNET rules are evaluated in the order in which they are listed within each Rule Group. Typically the default rule order is adequate. However, especially when custom rules exist within Rule Groups, there may be a reason to change the evaluation order for specific rules. To accomplish this, click the orange arrow icon in the Actions area and a Rule Group display will appear. You can use the orange up/down arrow icons to adjust the order of rule evaluation. Click Save to save your changes.

Copy Rule Definitions

Existing rules can be copied and modified, which provides a shortcut for creating new rules that have similar features. To copy an existing rule, click the Copy icon on the row which lists the rule you want to duplicate. Once the rule is copied, remember to give the new rule a unique name. Change any settings that need to be modified, and click Save to save the new rule.

Edit Rule Definitions

To edit rule definitions, click the Edit icon on the row for the rule you want to modify. You may do a Quick Edit or a Full Update, as described in the previous sections. Click Save to save any changes you have made to the rule.

Delete a Rule

To delete an individual rule, click the Delete icon on the row for the rule you want to delete. Confirm that you want to delete the rule by clicking Yes, or click Cancel to cancel this action.
Enable/Disable a Rule

To enable or disable an individual rule, check or uncheck the checkbox on the row for the rule you want to enable/disable. Confirm that you want to enable/disable the rule by clicking Yes, or click Cancel to cancel this action.

Show Device Selector List

To view the list of devices on which an individual rule will operate, click the green Run icon at the right side of the row containing the rule of interest. A popup window will appear containing the full list of existing devices to which the rule applies. To remove the popup, click the gray X in the upper right corner of the window.
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. Since it may be possible for a set of devices to be members of more than one collection schedule, you can adjust the order of evaluation for the schedule by clicking the up/down arrows to set the priority. The first matching schedule will be used.

Configure a Data Collection Schedule

1. Navigate to Administration > Collection Schedules.
2. On the Collection Schedules table, each row shows the current schedule for each type of device. To edit the collection schedule for any row, click the Edit icon.
3. You may also click the Add button to create a new collection schedule.
On the **Add** or **Update Collection Schedule** display, you may enter or change the values for each of the three types of data collection done by GE PulseNET (Configuration schedule, Performance interval, and Availability interval).

1. Enter or update the unique **Name** for the collection schedule, and provide a detailed **Description**.
2. Enter or update the **Device Selector**, which specifies which devices will be included on this schedule. You may choose to use an existing device filter or device group by selecting either from the first dropdown menu. Then choose the name of the device filter or group from the second dropdown menu. To see which devices will be included in the report, click the green **Run** icon. If you do not see an existing device filter or group which meets your needs, you can click the green **Add** icon to add a new device filter or group.
3. 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. Check the week days or days of the month that you want GE PulseNET to use for configuration collection.
4. 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.
5. You can also update the description text for this configuration collection, if desired.
6. Enter a new value (minutes) in the field.
7. Click Save 🖋️ to apply your settings to the collection schedule
MONITORING CONFIGURATION

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

Defining SNMP Properties

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.

---

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*. 
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.

Delete an SNMP Community String

- Click the Edit 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

Add SNMP v3 Credentials

1. Navigate to Administration > Monitoring Configuration > SNMP Configuration.
2. 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).
3. Type the username that will be used for authentication.
4. Select Read Permission, Write Permission, or both.
5. 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.
6. To change the permissions on an existing credential, click the value in the Permission column. In the dialog box, select the permission.
7. Select a Security Level:
   a. No authentication and no privacy — the identity of the sender is not verified
   b. Authentication and no privacy — the identity of the sender is verified, but the information is not encrypted
   c. Authentication and privacy — the identity of the sender is verified and the information is encrypted
8. If the **Security Level** that you selected requires authentication, specify the authentication protocol and passphrase (i.e., the password for the specified user name).

9. If the **Security Level** that you selected requires privacy, specify a privacy protocol and passphrase. The passphrase is the encryption key.

10. Click **Save** 🟪.

**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** 🟪.

**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.

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 NETCONF Settings

The NETCONF Protocol is used when GE PulseNET communicates with GE MDS Orbit-based devices. It is considered a next generation secure management protocol which may eventually supplant SNMPv3.

Configure NETCONF Settings

Navigate to Administration > Monitoring Configuration > NETCONF Configuration.

Enter or modify any settings as desired and then click Save to save the new settings.

- **Timeout** sets the amount of time GE PulseNET will wait for a NETCONF response before marking the device as unreachable.
- **Retries** sets the number of times GE PulseNET is allowed to retry a NETCONF request after a timeout is received.
- **Retry Interval** is the length of time that must pass before a retry can be issued.
- **Threads** sets the number of simultaneous parallel NETCONF queries that GE PulseNET can generate.
- **Port** is the default NETCONF communication port which GE PulseNET will connect with on the remote devices.
- **User Name/Password** sets the default credentials that NETCONF will use when authenticating to a remote device.

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.
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 a passive DLINK request.
- **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.
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 predefined 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 MissedPolls** — 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.
**MANAGING DEVICE FILTERS**

The Filters dashboard allows you to manage device filter definitions, which form the basis for Device Groups in GE PulseNET. To manage device filter settings, navigate to **Administration > Filters**. From the Filters table you can view, copy, edit, or delete filters, as well as adding new filter definitions.

**View Device List for a Filter**

Click the green **Run 🏆** icon in the **Actions** section of the row for the filter you are interested in examining. A popup list will show the devices captured by this filter, and you can click the **Blue Information 📝** icon on any of the devices to view a detailed list of device properties that are available for filtering. Click the gray **X** to close the popup window.

**Copy an Existing Filter**

Click the **Copy** icon in the Actions section of the row for the filter you want to copy. For more information on working with filter definitions, see the **Adding Device Filters** section below.

**View a Filter Definition**

Either hover over or click the **Blue Information 📝** icon to the right of the filter **Name** on the row for the filter you are interested in examining.

**Edit a Custom Filter Definition**

If you have added a custom filter definition, you may edit its settings by clicking the **Edit 📝** icon on the row for the filter you want to edit. Note that predefined filters delivered with GE PulseNET cannot be edited.

**Delete a Custom Filter Definition**

If you have added a custom filter definition, you may delete it by clicking the **Delete ⚠️** icon on the row for the filter you want to remove. Note that predefined filters delivered with GE PulseNET cannot be deleted.
Adding Device Filters

Click the Add button to add a new device filter. Enter a unique device filter name and a description of the devices that will be included by the filter. Next, define the device filter by adding one or more filter conditions. This feature provides a robust and powerful set of operators that can be used to create complex search parameters. Search parameters may be defined using several types of operators: And, Or, Not, Compare.

The Compare operator allows you to select devices that have a specific parameter that matches a chosen value. For example, you may compare to determine whether the IP address of a device starts with “10.0.0”.

Comparison operators include the following:

- **Equals**: The search string in the third field must exactly match the value of the chosen parameter. For example, if a device’s IP address EQUALS “10.0.0.54” it will be listed.
- **Not Equals**: The comparison will return a match if the parameter’s value contains anything except the literal search string. For example, any device with a “Firmware Version” NOT EQUAL to “3.1.0” will be listed.
- **Contains**: The comparison will return a match if the search string is contained anywhere within the parameter’s value. For example, if the device’s model CONTAINS “MDS” then radios with any of the following models will be listed: GE MDS Orbit, MDS Orbit, GE Orbit by MDS.
- **Starts With**: The comparison will return a match if the parameter’s value begins with the literal search string. For example, if the device’s serial number STARTS WITH “250” then any radio with a serial number beginning with that sequence will be matched.
- **Ends With**: The comparison will return a match if the parameter’s value ends with the literal search string. For example, if the device’s serial number ENDS WITH “394” then any radio with a serial number ending with that sequence will be matched.
- **Matches**: Allows the use of regular expression wildcards to form the search string. For example, a search string of ^Orbit.* would match anything that starts with Orbit followed by zero or more characters. The search string of Orbit[0-9] would match the word Orbit immediately followed by any one of the digits within the brackets. See the Appendix for examples of wildcards that are supported.
- **Is In**: The comparison will return a match if the parameter’s value matches any of the items in a comma separated list of values. For example, any device will be listed whose model is one of the following: “Orbit,MDS Orbit,Orbit-123,MyOrbit”.

See the Appendix for examples of wildcards that are supported.
The **AND** operator allows you to include devices which have all of the specific parameters and matching values that are included in the filter. For example, you may select devices whose IP address Starts With “10.10.” AND whose “Firmware Version” Equals “3.0.3”.

The **OR** operator allows you to include devices which have any of the specific parameters and matching values that are included in the filter. For example, you may select devices whose IP address Starts With “10.10.” OR whose IP address Starts With “10.11.”

![Filter example](image)

The **NOT** operator allows you to exclude devices which have the specific parameters and matching values in the filter. For example, you may select devices whose IP address does NOT Start With “10.20.”

At any time as you are defining your filter you may click the **Run Query** button to see the list of devices that match your settings. When you are satisfied that your filter definition is correct, click **Run Query** to view the list of devices that match your filter. In the device table at the bottom of the display, you can refine your device list even further by deselecting any matching devices that you do not want to include. This gives you complete control of the final device list that will become part of this filter.
You may save your final filter in two different ways. If you want your filter to contain all the devices that matched your search criteria, you can click **Create From Query**. If you want your filter to contain only the devices you selected from the device list at the bottom of the display, you can click **Create From Selected Devices**. Either of these options will result in a new filter that is displayed in your **Manage Filters** table.
MANAGING DEVICE BACKUP

GE MDS strongly recommends you create configuration backup files for devices managed by the GE PulseNET software. In the event of a device failure, the backup files can be used to recover configuration settings. At this time, GE PulseNET only supports device configuration backups for GE Reason S20 devices.

The Device Backup dashboard only appears when you have valid GE Reason S20 device licences in your network. This dashboard allows you to initiate and automate regular configuration backups of supported GE Reason S20 devices.

To manage device backup settings, navigate to Administration > Device Backup. From the Device Backup table, you can view, copy, edit, or delete device backups, as well as schedule new backup configurations.

If an error occurs during a scheduled device configuration backup, you will be sent an alert. To manage your alerts, see the Working with Rules section.
Add a Device Configuration Backup

To schedule a new backup, click the Add button above the Device Configuration Backup table.

1. In the Device Backup dialog box that appears, enter a unique Device Backup name and description that will be included in the new configuration.
2. Click the Enable checkbox to run the configuration.
3. The Device Config drop-down menu allows you to select the template for the device configuration backup to send to a remote FTP server.
4. Next, select a device or device group from the drop-down menu. Click the green Run icon to view a list of the devices that will be included in the device group.
5. Select the frequency of the Device Backup configuration from the Schedule drop-down menu.
6. In the File Server drop-down menu, select where the device should send its backup configuration.
7. In the Folder field, type the name of the folder where you would like to save your backup configurations.
8. In the Device Credential drop-down menu, select the SNMP Credential for the device or click the Add button to create a new one. See the Change Management section for more details on creating SNMP Credentials.
9. Click Save to create the new Device Configuration Backup.

NOTE: The FTP site where your Device Configuration Backups are stored may need to be manually cleaned up from time to time.
MANAGING DEVICE GROUPS

The Device Groups dashboard allows you to manage device group definitions, which are built using GE PulseNET filters. To manage device group settings, navigate to Administration > Device Groups. From the Device Groups table you can view, edit, or delete existing device groups, as well as adding new device groups.

GE PulseNET device groups consist not only of associated devices, but also of associated users and time windows during which changes to the group’s devices will be allowed. Each of these components are described in the Adding Device Groups section below.

View Device List for a Group

Click the green Run icon in the Actions section of the row for the group you are interested in examining. A popup list will show the devices included in this group, and you can click the Blue Information icon on any of the devices to view a detailed list of device properties that are available. Click the gray X to close the popup window.

Edit Device Group Definition

Click the Edit icon on the row for the group you want to edit. See Adding Device Groups for an explanation of the components that can be edited in a device group.

Delete Device Group

Click the Delete icon on the row for the group you want to remove. Click Yes to confirm the deletion, or Cancel to cancel this action.
Adding Device Groups

Click the Add button to add a new device group. Enter a unique device group name and a description of the devices that will be included in the group.

Next, select a device filter to be used to define the devices which are members of this group. If there is no appropriate filter in the dropdown list, click the green Add icon to add a new filter. See the Managing Device Filters section for more information. Once a filter is selected, you may click the green Run icon to view a list of the devices that will be included in this device group.

Next you must select the Change Window, which is the period of time during which changes will be allowed on this group of devices. You may use the global default change window, or you may define a custom time range. Finally, select the GE PulseNET users who are the owners or approvers for any change requests on this group of devices. Click Save to save your new device group.
CHANGE MANAGEMENT

GE PulseNET includes a special feature for INet, Mercury, Orbit, SD and Reason S20 Series devices which automates specified configuration changes on individual devices or on bulk groups of devices that you choose. The bulk change feature is useful in an environment where there are dozens, hundreds, or even thousands of remote radios which must be configured with specific settings.

GE PulseNET allows you to specify the exact change to be made, the specific set of devices on which the change must be made, the time window during which the change will be allowed, and escalation for change approval to the users who are device owners.

GE PulseNET uses the SNMP or NETCONF protocol to communicate securely with the remote radios.

Configuring Change Management

After navigating to Administration > Change Management, the first task is to configure Change Management defaults. Select Change Management Configuration and verify that all required fields (marked with a red asterisk) have been entered.
The following settings are global default values, but they can be overridden within the definition of each individual change request if desired.

- **Retries**: the number of times that GE PulseNET will retry a change if the first attempt is unsuccessful
- **Retry Interval**: the amount of time GE PulseNET will wait between retry attempts
- **Concurrent Sessions**: Change requests are multi-threaded so that several individual changes may be running simultaneously. This value sets the number of radio changes that GE PulseNET is allowed to attempt concurrently.
- **Radio Uses HTTPS**: check this checkbox to force GE PulseNET to use HTTPS protocol when displaying a radio’s web interface
- **Radio UI Port**: the port which GE PulseNET should use when attempting to connect to a radio’s web interface
- **Compliance**: check the Enable checkbox to force GE PulseNET to keep devices that are new to the system or devices that have been reset automatically updated with those change requests. **NOTE**: Only available for GE MDS Orbit devices.
- **Default Change Window**: All Day allows GE PulseNET to attempt radio changes at any time, but a specific time window can also be defined during which changes are allowed
• **Concurrent Reprogramming Sessions**: the number of radio firmware update requests that GE PulseNET is allowed to attempt simultaneously

• **Reprogram Timeout**: the amount of time GE PulseNET waits before marking a reprogramming request to have failed

• **Default Approver**: Change request approvers can be identified by one or more specific user IDs, by User Role, or by User Group. The users selected here will be the default change request approvers, but they can be overridden within the definition of each individual change request if desired.

Click **Save** to save these parameters.

### Managing Firmware Servers

The GE PulseNET **Firmware Management** feature allows for devices to be updated with new firmware images, as well as restarted using a specific firmware image. By doing this via Configuration Management, firmware upgrades and restarts can be scheduled to happen at a particular time for a set of devices. This would typically be scheduled to occur during a maintenance window and the status can be viewed when the operation is complete. If there are failures towards particular devices, the operation can be rescheduled for those devices during the next maintenance window.

**Manage Firmware Servers**

The firmware images must be manually transferred to the SFTP or TFTP server. Define a Firmware Server which supports SFTP or TFTP and contains the firmware images.

Navigate to **Administration > Change Management > Firmware Servers**.
The **Action** columns show the actions that can be taken on a firmware server entry, including showing the available firmware images on a server, editing firmware server connection settings, and deleting a firmware server from the list.

Click the **Add** button to add a new firmware server.

Enter a unique name to identify the firmware server, as well as a description of the services provided. This is a good place to describe the server’s location or the reason why some devices may need to retrieve their firmware images from this file repository.

Enter valid values for each of the following fields:

- **Protocol**: Currently the only supported file transfer protocols are Secure File Transfer Protocol (SFTP) and Trivial File Transfer Protocol (TFTP).
- **IP Address**: The IP address used to connect to this file transfer server.
- **Port**: The port on which this server is listening for connection requests.
- **Firmware Image File Folder**: The full path within this service to where firmware image files are stored. This folder is usually configured during SFTP/TFTP server installation.
- **Timeout**: The length of time in milliseconds that a device should wait for responses from the SFTP/TFTP server before aborting the firmware file transfer.
- **User**: The username that is required for authenticating with the SFTP/TFTP server.
- **Password**: The password for the above user. Enter this password in both fields for confirmation.

Once the Firmware Server connection settings have been entered, you may test the connection by clicking the **Test Connection** button. You should see a new dialog box that contains the list of firmware images (SFTP only) in the designated folder on this specific file server. If unsuccessful, an error message will indicate why the connection failed.
Managing Change Templates

To manage Change Templates navigate to Administration > Change Management > Change Templates.

Change Templates define actions which can be taken on groups of devices. Individual Change Requests will be defined using Change Templates which are configured here.

The Actions column shows the actions that can be taken on a change template, including the ability to edit the description and to delete the change template. The Name column includes a Blue Information icon that allows you to display a brief summary of any change requests which are using the change template. The Type column shows the type of change that will be performed (Configuration, Password, or Firmware). The Model column lists the type of device that will be targeted by the change. Configuration change templates require you to record changes that will be made based on a standard device configuration, so the Recording Device IP Address and Firmware Version will list the device that was used as the basis for the recording.

Add a Configuration Change Template

To create a new configuration change template, click the Add Change Template button and select Add Configuration Change from the dropdown list.

In the Add Configuration Change Template dialog box that appears, navigate to the Device Type drop-down menu and select the type of device to include in the template. For iNet, Mercury, SD and Reason S20 devices, proceed to the instructions in the next paragraph. For Obit devices, continue with the instructions in the following paragraphs.
For INet, Mercury, SD, and Reason S20 devices, enter a unique template Name and Description of the changes that will be included in the template. It is usually best practice to include the reason for this change in the description field. Next select the device properties to set from the dropdown menu. For more detailed information about the device properties, refer to your device’s user manual. Click the green Add icon to add additional properties. Click the Save button.

For Orbit devices, enter a unique template Name and Description of the changes that will be included in the template. It is usually best practice to include the reason for this change in the description field. Next you must select a device that will be used for recording the changes to be made on similar device models. Any device can be selected, but you will probably want to choose a device with a known good configuration to use as the basis for changes to be made on other devices in the network.
Click the **Device Selector** icon to view the device selector display for choosing your recording device.

When you click the **Initialize Template** button, GE PulseNET opens a communication channel to the recording device and makes a snapshot of that device’s configuration settings. You will then see that the first gray arrow has become green, indicating that you can proceed to the next button in the row.

When you click **Start Recording**, it opens the web interface and allows you to establish an interactive login session to the recording device. During your interactive session with the recording device, you make any desired changes to the configuration and then you must commit or save those changes on the device itself. You will then see that the second gray arrow in GE PulseNET has become green, indicating that you can proceed to the final step.

Return to GE PulseNET’s template configuration display to click the **Save Template** button. During this step GE PulseNET compares the initially recorded snapshot with the current state of the device after the desired changes were saved on the device. In the **Configuration Changes** window there will be a list of the required changes that you want included in the template.
At this point you must click the **Save** button at the bottom of the screen in order to save the completed template.

**Add a Password Change Template**

After choosing to add a password change template, enter a unique template name and a description of the changes that will be included in the template. Next, enter the new passwords for one or more local device accounts. This is accomplished by clicking the **Edit** icon at the right, which will open the password editor where you can enter and confirm the new password for any account as desired. Once entered, the New Value column will show asterisks in the password field. You may also choose to delete the newly entered password by clicking the red **Delete Action** icon. Click **Save** to save your completed template that contains the new passwords.

**Add a Firmware Change Template**

A firmware push is supported for iNET, Mercury, Orbit, and DLINK SDMS remote devices. After choosing to add a firmware change template, enter a unique template name and a description of the changes that will be included in the template. Next, select a **Firmware Server** from which the device will retrieve its image. If an appropriate firmware server is not shown in the dropdown list, you may click the green **Add** icon to add another firmware server. See the **Manage Firmware Servers** section for more information.
Once the firmware server is selected, you may click the Blue Information icon to see the connection settings for that server. Next, select or input the exact name of a Firmware File that you want devices to upload. The dropdown list of firmware files only contains images that are currently available on a selected SFTP server. Click Save to save your completed firmware change template.

### Add a Certificate Import Change Template

An authenticity certificate and its fingerprint are used for verifying firmware updates to a device. GE PulseNET supports firmware certificates for Obit devices. After choosing to add a Certificate Import Change Template, select the device type and create a unique certificate name and identity. Next, select a Firmware Server from which the device will retrieve the certificate. If an appropriate firmware server is not shown in the dropdown list, you may click the green Add icon to add another firmware server. See the Manage Firmware Servers section for more information.

Once the firmware server is selected, you may click the Blue Information icon to see the connection settings for that server. Next, select or input the exact name of the Firmware Certificate you want devices to upload. Click Save to save your completed Certificate Import Change Template.
Managing Change Requests

From the Change Management dashboard, select Change Requests. The Change Requests view allows you to create change requests as well as checking the status of existing requests.

Several kinds of network changes are incorporated into GE PulseNET’s Change Management feature, including configuration changes, changing the password on device user accounts, upgrading device firmware, and rebooting devices in the field. Select the type of Change Request from the dropdown list.

Adding a Configuration Change Request

It is very important to give meaningful descriptive Names to all change requests. A separate Description field is provided so that details for this change can be captured. Do not overlook the importance of using these two fields to clearly identify exactly what is being changed and the reason for these changes on the selected devices.
After entering the change request name and description, complete the following fields:

- Select a **Device Group** to which the changes will be applied. If you have device groups already defined, you can select the appropriate group from the dropdown menu. If you do not have a predefined device group for this change request, you can click the green **Add** icon to add a new device group. Once the device group is selected, the change request form will show the number of devices in that group. You may then narrow your selection even more by clicking the device icon to the right of the device count. Deselect any devices in the group that should not receive this change.

- **Start and Stop** times, which set the boundaries for the time window within which this change is allowed to take place. A default Change Window is configured within each device group and will be populated after a device group has been selected. However, you can adjust the change window as needed for this specific change request.

- Clicking the **Calendar** icon allows you to set the start or end time by selecting the day and time on the calendar widget. Clicking in the **Timestamp** field allows you to directly edit and change the day and time text string. Clicking the **Now** button will automatically set the start time to the current system time.
● A change request that is created by the owner of a device group will be submitted without the need for approval. That change request will start running as soon as the start time has been reached, or immediately if the Now option was selected. If the change request was created by someone who is not the owner or approver for the group of devices, then the request will be submitted as **Awaiting Approval**.

● If a change request does not complete successfully within the original time period, then it can be re-executed. The device group owner can schedule the change request to re-run at any time. However, the device group owner can also specify a time period during which a non-group-owner (for example, an operator) can re-execute a change request. If the non-owner re-runs the failed request within this time period, then the change request does not need to be reapproved.

● If applicable, click the **Force Compliance** checkbox to force this change request to be enabled for all Orbit devices.

● Select the **Configuration Change Template** to use for this change request. If you have an appropriate configuration change template already defined, you can select it from the dropdown menu. If you do not have a predefined configuration change template for this change request, you can click the green **Add** icon to add a new configuration change template. See the **Managing Change Templates** section for additional details.

● Once the **Configuration Change Template** is selected, you will see the description and change details for the device configuration items that will be changed as part of this change request.

● Click the **Save** button to submit the new Change Request.

### Adding a Password Change Request

After entering the change request name and description, complete the following fields:

- Select a **Device Group** to which this Password Change Request will apply.
- Select the **Start** and **Stop** times during which this change will be allowed. Set the Change Window if required.
Choose a **Password Change Template** from the dropdown list. If you do not have a predefined template for this change request, you can click the green **Add** icon to add a new password change template. Once the correct template is selected, you will see the description and details that will be changed as part of this request.

- Click the **Save** button to submit the new Change Request.

### Adding a Firmware Change Request

A firmware change request is supported for the following devices: iNET, Orbit, Mercury, and SDMS Remote Reprogramming. After entering the change request Name and Description, complete the following fields:

- Select a **Device Group** to which this Firmware Change Request will apply.
- Select the **Start** and **Stop** times during which this change will be allowed. Set the Change Window, if required.
- Choose a **Firmware Change Template** from the dropdown list. If you do not have a predefined template for this change request, you can click the green **Add** icon to add a new password change template.
- Once the correct template is selected, you will see the description and details that will be changed as part of this request.
- Click the **Save** button to submit the new Change Request.
- Once the Firmware Change is running the progress will be tracked for each device.
Adding a Restart Device Change Request

A restart device change request is supported for the following: iNET, Orbit, and Mercury devices. Select the type of restart request from the Change Request dropdown list (Active, Inactive, Latest, specific Version). After entering the change request Name and Description, complete the following fields:

- Select a **Device Group** to which this Restart Change Request will apply.
- Select the **Start** and **Stop** times during which this change will be allowed. Set the Change Window if required.
- Choose a **Restart Device Template** from the dropdown list. The available templates will be limited to those available for the type of **Restart Request** you selected on the **Change Request** menu.

- **Restart to Active** will have the remote radios reboot to their currently active firmware image
- **Restart to Inactive** will have the remote radios reboot to their currently inactive firmware image
- **Restart to Version** will allow you to specify the firmware version number on which to reboot the remote radios, no matter whether it is currently active or inactive.
- **Restart to Latest** will have the remote radios reboot to the highest firmware version that is available on the device
● Once the correct Restart Device Template is selected, you will see the description and details that will be sent to the remote radios as part of this request.

● Click the Save 💾 button to submit the new Change Request

### Managing Change Requests

Once a Change Request has been saved, its status will be displayed in the Change Requests Table. Valid change request options include Awaiting Approval, Queued to Run, Running, Awaiting Review, Completed, or Ran within the last day/week/month.

In addition to the Add Change Request button discussed above, change requests can be Approved, Marked as Complete, Deleted, or Canceled. A change request that has run and been marked as complete is eligible for deletion from GE PulseNET. A change request that has a status of Queued or Running is eligible to be Canceled.

One or more rows in the Change Request table can be selected using the checkboxes on the left. Clicking the textual name of the Change Request or clicking the Blue Information 🔄 icon will display a brief summary of the change request.
If an Edit icon appears in the column next to the Blue Information icon, then you are allowed to edit several of the Change Request fields. Editable fields include the Description and the Change Window for non-owners of the device group.

In the Number of Runs column, each number is a clickable link. Clicking the number itself will bring up the Change Request History display as shown below.

The Last Runtime columns show any previous times when the change request was run. The Next Runtime columns show any future times when the change request will run, and clicking the Clock icon allows you to change the next runtime if it is allowed.

The Number of Devices columns show the total number of devices that the change request will apply to, and if the change request has run it will also show the number of devices which updated successfully compared to those on which the request failed.

Each of the numbers is a clickable link, so clicking any number will display information about the devices in the list. If the change request has run, then the appropriate status will be displayed. Clicking the number for devices which were not updated will display any error messages that indicate why the change was unsuccessful (as shown in the following image).

If a green Add icon appears after a number, then you are allowed to add a new change request which will only apply to the devices in the column you selected. For example, clicking the green Add icon in the Not Updated section will allow you to create a new change request that will apply only to the devices on which your first change failed.

If a change request has a status of Awaiting Approval, the set of device owners are notified via email that a change request is awaiting their approval. When one of the device owners navigates to Manage Change Requests he or she will see that the Approve button is active. Edits can be made to the change request before approving the change for execution. If the change window is set to start immediately, note that the change request will immediately begin to run as soon as it is approved.
NOTE: It is possible that not all of the radios selected for a change request will support the same features as other radios in the group. If a change request action is not possible on a particular radio because it does not support the feature being changed, then that radio will be listed as having failed to receive the change. This would be normal and expected, since that specific radio does not support the feature being changed.

Editing SD Devices from the Device Details Page

Make Changes to Individual SD Device

- Navigate to the Summary page and click on the device.
- In the Device Details dialog box that appears, you can change all the fields with the Edit icon located to the right in the field.
- Click the Edit icon to make change.

NOTE: If you need to change more than one value of an SD Device, it is recommended that you use Changement Management to run the request rather than the Device Detail view (see Change Management for more details). If you are running more than one change on a device or a set of devices using a Change Request, be sure to verify that all of the values have been updated.

If you make a config change from the Device Detail view by updating a value, make sure that the configuration poll timestamp updates along with the value before entering another configuration change.
ACCESS CONTROL

The Access Control feature allows administrators to grant unprivileged users the ability to view dashboards which would normally only be accessible to administrators. This provides a way for GE PulseNET administrators to delegate some of their routine tasks to power users that they have identified. These extra privileges can be granted by specific User Name, by User Group, or by User Role.

View Access Control Properties

Navigate to Administration > Access Control.

Delete Access Control Records

- Select the checkbox on one or more rows which are to be deleted
- Click the Delete button and then confirm that you want to delete the selected rows
- Individual rows can also be deleted by clicking the Delete icon in the Actions section
Edit Access Control Records

Click the Edit icon on the row that you want to edit. You may edit any property except the unique Access Control Name.

Add Access Control Records

Click the Add button and enter the information for your new Access Control

Adding an Access Control Record

To add a new record, click the Add button at the top left of the Access Control table.

Enter a unique Name for this Access Control record, and provide a detailed Description. Select the specific dashboard or control that you want the users to be able to access by choosing one from the View Selector dropdown list.

You can construct your Access Control so that the selected dashboard is Allowed or Denied. This gives you the flexibility to add features for users who need them, or you can remove features for users who should not be allowed to access them.
Users can be specified using any combination of the three methods represented under the tabs in the bottom section. On the Users tab you can specify one or more exact User Names by checking the checkbox beside their names. On the **User Roles** tab you may also specify one or more User Roles to which your access control will be applied. Finally, on the User Groups tab you can specify one or more User Groups to which your access control will be applied.

When you have created your access control, click **Save** to save your changes and view the new control in the **Access Control** table. Since each record can only grant access to one view at a time for one set of selected user(s), you may need to create several different Access Control records each dashboard or user group.
DEVICE DISCOVERY

Before GE PulseNET can monitor your network devices it must first discover them and give you the opportunity to authorize them for management. Since Device Discovery is a task that could be delegated to non-Administrator users, the options for discovering devices appear on the Summary dashboard rather than the Administration dashboard. Click the Gear icon at the upper right corner of the Summary dashboard to select the discovery features from the dropdown list.

Discovering SNMP Devices

Discover SNMP Devices

1. Click the Discover SNMP Devices button.
2. 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 for more information.
   - 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).
   - **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.
3. 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.
   ○ To specify an IP address range to be included in the discovery, enter the IP address range and click Save. For example, an IP address range can be created using the dash (10.10.120.1-100) or by using the wildcard (10.10.120.*)

4. Specify any IP addresses to be excluded using the right panel.
5. 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 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.
Discover DLINK Devices

1. 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.

   **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.

   **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.

   **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.

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

3. 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.

4. Click Start to begin the discovery process.

![Discovery process screenshot](image)

Comma separated unit IDs or range for Active discovery (e.g. 1000, 1100-1120)

Based on the information provided, 10 device(s) may be discovered.

Your discovery request is processed and a list of eligible devices will be displayed in the left panel.
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.
Discovering DLINK Redundant Clusters

During the normal DLINK discovery and authorization process GE PulseNET may identify devices that it is already managing in its database. If this occurs, an Authorize DLINK Devices dialog box with a warning will appear. GE PulseNET will give you the option of authorizing the devices as members of a redundant cluster. Click Authorize to continue.

**NOTE:** Only Cold and Warm Redundant Clusters can be created during discovery. See [Working with Redundant Clusters](#) for more details.

In order to create a redundant cluster during discovery in GE PulseNET, follow these steps:

1. Verify that the currently active master device and its downstream remotes have been discovered and authorized in GE PulseNET. You must wait until GE PulseNET completes the initial configuration collection and the Device Model field is filled in.
2. Physically access the redundant equipment and perform a failover to the secondary master.
3. Return to GE PulseNET and perform a re-discovery using the same IP/port numbers as the primary master device.
4. Select the newly discovered secondary device by clicking the checkbox and click the Authorize button.
5. In the Create Redundant Cluster window (pictured to the right), type a name into the Cluster Name field.

6. Click the Save button. Click Cancel to leave devices unclustered. See Working with Redundant Clusters for more information. The data collection settings for both members of the cluster are automatically set to those of the first master you discovered.

**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, information about new remote devices will be listed. Administrators can view and authorize the newly discovered remote devices by clicking Auto-discovery. Eligible devices will be displayed in the left panel, where they can be selected and authorized for monitoring.
Trigger Force Compliance

Click the Gear 🔄 icon at the upper right corner of the Summary dashboard to select Trigger Force Compliance feature from the dropdown list. This feature will force GE PulseNET to look for any Orbit devices on the network that are missing configuration changes and begin applying those changes to the devices immediately. This will only apply to the Orbit devices that are missing changes.
**Authorizing Devices**

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

**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.

**Working with Redundant Clusters**

GE PulseNET has the ability to associate two or more redundant devices into “clusters.” This allows GE PulseNET to know which redundant device is active at any point in time. There are three types of redundant clusters.

1. **Cold Redundant Cluster (cRC):** Two devices that share a single IP address/port and both connect to the same set of remote devices. One of the two redundant devices remains powered off until a failover occurs.
2. **Warm Redundant Cluster (wRC):** Two devices that share a single IP address/port and both connect to the same set of remote devices. Both of the redundant devices remain powered on, but only the active device is communicating with the remote devices.
3. **Hot Redundant Cluster (hRC):** Two master devices, existing cold clusters, or a combination of both that have their own separate IP addresses/ports and remain powered on, but only one is in communication with the downstream devices.
Different GE MDS radio models are capable of supporting different types of redundancy. For more information, contact your GE MDS support team. To create and work with redundant clusters, you must be assigned the Failover Configuration permission. When selecting potential members to place in a redundant cluster, they must have the following prerequisites:

- Cluster devices must not be members of another cluster. If a potential member you want to use is already a member of another cluster, you can edit the old cluster to delete the potential member before you add that device to your new cluster. For information on deleting a member of an existing cluster, see Editing Redundant Clusters.
- If a potential member you want to use is decommissioned, you must re-discover and reauthorize it before adding it to a redundant cluster. For information on discovering devices, see Discovering DLINK Devices.
- In order to be members of a new Hot Redundant Cluster, any existing Cold Redundant Clusters must not already be members of another Hot Redundant Cluster.
- Candidate cluster devices must be the same device model and have the same configuration settings. Once member devices are clustered, the same configuration and maintenance window settings will be applied to all other cluster members.

**NOTE:** Cold and Warm redundant clusters can be created during the device discovery process. See Discovering DLINK Redundant Clusters for more details. The devices in a Hot redundant cluster must be discovered separately and the cluster created after discovery (see instructions below). At the present time Warm clusters can only be formed with x790 radios (also following the steps below).

Creating a New Hot Redundant Cluster

1. Before creating a new redundant cluster, wait until GE PulseNET completes the initial configuration collection for all masters and the Device Model field is filled in.
2. Verify that the master device(s) and downstream remotes have been discovered and authorized in GE PulseNET.
3. Verify that the master devices have their data collection settings configured for Passive Data Collection. Hot redundant SD masters cannot be clustered using Active Data Collection.
4. Drill down to the Device Detail View for one of the master devices in the cluster.
5. Navigate to the Administration menu in the Device Details page and select Create Redundant Cluster.

6. In the Create Redundant Cluster wizard that appears, type the name of the new cluster.

7. Select the Cluster Type.
8. Select the candidate device(s) from the device selector table and click Add to add them to the cluster under the authorized master. A cRC can only have two Cluster Member devices. A hRC can be made up of multiple masters or cRCs.

9. When you have added all the candidates you require, click Save.

The Summary View now shows a single line for the cold cluster instead of the individual masters and hot clusters will show as individual rows for each member.

The Device Detail view now shows the device as a member of the redundant cluster. The hot cluster detail is accessed by selecting the hRC icon in the top right corner of the window of any cluster.
Click on the **Topology View** button to see all of the remotes connected to the redundant cluster.

**Triggering Config Collection for Redundant Cluster**

To trigger config collection for a cold redundant cluster, follow these steps:

1. Navigate to the **Cluster Administration** menu and click on **Trigger Config Collection**.
2. In the Trigger Config Collection window, confirm the configuration collection.
3. Click **OK** or **Cancel**.
Triggering Performance Collection for Redundant Cluster

To trigger performance collection for a cold redundant cluster, follow these steps:

1. Navigate to the Cluster Administration menu and click on Trigger Performance Collection.
2. In the Trigger Performance Collection window, confirm the performance collection.
3. Click OK or Cancel.

Editing Collection Configuration

For more details about Collection Configuration of master devices see Configuring data collection on DLINK master devices. Editing collection configuration through the Cluster Administration menu will apply the modified collection configuration to all master devices in the redundant cluster.

Editing Redundant Clusters

Edit a Redundant Cluster

1. Navigate to the detail view of the redundant cluster.
2. Click the Administration menu icon and select Edit Redundant Cluster from the list.
3. In the wizard that appears, edit the cluster by removing or adding members. A cRC contains only two members. An hRC contains two or more members.
a. To remove members, in the Cluster Members table, click the **Decommission** icon in the device row. This member will be decommissioned and must be re-discovered and re-authorized. Continue until all desired devices are removed. If you decommission devices in a cluster until only one device remains, the cluster itself will be decommissioned.

b. To add new members, in the **Cluster Candidates** table, select a candidate and click **Add**. Continue until all desired devices are added.

4. Click **Save**.

**Moving Redundant Clusters to Staging or Production**

To move a redundant cluster to staging or production, follow these steps:

1. Navigate to the **Cluster Administration** menu and click on **Move to Staging** or **Move to Production**.
2. In the Change Environment window, confirm the move.
3. Click **OK** or **Cancel**.

**Creating Maintenance Windows for RedundantClusters**

To create a maintenance window for redundant clusters and downstream devices, follow these steps:

1. Navigate to the **Device Administration** menu and click on **Enter Maintenance**.
2. In the **Device Maintenance Mode** window, click the checkbox next to Blackout downstream devices.
3. Click the **OK** button. Click the **Cancel** button to cancel.

When you create a maintenance window, all members of the redundant cluster are placed in maintenance mode. You cannot create a maintenance window for an individual member of a cRC. To create a maintenance window for an individual master device in an hRC, navigate to the Device Detail Page of the cluster member, not the Cluster Detail Page.

**Decommissioning Redundant Clusters**

In the Cluster Detail Page, navigate to the **Cluster Administration** menu. Click **Decommission** to decommission the whole cluster. In the **Decommission Devices** window, you will see all the master and downstream devices to be decommissioned. Click **OK** or **Cancel**. To decommission individual master devices, see **Edit Redundant Clusters**.
MANAGING DEVICE SETTINGS

Device Actions

GE PulseNET Administrators and privileged users can manage settings and take several actions by selecting them from the dropdown list under the Gear ⚙ icon on each Device Detail dashboard. These actions include decommissioning the device, configuring collections for a DLINK master, and triggering on-demand performance and configuration collections for the device.

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.

Decommission a Monitored Device

1. On the Device Detail display for any radio, click the Gear ⚙ icon near the top right corner and select Decommission.
2. Check any associated downstream device(s) that you also want to decommission at the same time. To select all downstream devices, click the checkbox in the table header. Be aware that when you decommission a DLINK master, all downstream devices are automatically decommissioned along with it.
3. 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

It is also possible to decommission devices by using the Authorized Device list.

For SNMP devices, navigate to SNMP Discovery and 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 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).

Define Settings for an Individual Master Device

1. On the Detail view for the master, click the Gear 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 Auto-Discovery (see Continuous Passive Auto-Discovery).

4. Choose the Collection Size for configuration data. To minimize the impact of GE PulseNET’s 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.
Triggering Data Collections

**Trigger an On-demand Configuration Collection**

1. On the Device Detail display for any radio, click the Gear icon near the top right corner and select Trigger Config Collection.
2. Confirm that you want to trigger an on-demand configuration collection for this device (Yes/Cancel).

**Trigger an On-demand Performance Collection**

1. On the Device Detail display for any radio, click the Gear icon near the top right corner and select Trigger Performance Collection.
2. Confirm that you want to trigger an on-demand configuration collection for this device (Yes/Cancel).

**Trigger Compliance Checks**

**Trigger a Compliance Check for a Device**

1. On the Device Detail display for any Orbit radio, click the Gear icon near the top right corner and select Trigger Compliance Check.
2. In the Device Compliance window, confirm the missing changes from that device.
3. Confirm that you want to immediately force compliance for the missing changes on that device by clicking on Force Compliance.
GETTING SUPPORT

If problems arise, diagnostic data can be gathered and saved in a group of files called a support bundle. Support bundles can then be forwarded to the GE MDS Technical Support team to aid in identifying and correcting any issues. Each support bundle contains a diagnostic snapshot of the GE PulseNET services 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.

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 to your local machine.

In order to conserve storage space, support bundles are not stored on the GE PulseNET machine.

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.
## APPENDIX

### Traps Format

The following is a list of variable bindings and their payload of the traps sent by GE PulseNET to a remote trap listener:

<table>
<thead>
<tr>
<th>Variable Binding</th>
<th>Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.4.1.4130.9.1.1</td>
<td>MESSAGE</td>
</tr>
<tr>
<td>1.3.6.1.4.1.4130.9.1.4</td>
<td>SERVICE</td>
</tr>
<tr>
<td>1.3.6.1.4.1.4130.9.1.6</td>
<td>RULE</td>
</tr>
<tr>
<td>1.3.6.1.4.1.4130.9.1.7</td>
<td>OBJECT_ID</td>
</tr>
<tr>
<td>1.3.6.1.4.1.4130.9.1.8</td>
<td>OBJECT_NAME</td>
</tr>
<tr>
<td>1.3.6.1.4.1.4130.9.1.9</td>
<td>SEVERITY</td>
</tr>
<tr>
<td>1.3.6.1.4.1.4130.9.1.10</td>
<td>HOST_NAME</td>
</tr>
<tr>
<td>1.3.6.1.4.1.4130.9.1.11</td>
<td>HOST_IP</td>
</tr>
<tr>
<td>1.3.6.1.4.1.4130.9.1.13</td>
<td>URL</td>
</tr>
<tr>
<td>1.3.6.1.4.1.4130.9.1.14</td>
<td>DATE_TIME</td>
</tr>
</tbody>
</table>
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.e2etechinc.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.e2etechinc.com/index.php/about/legal.