GE VERNOVA

MDS PulseNET

Network Management System

GE PulseNET

Enterprise and Standard Administration Guide

Version 6.0

INTRODUCTION

The Administration Guide is intended to assist in configuring and managing GE PulseNET. It 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 is available when logging 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 greater than 500 devices. In this version of GE PulseNET Enterprise, the support for additional vendors' devices is included. Some examples are: 4RF, Cambium, Freewave, Radwin, and Sierra Wireless.

NOTE: Documentation regarding features that apply to PulseNET Enterprise will be marked - **Enterprise Only**.

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 the operators. An administrator has several 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

- 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

- Installation prerequisites, system recommendations, and planning guidelines
- 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 - *Note: this must be run as Administrator*

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 - *Note: this must be run as Root*

Stopping GE PulseNET

Windows

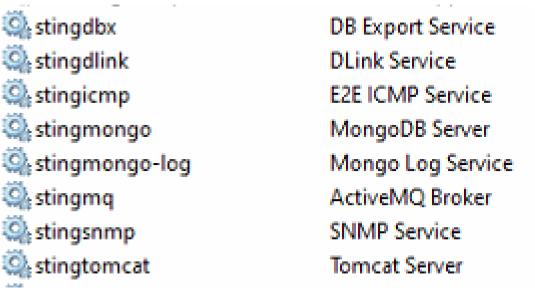
- Navigate to the directory <pulsenet_home> and execute the following command: stop.bat - *Note: this must be run as Administrator*

Linux

- Open a terminal window and navigate to <pulsenet_home> and execute the following command: stop.sh - *Note: this must be run as Root*

Services

Below is an example of some of the services that will be running.



stingdbx	DB Export Service
stingdlink	DLink Service
stingicmp	E2E ICMP Service
stingmongo	MongoDB Server
stingmongo-log	Mongo Log Service
stingmq	ActiveMQ Broker
stingsnmp	SNMP Service
stingtomcat	Tomcat Server

Screen Resolution:

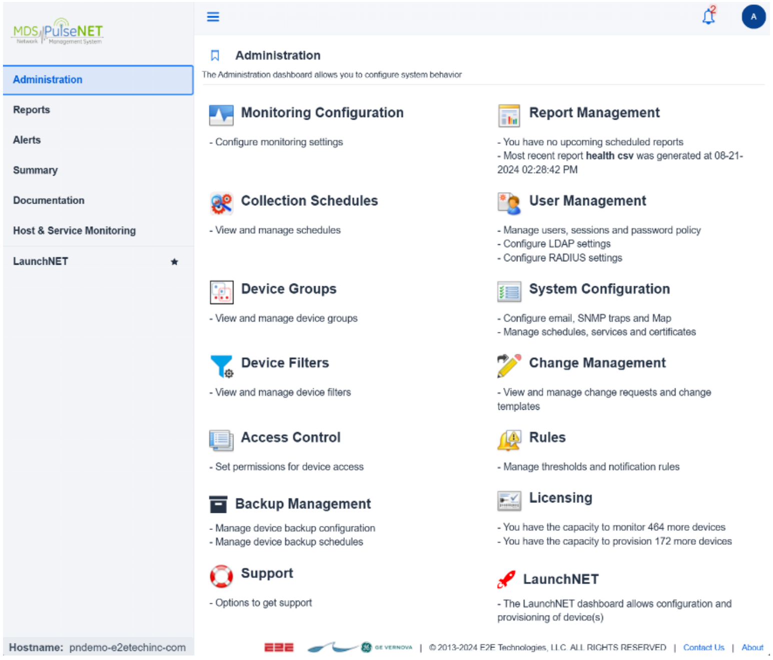
The recommended screen resolution is 1920x1080. The minimum supported resolution for PulseNET is 1024 x 768. Any resolution lower than this will cause the page to not display correctly. If an error message appears while on a higher resolution, please increase the size of the browser.

Local MIB Folder

The mds_software and mdsreg MIB files are included with the PulseNET install, and can be located at: **GE_MDS\PulseNET\mib**

Using the Administration Dashboard

The Administration dashboard is the default home page for a GE PulseNET administrator. It provides links to other dashboards where administrative tasks can be accomplished.



Administration

The Administration dashboard allows you to configure system behavior

Monitoring Configuration

- Configure monitoring settings

Report Management

- You have no upcoming scheduled reports
- Most recent report **health csv** was generated at 08-21-2024 02:28:42 PM

Collection Schedules

- View and manage schedules

User Management

- Manage users, sessions and password policy
- Configure LDAP settings
- Configure RADIUS settings

Device Groups

- View and manage device groups

System Configuration

- Configure email, SNMP traps and Map
- Manage schedules, services and certificates

Device Filters

- View and manage device filters

Change Management

- View and manage change requests and change templates

Access Control

- Set permissions for device access

Rules

- Manage thresholds and notification rules

Backup Management

- Manage device backup configuration
- Manage device backup schedules

Licensing

- You have the capacity to monitor 464 more devices
- You have the capacity to provision 172 more devices

Support

- Options to get support

LaunchNET

- The LaunchNET dashboard allows configuration and provisioning of device(s)

Hostname: pndemo-e2etechinc-com

E2E GE VERNOVA | © 2013-2024 E2E Technologies, LLC ALL RIGHTS RESERVED | Contact Us | About

Note: Above screenshot is from PulseNET Enterprise, adding a license other than

PulseNET Enterprise may change options on the Administration Menu.

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 **[Enterprise only]**
Device Filters — for creating and saving filter definitions **[Enterprise only]**
Access Control — for granting users access to specific views and features **[Enterprise only]**
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, managing map options, and viewing a summary of the GE PulseNET system configuration [Enterprise only]
Change Management — for managing device change requests and settings **[Enterprise only]**
Licensing — for requesting, installing, and managing GE PulseNET licenses
LaunchNET — for managing and staging LaunchNET provisioning templates (if licensed for LaunchNET)
Support — for generating and downloading support bundles and requesting support
Device Backup — for GE Reason and Orbit devices only. Creates snapshots of current device state

WORKING WITH LICENSES

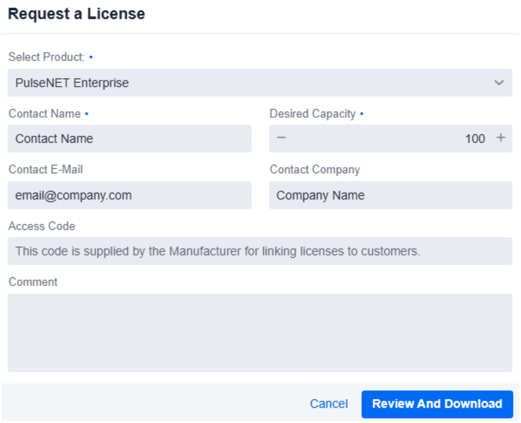
One of the first administrative tasks that should be accomplished is to request and install a valid GE PulseNET license. A license provides GE PulseNET with the capability to authorize and monitor devices. Each device authorized in GE PulseNET will require a unique license. Dependent on the upgrades currently applied to the system, the products available for licensing are as follows:

PulseNET - Standard license for basic monitoring functionality.
PulseNET Enterprise - Enhanced monitoring and configuration features.*
GE Reason - Standalone, or PN addon to monitor GE Reason S20 series.
GE LaunchNET - Addon to unlock GE LaunchNET provisioning features.**

GE LaunchNET Device - Used to license each GE LaunchNET device.
PulseNET Device Monitor - ICMP Ping Only for availability monitoring. (Enterprise license required.)

Request a License

1. Navigate to **Administration** > **Licensing** > **Request a License**. A dialog box will appear.



Request a License

Select Product: •	PulseNET Enterprise
Contact Name •	Contact Name
Desired Capacity •	100
Contact E-Mail	email@company.com
Contact Company	Company Name
Access Code	This code is supplied by the Manufacturer for linking licenses to customers.
Comment	

2. Select a product from the **Select Product** dropdown list.
3. In the **Contact Name** field, type the name of the person at the company who will be the primary contact.
4. In the **Access Code** field, type the access code which can be obtained from the GE Sales team if applicable.
5. In the **Desired Capacity** field, type the total number of licenses required. For example, if 100 access points and 300 remote devices will be monitored, enter 400.
6. In the **Comment** field, enter any comments which would help the Licensing team fulfill the license request.
7. Click **Save Request to a File** to create a licenseRequest.txt file. This must be sent directly to the GE Licensing Team at: gemds.pulsenet@ge.com

When the request is approved, the new license will be sent via email by GE.

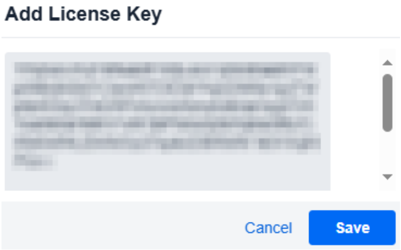
*When a PulseNET Enterprise License is applied the system cannot be reverted to PulseNET Standard. It will require a re-installation of the PulseNET application to revert to Standard.
**See external LaunchNET documentation.

Adding Licenses

After receiving the new licenses, they must be added to the PulseNET instance.

1. From **Administration > Licensing**, click Add License Key and directly paste the

received license key into the provided field and click Save.

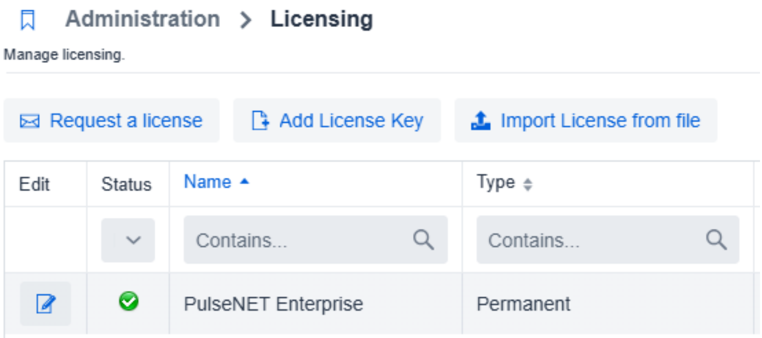


2. Or click **Import License from File** to locate the license file on the computer (the .txt file must be on the machine where the browser is running.) Then click Import.

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

Managing Licenses

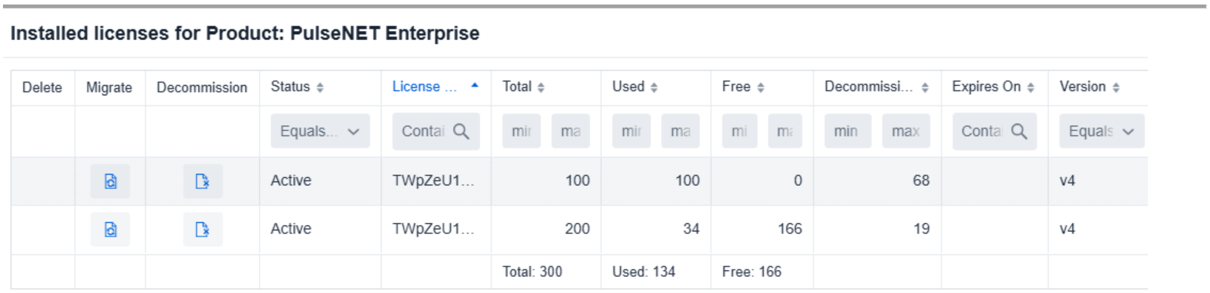
Installed licenses appear under **Administration > Licensing**. This menu allows deletion of expired licenses, migrating devices to new licenses, or requesting replacement licenses.



Edit	Status	Name ▲	Type ⬍
		Contains...	Contains...
✎	✓	PulseNET Enterprise	Permanent

Click the Edit icon on any license row to view the details for a specific license. Here the Hardware ID that identifies the server to GE PulseNET is displayed. Click the checkbox on a row to select it. Selected rows may be deleted from the system. Click on the **License Key** field to view the GE PulseNET license key associated with this license.

The **Used** column provides the option to migrate devices that have been associated with this license. Click the **Migrate** link to view the list of devices and select them for migration. Once selected, choose another GE PulseNET license to which the selected devices should be migrated.



Installed licenses for Product: PulseNET Enterprise

Delete	Migrate	Decommission	Status	License ...	Total	Used	Free	Decommissi...	Expires On	Version
			Equals...	Contai	min max	min max	min max	min max	Conta	Equals
	🗎	🗎	Active	TWpZeU1...	100	100	0	68		v4
	🗎	🗎	Active	TWpZeU1...	200	34	166	19		v4
					Total: 300	Used: 134	Free: 166			

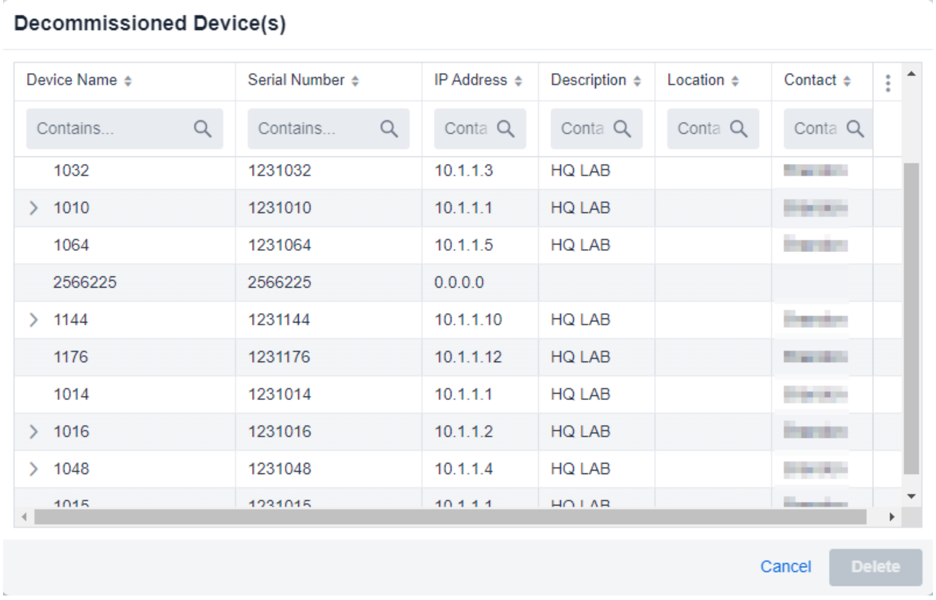
Requesting Replacement Licenses

If an eligible GE device is removed from service and replaced with a new device, a request must be sent to GE for a replacement PulseNET license for the new device. Existing licenses are bound to the serial numbers of GE devices.

Permanently Deleting Authorized Device

The *Decommissioned* column shows devices that are decommissioned and still linked to a license. A licensed device can be deleted *PERMANENTLY* from PulseNET and the license count is added back to the free license(s). ***This is a permanent action and that device serial # will never be authorized within PulseNET again.***

To permanently remove a decommissioned device, go to the decommissioned devices column under the license and click on the number. Find the serial number or IP of the device to permanently delete and click on the row. Then click on the delete button.



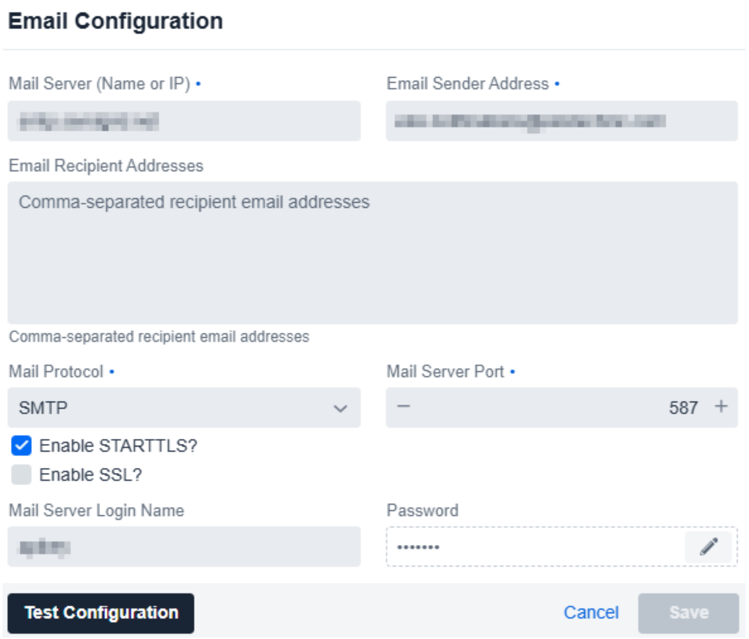
Decommissioned Device(s)

Device Name	Serial Number	IP Address	Description	Location	Contact
Contains...	Contains...	Conta	Conta	Conta	Conta
1032	1231032	10.1.1.3	HQ LAB		[redacted]
› 1010	1231010	10.1.1.1	HQ LAB		[redacted]
1064	1231064	10.1.1.5	HQ LAB		[redacted]
2566225	2566225	0.0.0.0			
› 1144	1231144	10.1.1.10	HQ LAB		[redacted]
1176	1231176	10.1.1.12	HQ LAB		[redacted]
1014	1231014	10.1.1.1	HQ LAB		[redacted]
› 1016	1231016	10.1.1.2	HQ LAB		[redacted]
› 1048	1231048	10.1.1.4	HQ LAB		[redacted]
1015	1231015	10.1.1.1	HQ LAB		[redacted]

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.



Email Configuration

Mail Server (Name or IP) •
[redacted]

Email Sender Address •
[redacted]

Email Recipient Addresses
Comma-separated recipient email addresses

Comma-separated recipient email addresses

Mail Protocol •
SMTP

Mail Server Port •
587

☑ Enable STARTTLS?
□ Enable SSL?

Mail Server Login Name
[redacted]

Password
•••••••

Define Email Settings

1. Navigate to **Administration > System Configuration > Email Configuration**.
2. In the **Email Configuration** dialog box, fill in each property and define the required values to be notified about system issues (see the table below for information about these values).
3. When finished editing the properties, click **Test Configuration** to ensure that emails can be sent.
4. Click **Save**.

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

Below are explanations of the values that must be defined to receive email notifications about system issues:

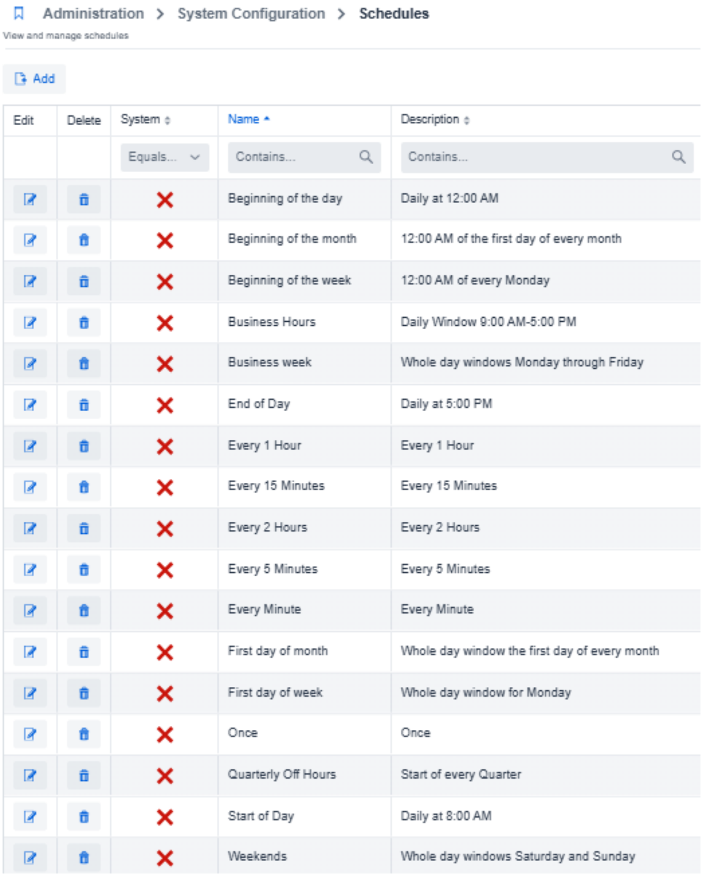
Mail Server	The host name or IP address of the mail

	server to be used for sending email.
Sender Address	The email address that will appear in the From portion of the sent email.
Recipient Addresses	The list of destination email addresses that should receive GE PulseNET email notifications. Separate multiple email addresses with a comma.
Mail Server Port	The port number that GE PulseNET uses to communicate with the mail server.
Mail Protocol	Transport protocol for sending email. Supports SMTP and SMTPS.
Enable STARTTLS?	Indicates whether the START- TLS protocol will be enabled and use encryption when sending emails from GE PulseNET.
Enable SSL?	Indicates whether the SSL protocol will be enabled and use encryption when sending emails from GE PulseNET.
Mail Server Login	The user name of the email account required by the mail server in order to send email.
User Password	The password for the above user account.

Schedules - Enterprise Only

GE PulseNET contains several predefined schedules which can be used during the process of scheduling reports. These schedules are different from 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.

Note: The timezone for these schedules is inherited from the GE PulseNET server time.



Administration > System Configuration > Schedules
View and manage schedules
Add

Edit	Delete	System	Name	Description
		Equals...	Contains...	Contains...
✎	🗑	✗	Beginning of the day	Daily at 12:00 AM
✎	🗑	✗	Beginning of the month	12:00 AM of the first day of every month
✎	🗑	✗	Beginning of the week	12:00 AM of every Monday
✎	🗑	✗	Business Hours	Daily Window 9:00 AM-5:00 PM
✎	🗑	✗	Business week	Whole day windows Monday through Friday
✎	🗑	✗	End of Day	Daily at 5:00 PM
✎	🗑	✗	Every 1 Hour	Every 1 Hour
✎	🗑	✗	Every 15 Minutes	Every 15 Minutes
✎	🗑	✗	Every 2 Hours	Every 2 Hours
✎	🗑	✗	Every 5 Minutes	Every 5 Minutes
✎	🗑	✗	Every Minute	Every Minute
✎	🗑	✗	First day of month	Whole day window the first day of every month
✎	🗑	✗	First day of week	Whole day window for Monday
✎	🗑	✗	Once	Once
✎	🗑	✗	Quarterly Off Hours	Start of every Quarter
✎	🗑	✗	Start of Day	Daily at 8:00 AM
✎	🗑	✗	Weekends	Whole day windows Saturday and Sunday

Adding a New System Schedule Definition

Navigate to Administration > System Configuration > Schedules. Add to the list of predefined system schedules by clicking the Add button.

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 chosen.
   a. **Once:** This option will set the start day/time for a single occurrence.

b. **Periodical:** This option will 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. The daily event can also be limited 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 that will be updated. Even though the schedule name cannot be changed, the description may need to be updated depending on the type of modification made to the existing schedule.

Deleting a System Schedule Definition

Delete a schedule by clicking the **Delete** icon for the row that will be removed. Click **Yes** to confirm deletion of the row.

Complementary Database - Enterprise Only

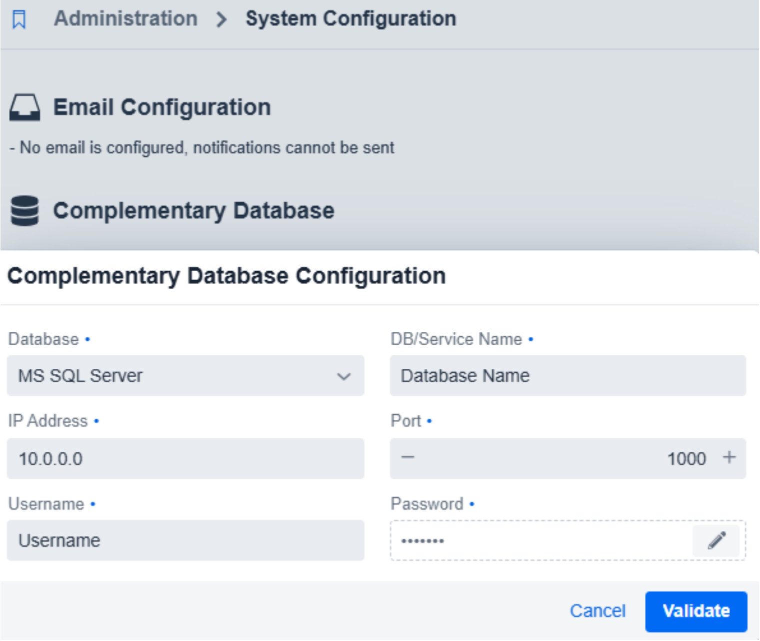
To connect and populate a complementary database, navigate to **Administration > System Configuration > Complementary Database**. GE PulseNET supports a complementary database for carrying alert history, device configuration and performance information only.

In the **Complementary Database Configuration** window, fill in the required fields. In the **Database** field, select whether to populate either an Oracle or Microsoft SQL complimentary database. In the following fields, enter the **IP Address**, **Port**, **Username** and **Password**.

NOTE: When connecting to and populating a Microsoft SQL server, PulseNET will connect to the default database. If the PulseNET database was set as the 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 the complimentary 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.



Administration > System Configuration

Email Configuration

- No email is configured, notifications cannot be sent

Complementary Database

Complementary Database Configuration

Database • MS SQL Server

DB/Service Name • Database Name

IP Address • 10.0.0.0

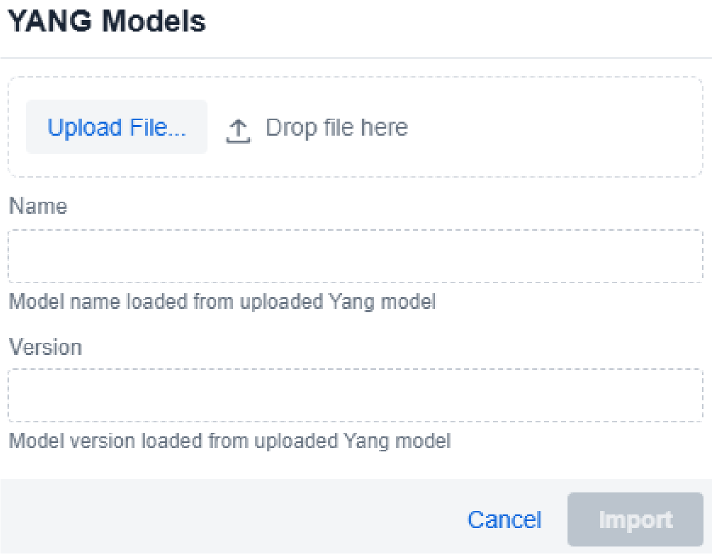
Port • 1000

Username • Username

Password • •••••••

YANG Model - Enterprise Only

The YANG Model is used with Change Management. The Yang Model **MUST** match that of the firmware in which you are using for making changes. A YANG model that GE MDS releases for an Orbit radio can be imported using this option under Administration => System Configuration. Selecting the YANG Model option brings up this view to enter the name of the YANG file or use the Upload button to select the file. The YANG file will be available from the GE MDS web site.


YANG Models

Name

Model name loaded from uploaded Yang model

Version

Model version loaded from uploaded Yang model

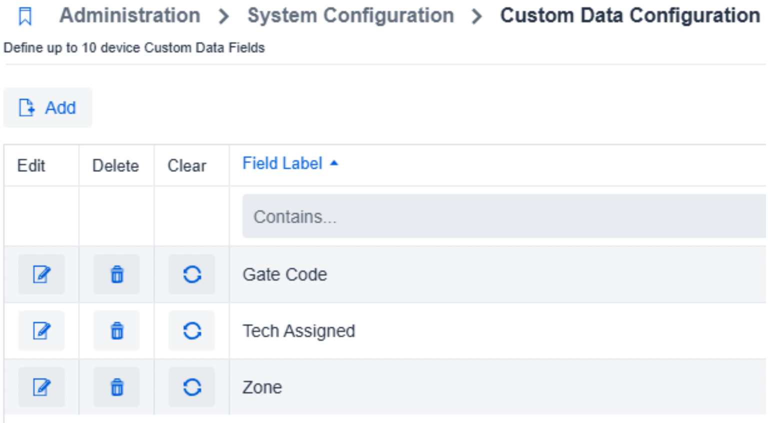
Yang Models already included:

4.3.8	7.1.1 (MPR)	9.0.3 (MCR/ECR)	9.5.1 (MPR)
4.8.3	7.6.5 (MCR/ECR)	9.0.3 (MPR)	9.6.3 (MCR/ECR)
5.0.8	7.6.5 (MPR)	9.1.5 (MCR/ECR)	9.6.3 (MPR)
6.1.2	8.0.7 (MCR/ECR)	9.1.5 (MPR)	9.6.4 (MCR/ECR)
6.6.1	8.0.7 (MPR)	9.2.2 (MCR/ECR)	9.6.4 (MPR)
6.7.8	8.0.8 (MCR/ECR)	9.2.2 (MPR)	9.6.11 (MCR/ECR)
6.8.0	8.0.8 (MPR)	9.3.3 (MCR/ECR)	9.6.11 (MPR)
6.8.1 (MCR/ECR)	8.2.2 (MCR/ECR)	9.3.3 (MPR)	
7.1.1 (MCR/ECR)	8.2.2 (MPR)	9.5.1 (MCR/ECR)	

Custom Data Configuration - Enterprise Only

If needing to store device information that GE PulseNET does not collect, up to ten device **Custom Data Fields** can be created in the **Custom Data Configuration** window.

Navigate to **Administration > System Configuration > Custom Data Configuration**



Administration > System Configuration > **Custom Data Configuration**

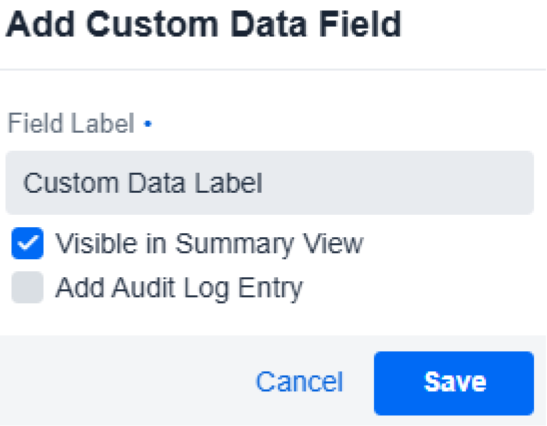
Define up to 10 device Custom Data Fields

Add

Edit	Delete	Clear	Field Label ▲
			Contains...
✎	🗑	↻	Gate Code
✎	🗑	↻	Tech Assigned
✎	🗑	↻	Zone

Create a Custom Data Field

1. In the **Custom Data Configuration** menu, click **Add**.



Add Custom Data Field

Field Label •

Custom Data Label

☑ Visible in Summary View

□ Add Audit Log Entry

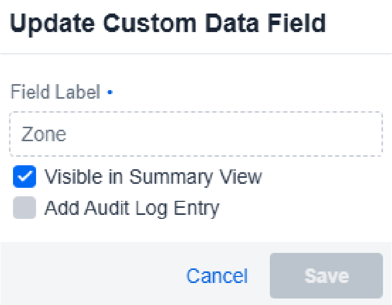
Cancel   **Save**

2. In the **Add Custom Data Field** dialog box that opens, type a label for the field in the **Field Label** field.
3. If the field will be visible in the **Summary View** for applicable devices, select the **Visible in Summary View** checkbox. Then navigate to Summary and select the new custom data field to display as a column. For more information on the Summary view, see the **Working with GE PulseNET** section of the **GE PulseNET User Guide**.
4. Check **Add Audit Log Entry** if changes to this custom field will be tracked in the device **Audit Log**.
5. Click **Save**.

The new field is added to the **Custom Data Field** tab on the **Device Detail View** for every monitored device, and as a column in the **Summary** view for applicable devices if the **Visible in Summary View** checkbox was selected. The field is a free-form text field with unlimited length.

Edit a Custom Data Field

1. In the **Custom Data Configuration** menu, click the **Edit** icon for the data field that will be edited.
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.



Update Custom Data Field

Field Label •

Zone

☑ Visible in Summary View

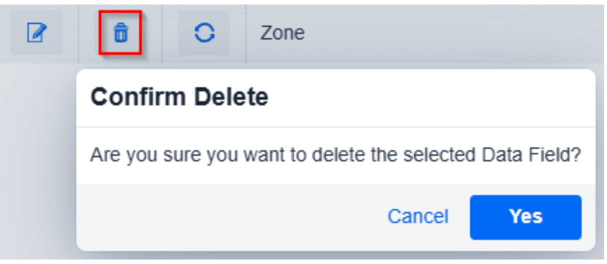
☐ Add Audit Log Entry

3. If the field will be visible in the **Summary View** for applicable devices, ensure the **Visible in Summary View** checkbox is selected. If not, clear that checkbox. 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 Admin or Operators to edit on the **Custom Data Field** tab on the **Device Detail View** for every device in the network. Input the data that will be displayed in the custom Summary column into the **Field Value** box and click Save. (See the **GE PulseNET User Guide** for details.)

Delete a Custom Data field

1. In the **Custom Data Configuration** menu, click the **Delete** icon on the row of the data field that will be deleted.



Zone

Confirm Delete

Are you sure you want to delete the selected Data Field?

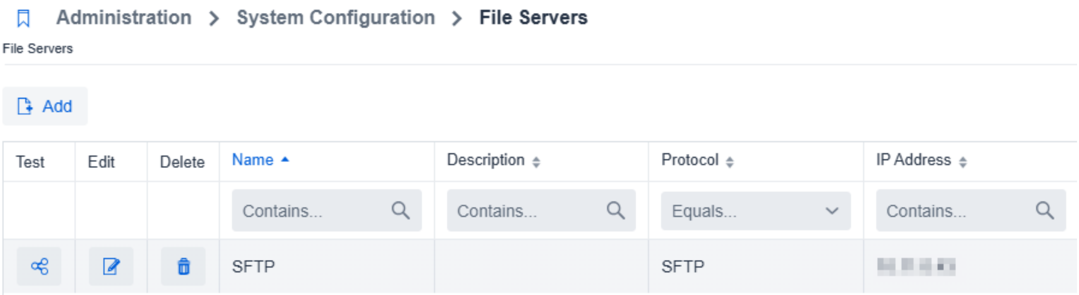
2. In the **Confirm Delete** dialogue box that appears, confirm the deletion of the data field by clicking the **Yes** button. Click the **Cancel** button to abort deletion

of the data field.

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

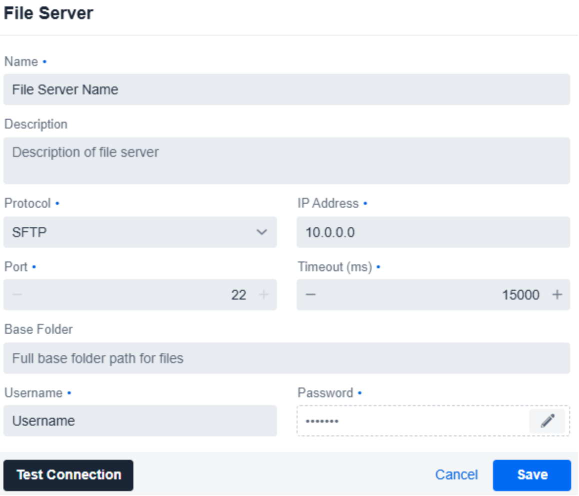
File Servers - Enterprise Only

To manage File Servers in GE PulseNET, navigate to **Administration > System Configuration > Files Servers**. This menu is used to define FTP/TFTP/SFTP servers for PulseNET firmware storage or backup storage.



Test	Edit	Delete	Name ▲	Description ⬍	Protocol ⬍	IP Address ⬍
			Contains...	Contains...	Equals...	Contains...
			SFTP		SFTP	[redacted]

Click the **Add** button to input the file server configuration, including the desired protocol desired and authentication information if applicable before clicking **Save**.



File Server

Name • File Server Name	
Description Description of file server	
Protocol • SFTP	IP Address • 10.0.0.0
Port • 22	Timeout (ms) • 15000
Base Folder Full base folder path for files	
Username • Username	Password • •••••••

Once the file server is defined it will show in the **Administration > System Configuration > File Servers** menu. Multiple file servers can be defined.

Note: The file server itself is external to PulseNET and configuration information will need to come from the company IT team, etc...

SNMP Trap Configuration - Enterprise Only

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.

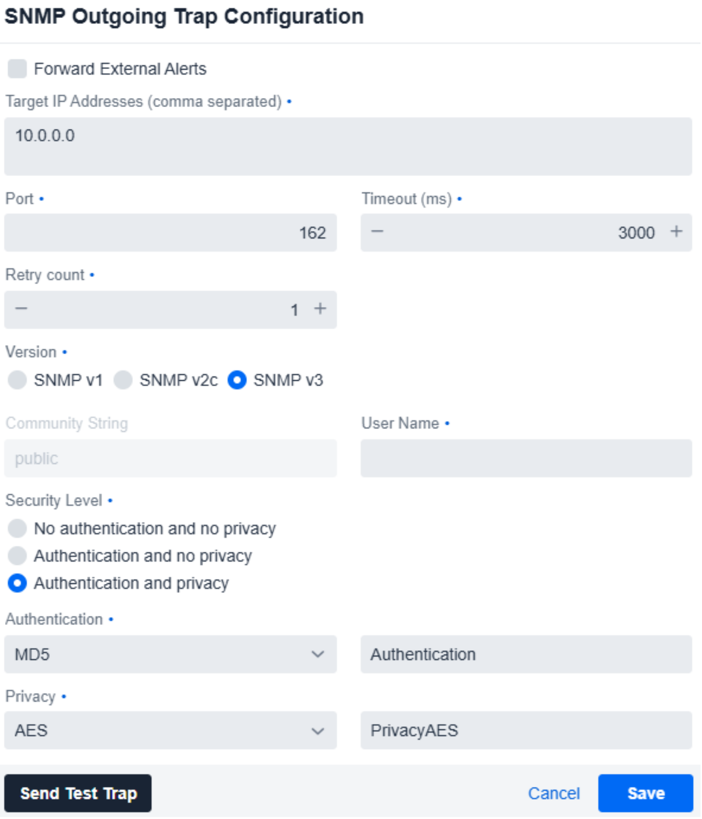
Navigate to **Administration > System Configuration**

Note: Refer to Appendix A for the traps format.

SNMP Outgoing Trap Configuration

In the **Outgoing** configuration, enable and define where to send the outgoing alerts, including the destination and credentials for the 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 the trap messages are being sent, verify the test message has been received.



SNMP Outgoing Trap Configuration

□ Forward External Alerts

Target IP Addresses (comma separated) •: 10.0.0.0

Port •: 162

Timeout (ms) •: 3000

Retry count •: 1

Version •: ○ SNMP v1 ○ SNMP v2c ● SNMP v3

Community String: public

User Name •:

Security Level •:
○ No authentication and no privacy
○ Authentication and no privacy
● Authentication and privacy

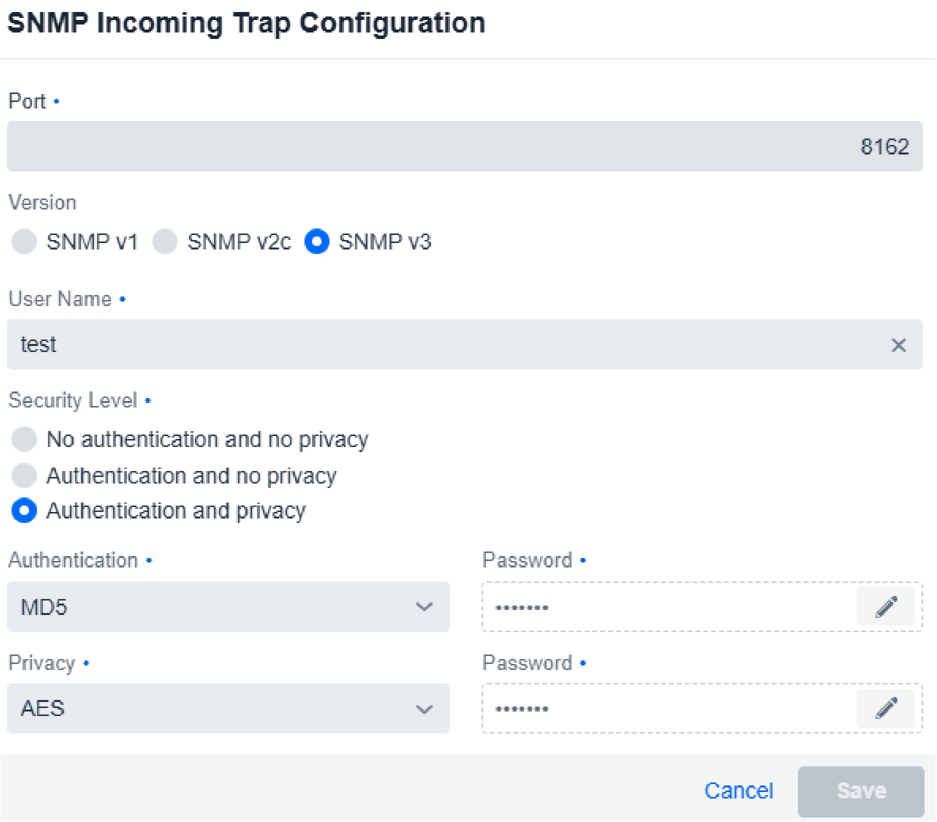
Authentication •: MD5 | Authentication

Privacy •: AES | PrivacyAES

SNMP Incoming Trap Configuration

In the **Incoming** configuration, enable and define how to receive incoming traps as device alerts, including the incoming trap port, SNMP version, 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: Orbit, iNET, Mercury, EntraNET and TD220X access points.



SNMP Incoming Trap Configuration

Port •
8162

Version
○ SNMP v1 ○ SNMP v2c ● SNMP v3

User Name •
test

Security Level •
○ No authentication and no privacy
○ Authentication and no privacy
● Authentication and privacy

Authentication •
MD5

Password •
•••••••

Privacy •
AES

Password •
•••••••

Certificate Management - Enterprise Only

The **Certificate Management** window allows for the management of Simple Certificate Enrollment Protocol (SCEP) security certificates and firmware certificates **only** on the GE MDS Orbit devices. To manage 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 modification of individual security certificate attributes, if needed.

The **Pre-expiration Window** is the number of days prior to the certificate's expiration that PulseNET will attempt to renew the certificate.

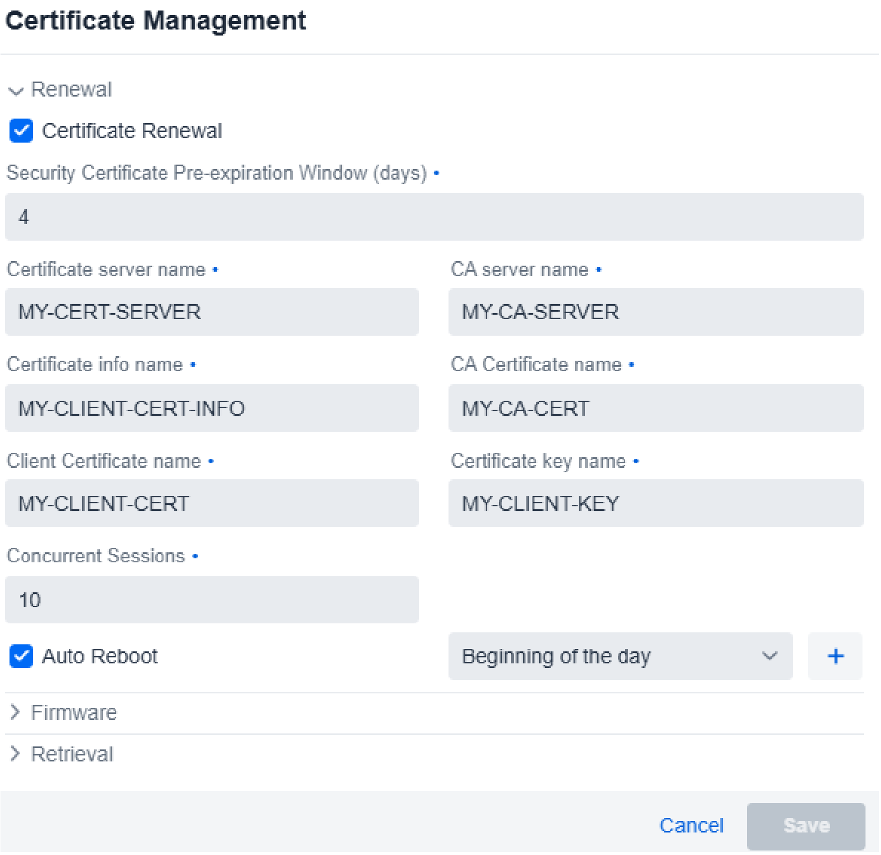
Concurrent Sessions defines how many Orbits PulseNET will run Certificate Retrieval Requests one at a time.

The **Auto Reboot** check box instructs PulseNET to initiate an auto reboot of the device when the reboot schedule is configured. This only happens if the certificate “from date” was updated since the last reboot (compare the uptime to the certificate “from date” to determine if Orbit needs reboot). Note: PulseNET will not reboot if the SGN and the ENC are the only certificates that are updated.

Reboot Schedule defines when to run the Auto Reboot.

Firmware Certificate Retrieval checkbox - when checked will retrieve each Orbit radios firmware certificate according to the retrieval schedule.

Select when the security and firmware certificates will be retrieved from the **Retrieval Schedule** dropdown menu.



Certificate Management

Renewal

☑ Certificate Renewal

Security Certificate Pre-expiration Window (days) •: 4

Certificate server name •: MY-CERT-SERVER

CA server name •: MY-CA-SERVER

Certificate info name •: MY-CLIENT-CERT-INFO

CA Certificate name •: MY-CA-CERT

Client Certificate name •: MY-CLIENT-CERT

Certificate key name •: MY-CLIENT-KEY

Concurrent Sessions •: 10

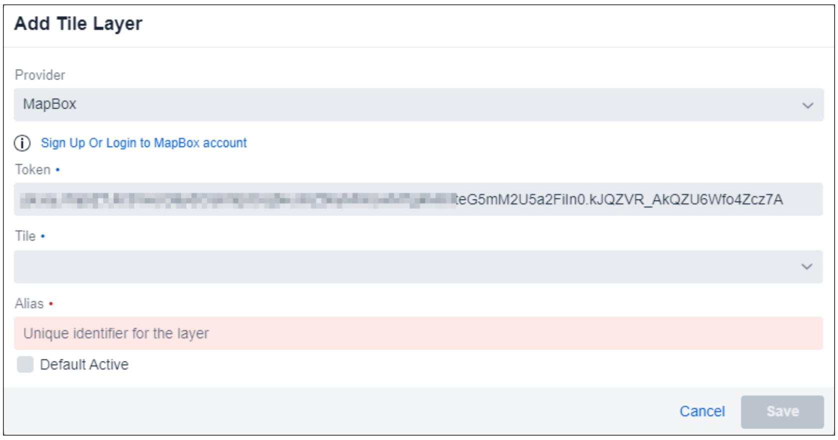
☑ Auto Reboot — Beginning of the day

Map Configuration

An Open Street Map is delivered with the product, but other map providers can be added. Navigate to **Administration > System Configuration > Map Configuration** and click the Add button to open the Add Tile Layer menu.

Select a **Provider** from the dropdown menu – MapBox, GoogleMap, or Custom – then provide the API token from the map provider.

Multiple **Tile** options may be available for use under the dropdown menu, depending on the mapping service used. Enter an Alias for the Map – and click Save.



Add Tile Layer

Provider: MapBox

Sign Up Or Login to MapBox account

Token •: [redacted]teG5mM2U5a2Filn0.kJQZVR_AkQZU6Wfo4Zcz7A

Tile •:

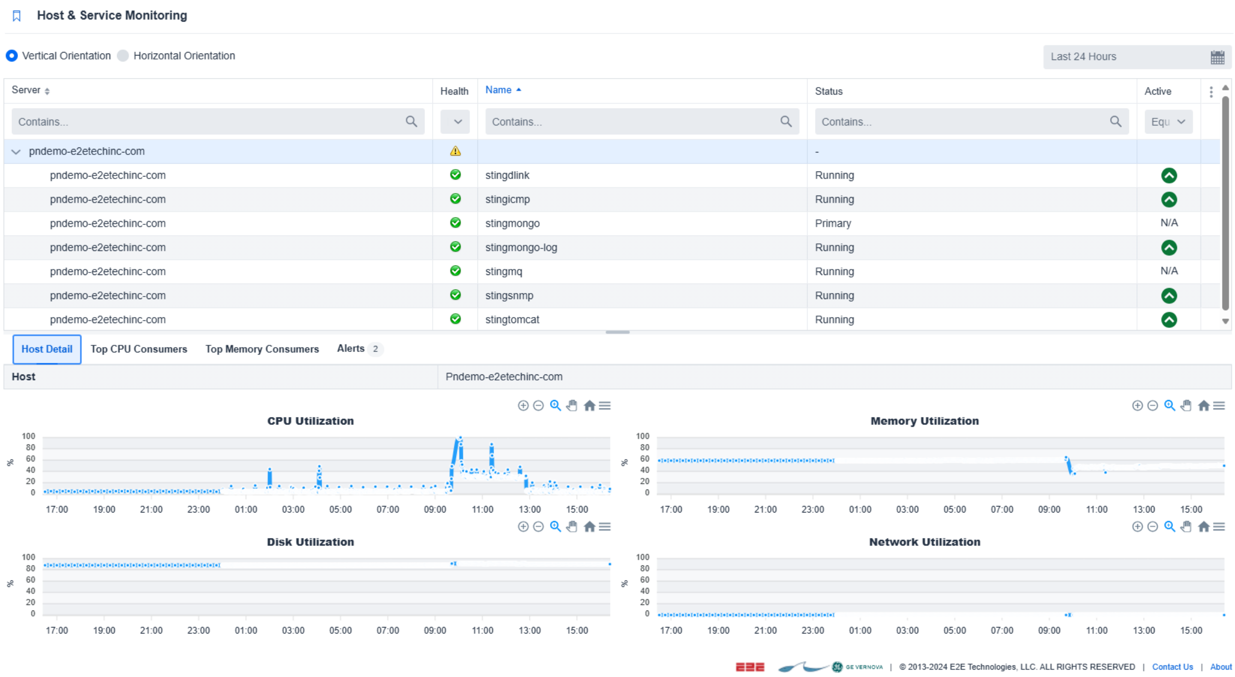
Alias •: Unique identifier for the layer

□ Default Active

Host and Service Monitoring

When GE PulseNET is installed, the software creates several 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.

Users can access the Host & Service Monitoring view from the left pane.



Host & Service Monitoring

● Vertical Orientation ○ Horizontal Orientation

Last 24 Hours

Server	Health	Name	Status	Active
pndemo-e2etechinc-com	⚠		-	
pndemo-e2etechinc-com	✓	stingdlink	Running	⬆
pndemo-e2etechinc-com	✓	stingicmp	Running	⬆
pndemo-e2etechinc-com	✓	stingmongo	Primary	N/A
pndemo-e2etechinc-com	✓	stingmongo-log	Running	⬆
pndemo-e2etechinc-com	✓	stingmq	Running	N/A
pndemo-e2etechinc-com	✓	stingsnmp	Running	⬆
pndemo-e2etechinc-com	✓	stingtomcat	Running	⬆

Host Detail | Top CPU Consumers | Top Memory Consumers | Alerts 2

Host	Pndemo-e2etechinc-com

From this view users can easily see the performance metrics of the host of where PulseNET is installed. Users will also be able to determine if a particular service(s) is running or stopped. Users can also change the orientation of the layout for better viewing using the Vertical and Horizontal orientation buttons at the top of the view.

This table works as a tree. At the top level you will have your host. This is where PulseNET is installed. The children underneath the top level are services installed on the server.

The **Health** column displays the current health of the host or service.

The **Name** column displays the name of the service.

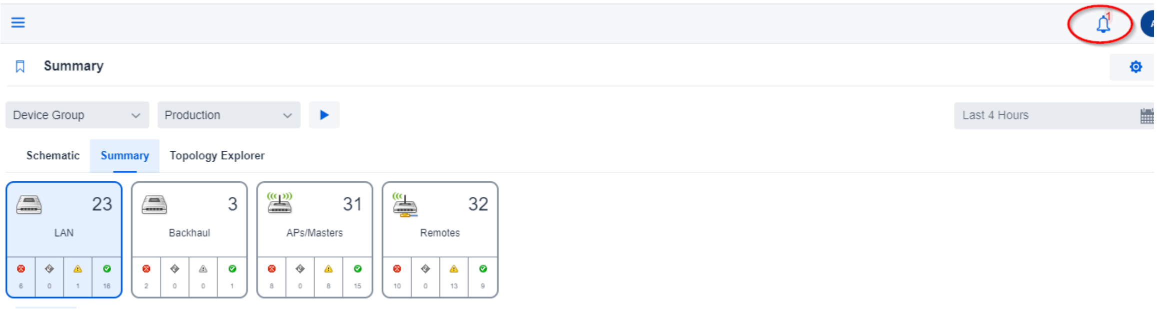
The **Status** column shows if the service is running on the host. Some services may read something other than runnning or not running. Such as the stingmongo service, it could be Startup2, primary, secondary, or arbiter.

The **Active** column indicates if the service is active or standby. In some cases, they may read something different. Other services such as stingmq and stingmongo will read N/A.

Service(s) may be selected by clicking to view more performance details in the charts below.

Notification Bell

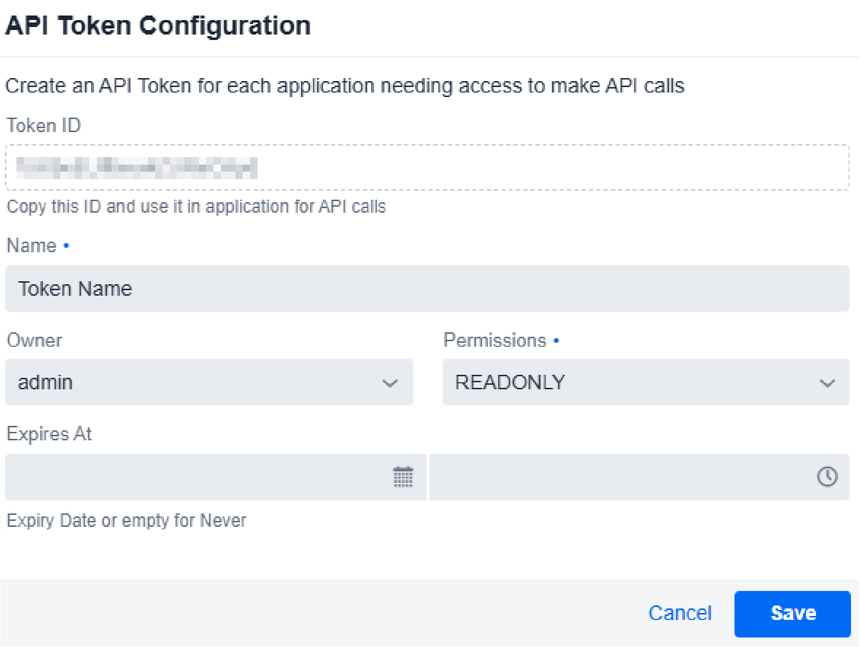
An alert will be shown in the **Notification Bell** window for services which are not running properly. To navigate to this window, look for the bell icon in the top-right of the screen which is displayed on all views and dashboards.



Click the **Notification Bell** icon 🔔 to show the **System Notifications** menu. This window will display any services that are not currently running.

API Tokens - Enterprise Only

An API token is a unique identifier created by GE PulseNET for other applications to request access. To integrate with PulseNET, generate an API token and provide that token to the other application. To generate an API Token, navigate to **Administration > System Configuration > API Tokens**. Click **Add** to create a random Token ID.



API Token Configuration

Create an API Token for each application needing access to make API calls

Token ID

[redacted]

Copy this ID and use it in application for API calls

Name •

Token Name

Owner	Permissions •
admin	READONLY

Expires At

Expiry Date or empty for Never

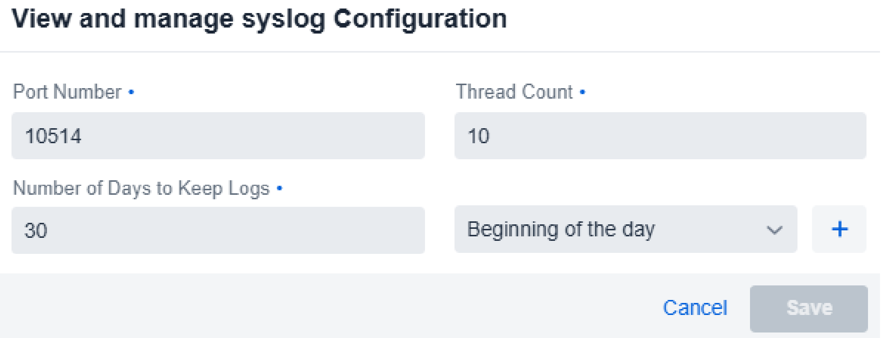
In the **API Token Configuration** dialog box, view the unique **Token ID** in the first field. The **Name** field adds a descriptive name to the token ID to help identify it. The **Expires At** field sets an expiry date for the token to determine when it expires. Use the **Permissions** drop-down menu, to determine which privileges the 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.

Click **Save** to return to the **Token ID** table, which lists and describes all of the unique token IDs that have been generated. 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 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.

Syslog Configuration and Rules - Enterprise Only

The **Syslog Configuration and Rules** summary allows creation, viewing, and management of 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 Configuration window, navigate to Administration > System Configuration and Rules > Syslog Configuration**.



View and manage syslog Configuration

Port Number • 10514

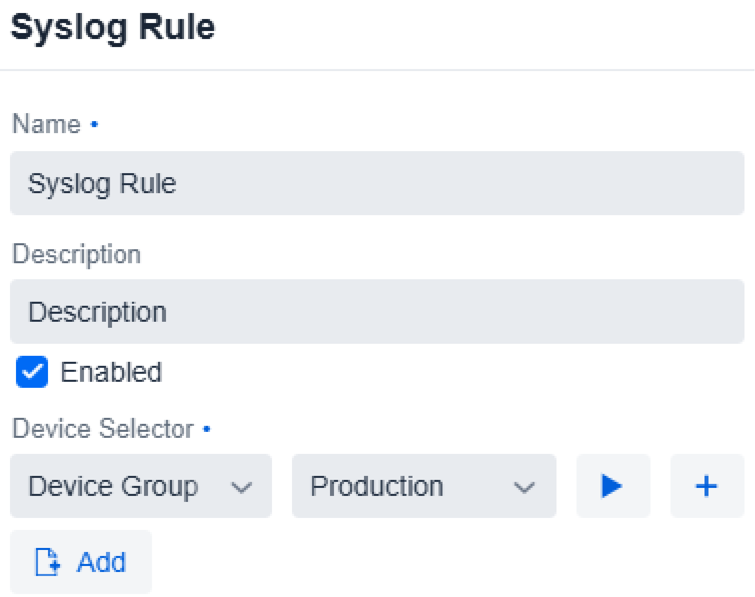
Thread Count • 10

Number of Days to Keep Logs • 30

Beginning of the day

Define the Port Number, Thread Count, Number of Days to Keep Logs, and the Purge Schedule, i.e. what time of day the logs will be deleted once the Number of Days threshold is reached.

To view existing Syslog Rules, or create new ones, navigate to **Administration > System Configuration and Rules >** Syslog Rules. To create a new syslog rule, click the **Add** button.



Syslog Rule

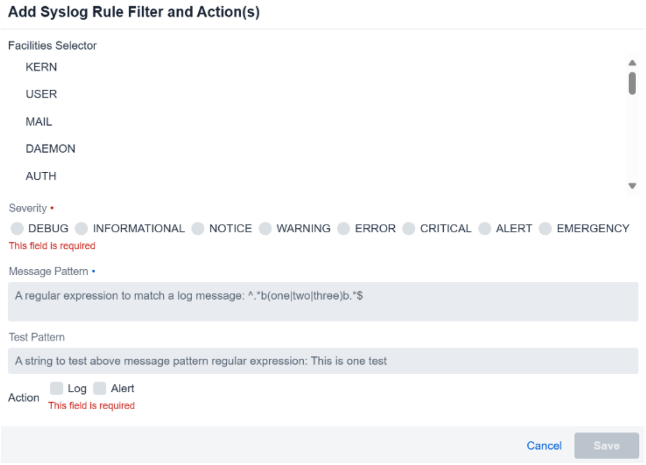
Name • Syslog Rule

Description: Description

☑ Enabled

Device Selector • Device Group, Production

In the **Syslog Rule** window, set the rule **Name** and **Description** and select the Device Group, Device Filter or Devices. Then click the **Add** button to create an associated Rule Filter and Action(s)



Add Syslog Rule Filter and Action(s)

Facilities Selector

KERN
USER
MAIL
DAEMON
AUTH

Severity •

○ DEBUG ○ INFORMATIONAL ○ NOTICE ○ WARNING ○ ERROR ○ CRITICAL ○ ALERT ○ EMERGENCY

This field is required

Message Pattern •

A regular expression to match a log message: ^.*b(one|two|three)b.*$

Test Pattern

A string to test above message pattern regular expression: This is one test

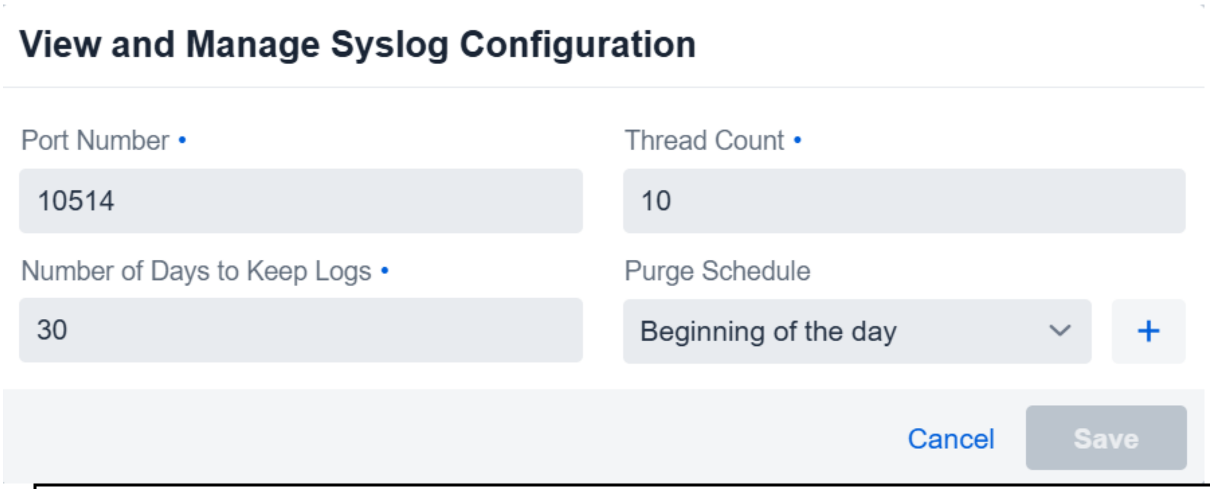
Action □ Log □ Alert

This field is required

In the **Add Syslog Rule Filter and Action(s)** window, set the parameters of the 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.

Syslog Rules 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 Configuration and Rules**.



View and Manage Syslog Configuration

Port Number • 10514

Thread Count • 10

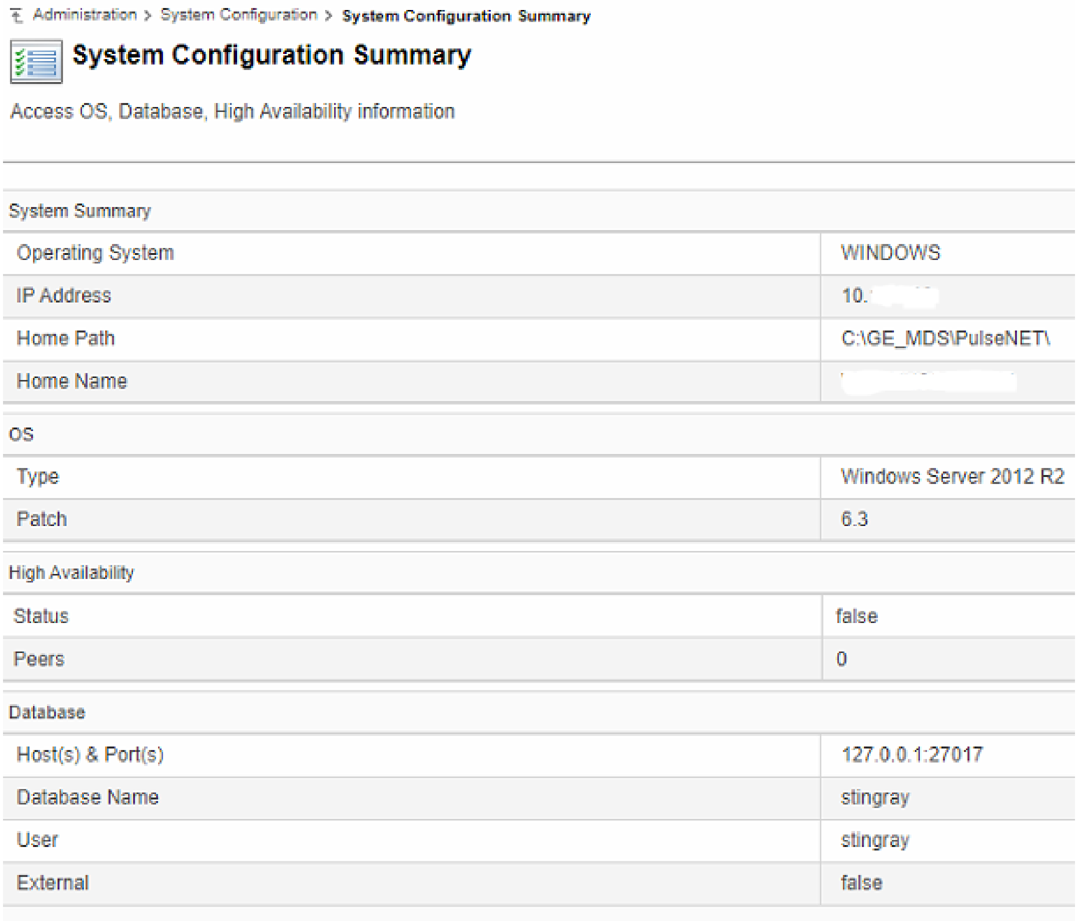
Number of Days to Keep Logs • 30

Purge Schedule: Beginning of the day

NOTE: Consider the size of the database when setting the 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.

System Configuration Summary - Enterprise Only

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**.

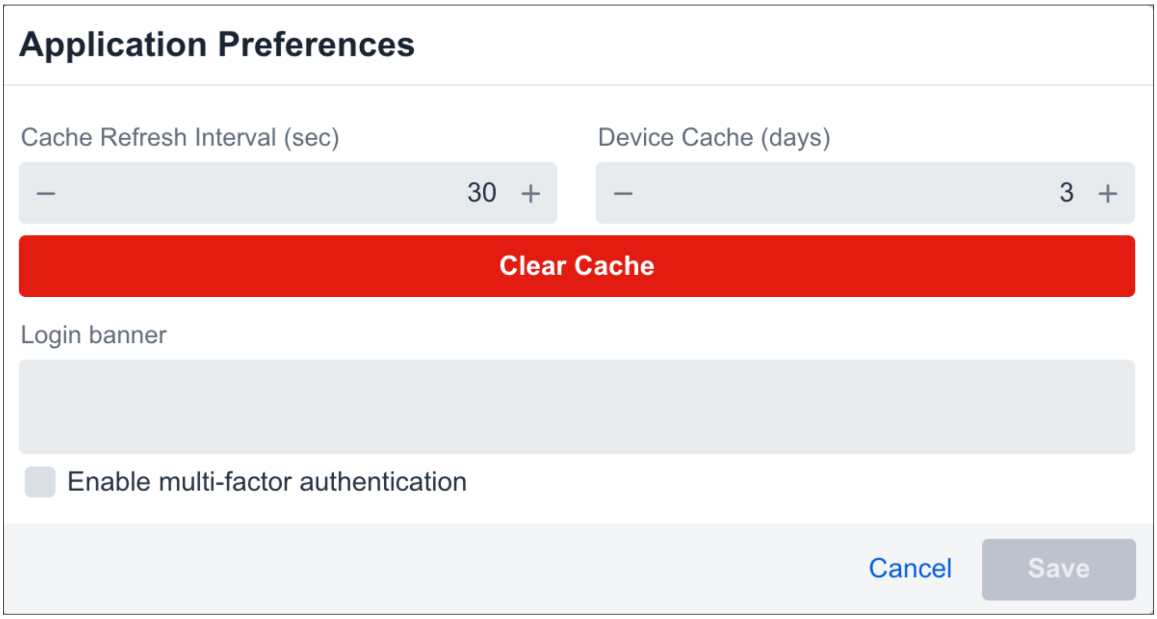


System Configuration Summary

Access OS, Database, High Availability information

System Summary	
Operating System	WINDOWS
IP Address	10.[redacted]
Home Path	C:\GE_MDS\PulseNET\
Home Name	[redacted]
OS	
Type	Windows Server 2012 R2
Patch	6.3
High Availability	
Status	false
Peers	0
Database	
Host(s) & Port(s)	127.0.0.1:27017
Database Name	stingray
User	stingray
External	false

Application Preferences



Application Preferences

Cache Refresh Interval (sec): 30

Device Cache (days): 3

Login banner

□ Enable multi-factor authentication

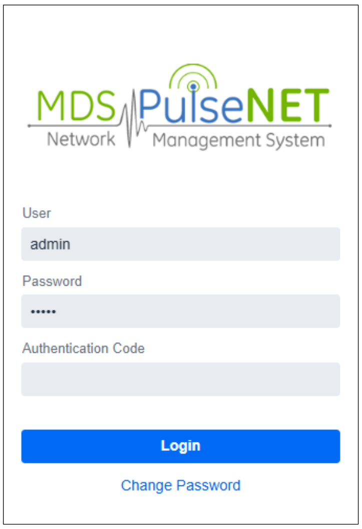
The Application Preferences menu is accessible from the user dropdown in the top-right corner by Administrator only. The Application preferences allow administrative users to change the behavior of the application. From here the user can set the following:

- **Cache Refresh Interval (secs):** This is how often the application will retrieve data from the database to store in cache. This will require restart of stingtomcat.
- **Device Cache (days):** This is how long of a period to store in cache. This will require restart of stingtomcat.
- **Clear Cache:** This option will clear all current cached data in the Total Summary and reload Device Data from the latest value polled in the Database. Note: The refresh will affect all users.
- **Login Banner:** This allows user to enter text to display before login.
- **Two-Factor Authentication:** When this button is checked two-factor authentication will be enabled.

Two Factor Authentication

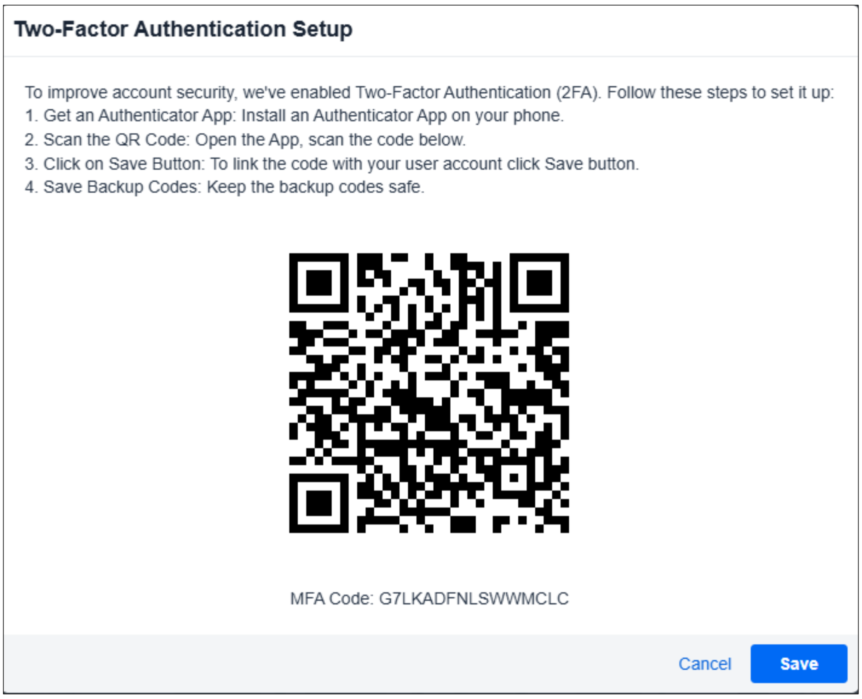
After Two-Factor Authentication has been enabled by an Administrator, any currently logged-in user(s) will be required to sign-out before two-factor authentication can be enforced.

On the first login use your username and password as normal, without the authentication code.



User
admin
Password
•••••
Authentication Code

A pop-up menu will appear with a QR code and instructions on how to link your user account.



Two-Factor Authentication Setup

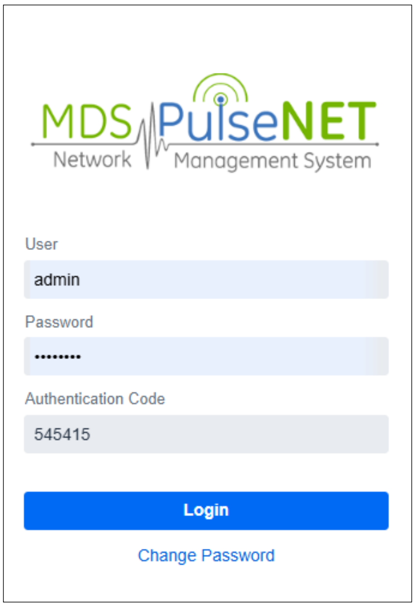
To improve account security, we've enabled Two-Factor Authentication (2FA). Follow these steps to set it up:
1. Get an Authenticator App: Install an Authenticator App on your phone.
2. Scan the QR Code: Open the App, scan the code below.
3. Click on Save Button: To link the code with your user account click Save button.
4. Save Backup Codes: Keep the backup codes safe.

MFA Code: G7LKADFNLSWWMCLC

Scan the QR code displayed on your screen with an authentication application of your choice.

Once the QR Code has been scanned, click Save to activate the associated PulseNET login.
Note: If Cancel is clicked instead, the Multi-Factor Authentication will not be enabled for the user, and they will not be able to log in.

Once the Authentication App has been connected, login with the user credentials and Authentication Code to proceed to PulseNET as shown below.

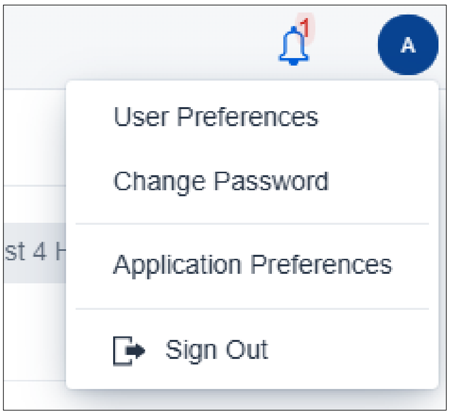


User: admin

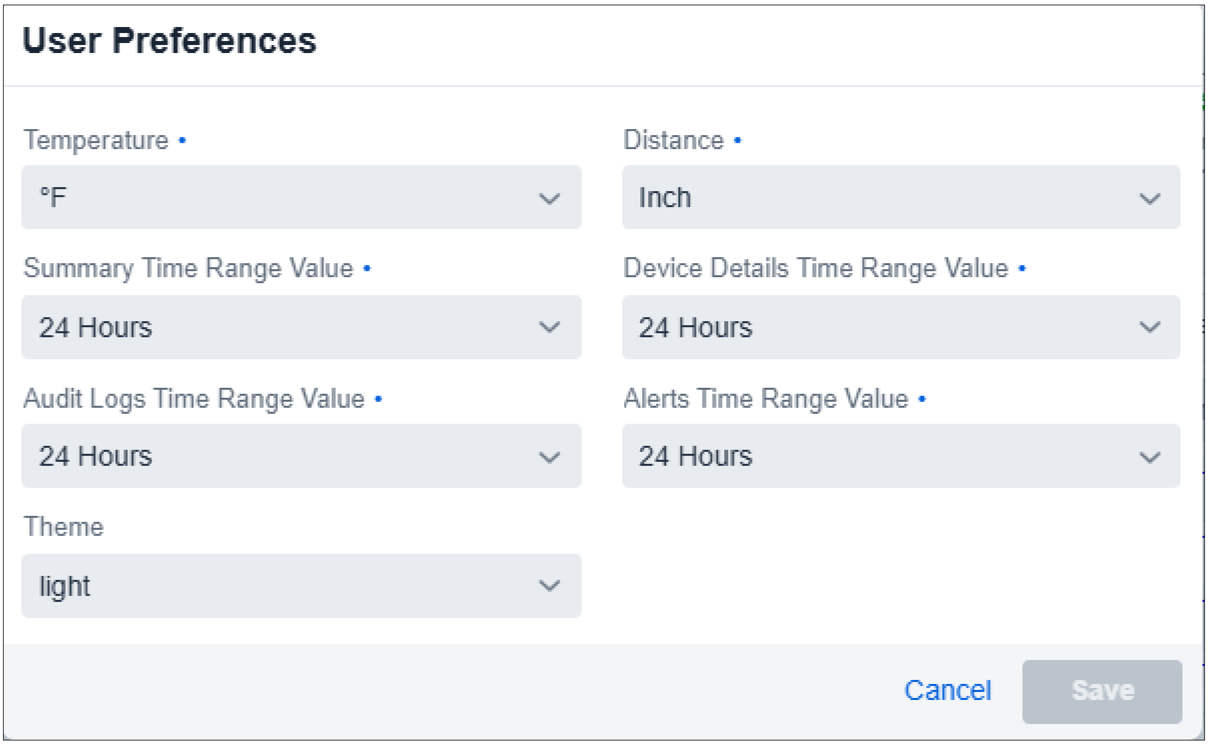
Password: ••••••••

Authentication Code: 545415

User Preferences



The User Preferences menu is accessible from the user dropdown in the top-right corner. It allows for the modification of user-specific settings such as desired system units for temperature and measurements, light or dark theme, and how the time range zonar will be set on the Summary, Device Detail, Audit Log and Alerts view.



User Preferences

Temperature •
°F

Distance •
Inch

Summary Time Range Value •
24 Hours

Device Details Time Range Value •
24 Hours

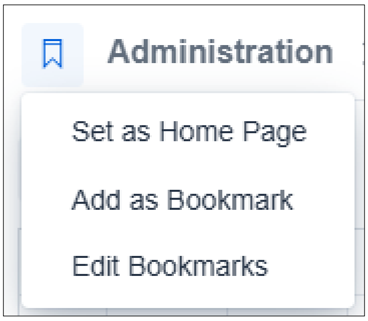
Audit Logs Time Range Value •
24 Hours

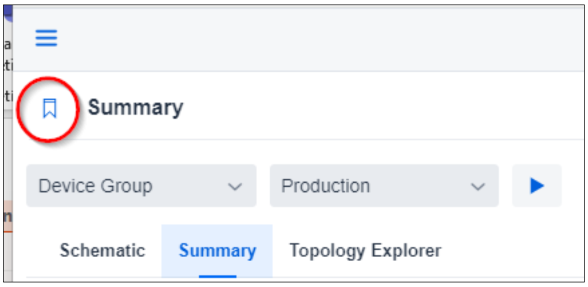
Alerts Time Range Value •
24 Hours

Theme
light

Bookmarks

Bookmarks can be set and managed via the use of the bookmark icon located in the top-left of any page. Adding a page as a bookmark will allow it to appear in the left-hand navigation column.





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 - Enterprise Only

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 - Enterprise Only

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.

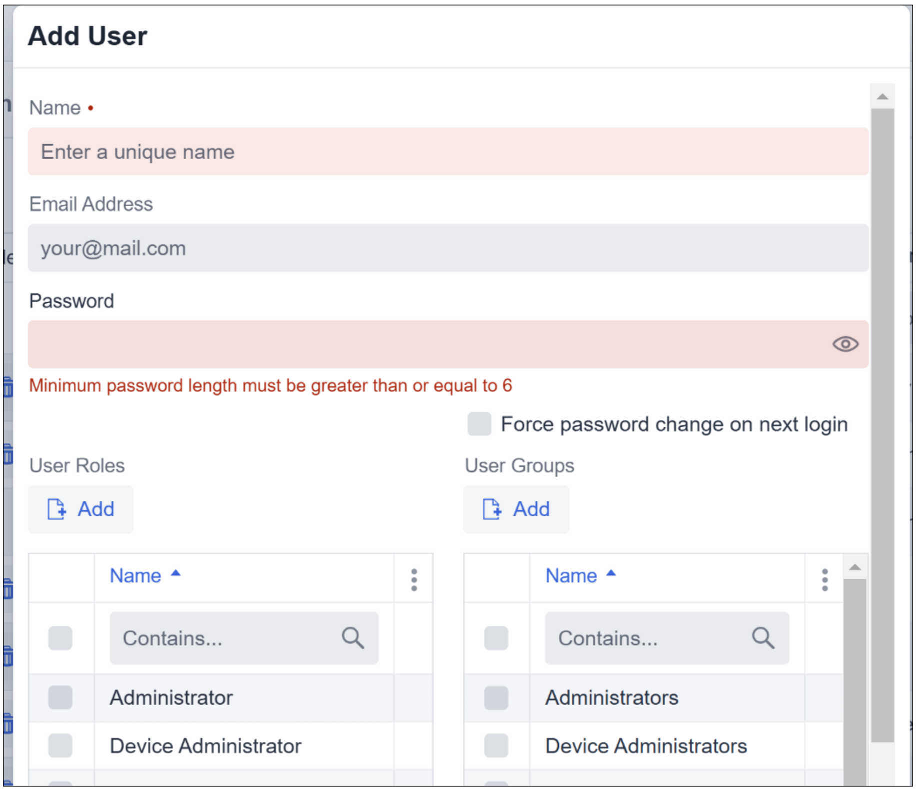
For most customers, the two default user groups will be adequate to delineate the needs of their GE PulseNET users. However, GE PulseNET also provides Administrators with the ability to create custom groups as needed. To create a new group, click the **Add** button at the upper left corner of the user 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. Optionally assign the new user to one or more user groups
8. Click **Save**.

The new user now appears in the users table.



Add User

Name •

Enter a unique name

Email Address

your@mail.com

Password

Minimum password length must be greater than or equal to 6

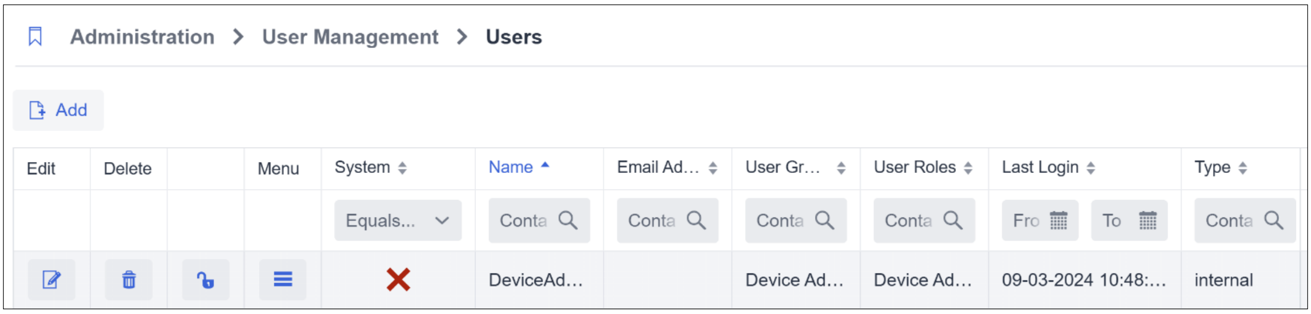
□ Force password change on next login

User Roles	User Groups
Add	Add

□	Name ▲
□	Contains...
□	Administrator
□	Device Administrator

□	Name ▲
□	Contains...
□	Administrators
□	Device Administrators

Managing Users



Administration > User Management > Users

Add

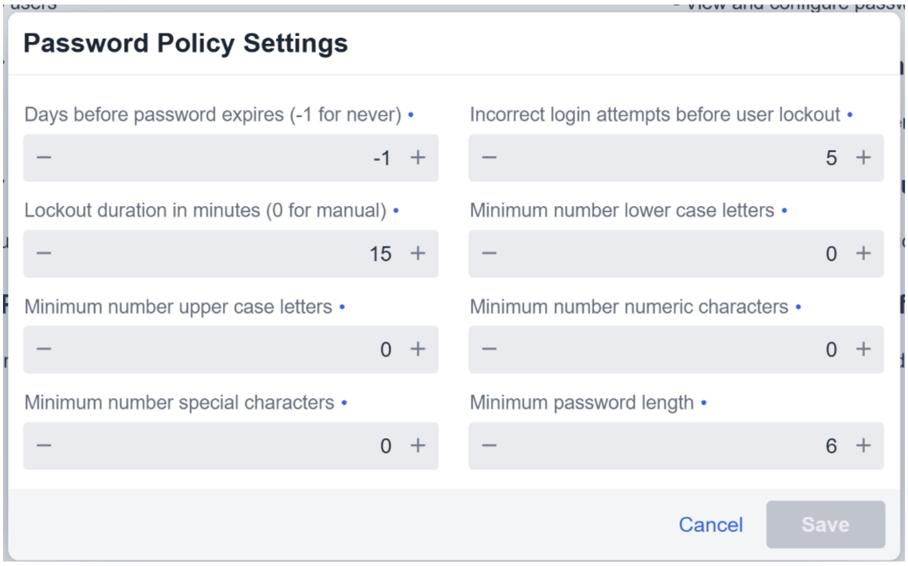
Edit	Delete		Menu	System	Name ▲	Email Ad...	User Gr...	User Roles	Last Login	Type
				Equals...	Conta	Conta	Conta	Conta	Fro To	Conta
				✗	DeviceAd...		Device Ad...	Device Ad...	09-03-2024 10:48:...	internal

All users are listed in the **Users** table. Each contains options to lock the account, edit the settings, or delete the user.

- 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 Logs** ≡ icon to view the GE PulseNET activity by this user

Configuring Password Policy

An Administrator can configure the global default password policy for user accounts.

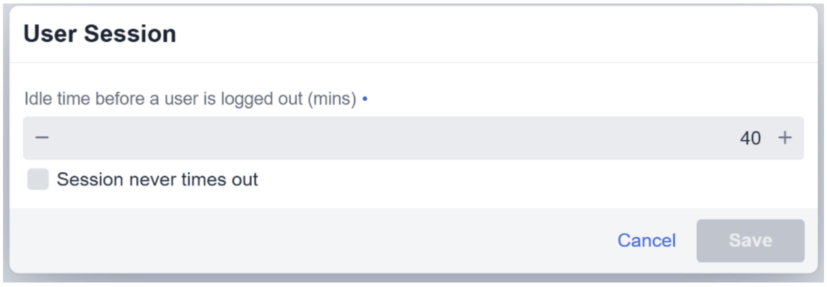


Password Policy Settings

Days before password expires (-1 for never) •	Incorrect login attempts before user lockout •
− -1 +	− 5 +
Lockout duration in minutes (0 for manual) •	Minimum number lower case letters •
− 15 +	− 0 +
Minimum number upper case letters •	Minimum number numeric characters •
− 0 +	− 0 +
Minimum number special characters •	Minimum password length •
− 0 +	− 6 +

Setting User Session Timeout

An Administrator can set the user session timeout in minutes. Or check the box which disables session timeout.



User Session

Idle time before a user is logged out (mins) •

− 40 +

□ Session never times out

Configuring LDAP - Enterprise Only

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

Familiarity with the details of the LDAP Directory Service, and related parameters is required to configure the feature 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

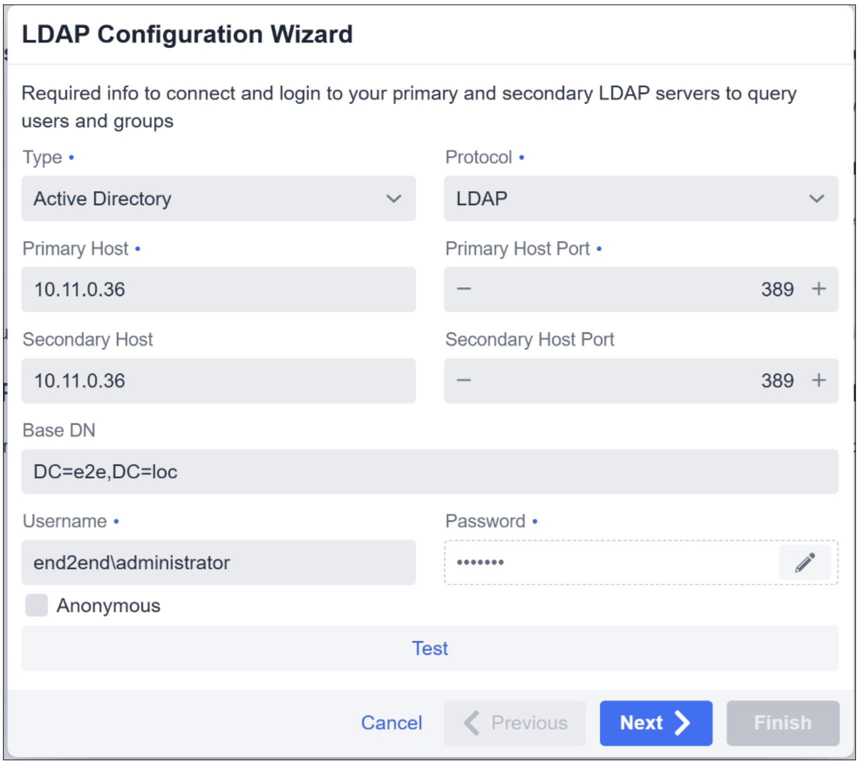
LDAP groups can be imported into GE PulseNET and assigned GE PulseNET roles. This allows users who have been granted special permissions within an organization to have associated permissions in GE PulseNET.

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 created 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 configuration of connectivity and login with the LDAP server.



LDAP Configuration Wizard

Required info to connect and login to your primary and secondary LDAP servers to query users and groups

Type • Active Directory

Protocol • LDAP

Primary Host • 10.11.0.36

Primary Host Port • 389

Secondary Host 10.11.0.36

Secondary Host Port 389

Base DN DC=e2e,DC=loc

Username • end2end\administrator

Password • •••••••

□ Anonymous

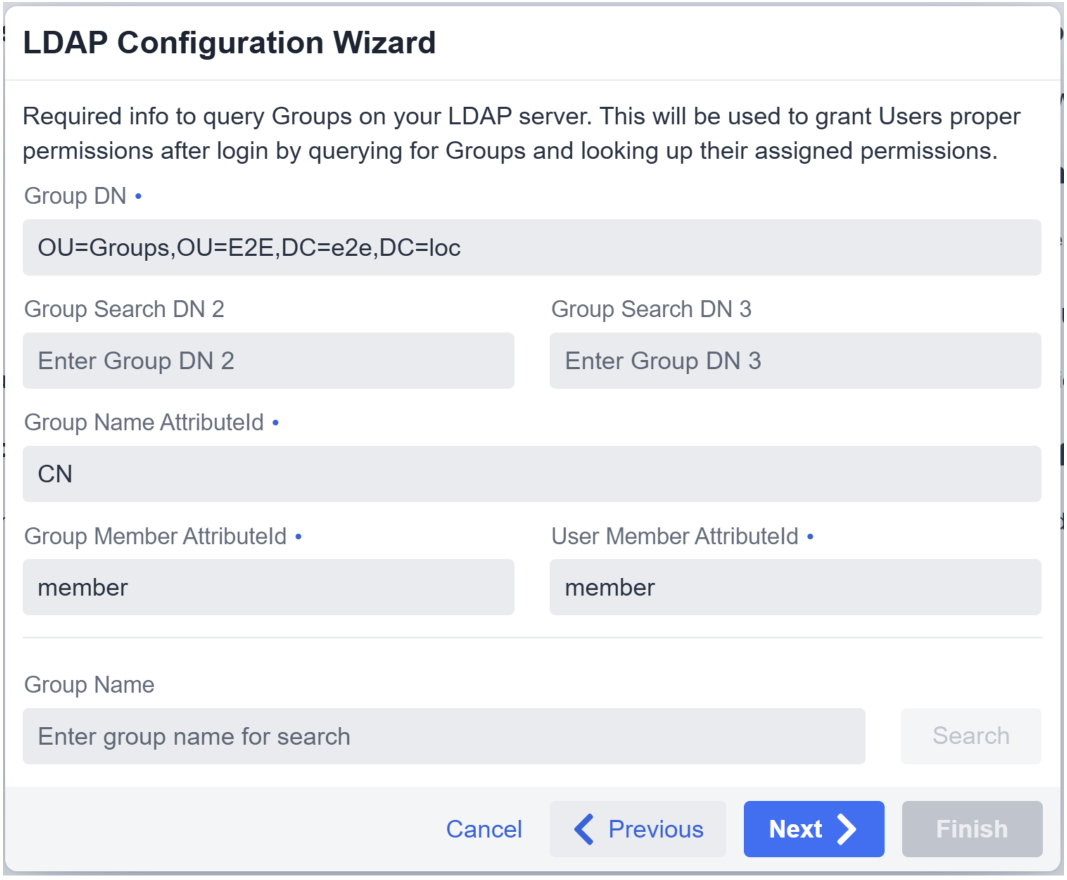
1. In the **LDAP Configuration Wizard** window, select the Type of LDAP server, either Active directory or other.
2. In the **Primary Host** field, select LDAP or LDAP over SSL.
3. In the **Primary Host Port** field, the default port will appear.
4. If using a failover server, enter the details in the **Secondary Host and Secondary Host Port** fields.
5. 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.
6. If the **Anonymous** checkbox is enabled, GE PulseNET will use an anonymous service account to search for users in the extended directory. The default username for anonymous service accounts is _anonymous_ and enabling this option sets the Distinguished Name of the service account to _anonymous_.
7. In the **Username** and **Password** fields, enter the username and password of the service account used for user searching in the external directory.
8. Click the **Test** button to test the system connection and login credentials for the LDAP

server. If the Test is successful, proceed to the next step.

9. Click the **Next >** button.

Find LDAP User Groups

Once configured, the second window in the **LDAP Configuration Wizard** will grant Users proper permissions after login by querying for Groups and looking for their assigned permissions.



LDAP Configuration Wizard

Required info to query Groups on your LDAP server. This will be used to grant Users proper permissions after login by querying for Groups and looking up their assigned permissions.

Group DN •
OU=Groups,OU=E2E,DC=e2e,DC=loc

Group Search DN 2
Enter Group DN 2

Group Search DN 3
Enter Group DN 3

Group Name AttributeId •
CN

Group Member AttributeId •
member

User Member AttributeId •
member

Group Name
Enter group name for search

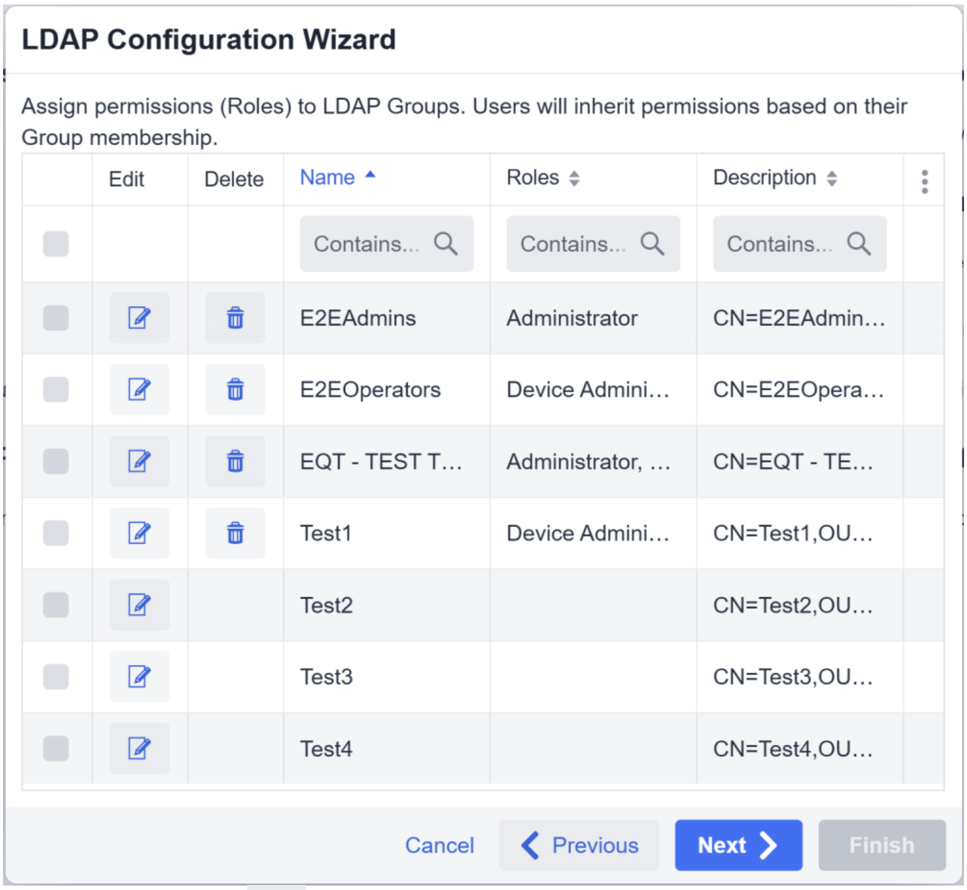
1. In the **Group DN** field, enter the search path for groups identified in the LDAP server. For example: OU=Groups,DC=2k3,DC=dom. The order in which the groups are searched is determined by the order of the groups listed in these settings. The **Group Search DN 2** and **3** fields are optional.
2.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

   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."

4. 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 for assigning permissions (roles) to LDAP Groups.

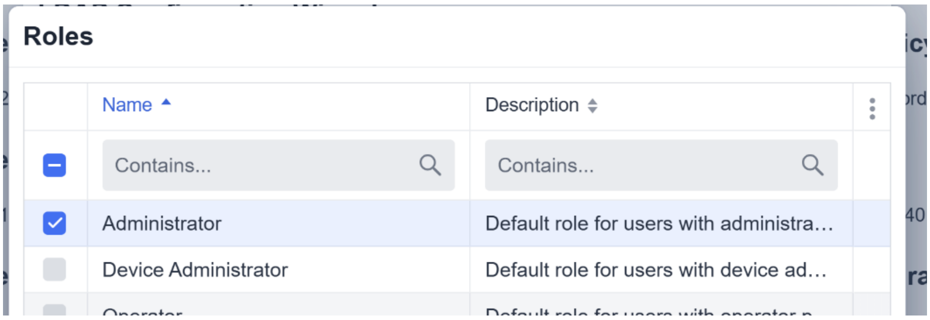


LDAP Configuration Wizard

Assign permissions (Roles) to LDAP Groups. Users will inherit permissions based on their Group membership.

	Edit	Delete	Name ▲	Roles ⬍	Description ⬍
☐			Contains...	Contains...	Contains...
☐	✎	🗑	E2EAdmins	Administrator	CN=E2EAdmin…
☐	✎	🗑	E2EOperators	Device Admini…	CN=E2EOpera…
☐	✎	🗑	EQT - TEST T…	Administrator, …	CN=EQT - TE…
☐	✎	🗑	Test1	Device Admini…	CN=Test1,OU…
☐	✎		Test2		CN=Test2,OU…
☐	✎		Test3		CN=Test3,OU…
☐	✎		Test4		CN=Test4,OU…

1. Select the edit icon ✎ of the LDAP Group to which roles will be assigned.

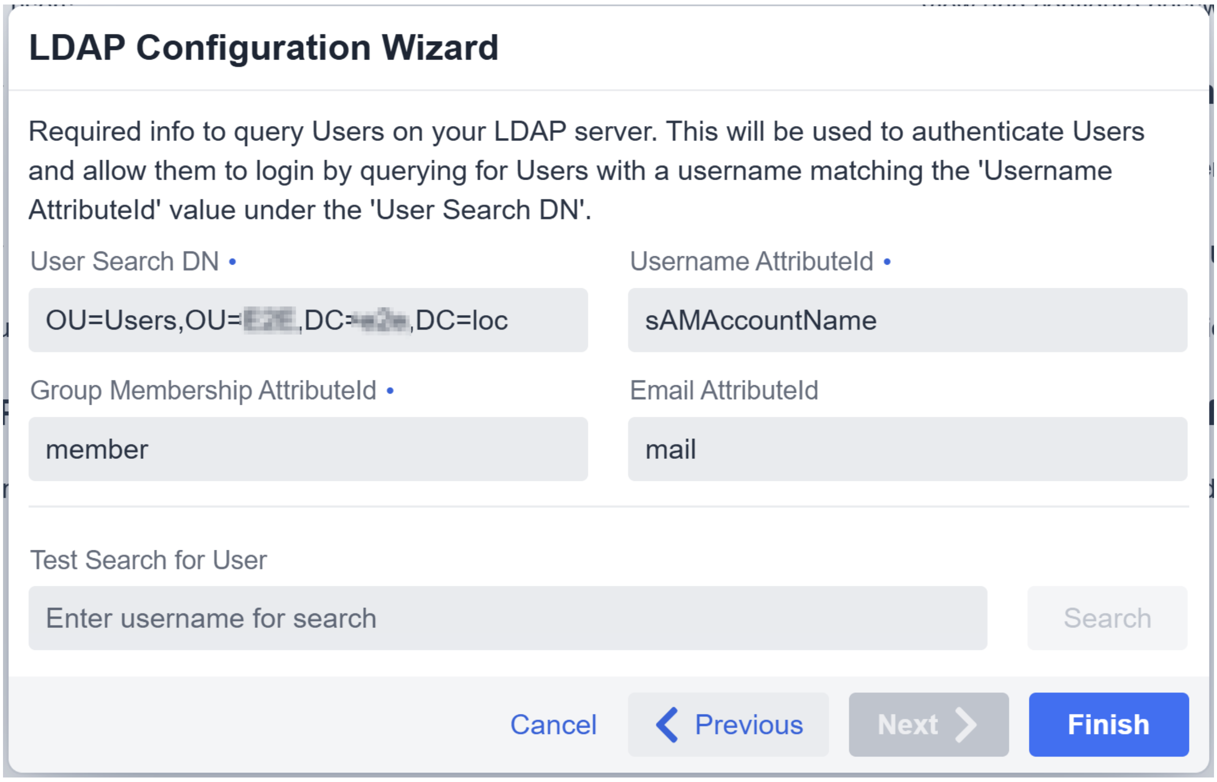


Roles

	Name ▲	Description ⬍
⊟	Contains...	Contains...
☑	Administrator	Default role for users with administra…
☐	Device Administrator	Default role for users with device ad…
☐	Operator	Default role for users with operator p…

Finding LDAP Users

The fourth window in the **LDAP Configuration Wizard** will test the connection and find LDAP Users.



LDAP Configuration Wizard

Required info to query Users on your LDAP server. This will be used to authenticate Users and allow them to login by querying for Users with a username matching the 'Username AttributeId' value under the 'User Search DN'.

User Search DN • OU=Users,OU=[redacted],DC=[redacted],DC=loc

Username AttributeId • sAMAccountName

Group Membership AttributeId • member

Email AttributeId mail

Test Search for User: Enter username for search

2. In the **User Search DN** field, enter the search path for users identified in the 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
3. In the **Username Attribute-ID** field, enter the Attribute-ID which contains the Username. For example, in Active Directory, the default is sAMAccountName.
4. 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.
5. 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.
6. 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.

7. 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 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 the LDAP server, ensure that the GE PulseNET LDAP client trusts the LDAP server by installing 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 the secure LDAP server and make sure it is accessible under <pulsenet_home>
3. Use the Java keytool program to import the LDAP server's root CA certificate into the keystore. Refer to the documentation for the Java keytool command if needed. *(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 to 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 the secure LDAP server.

LDAP User Groups - Enterprise Only

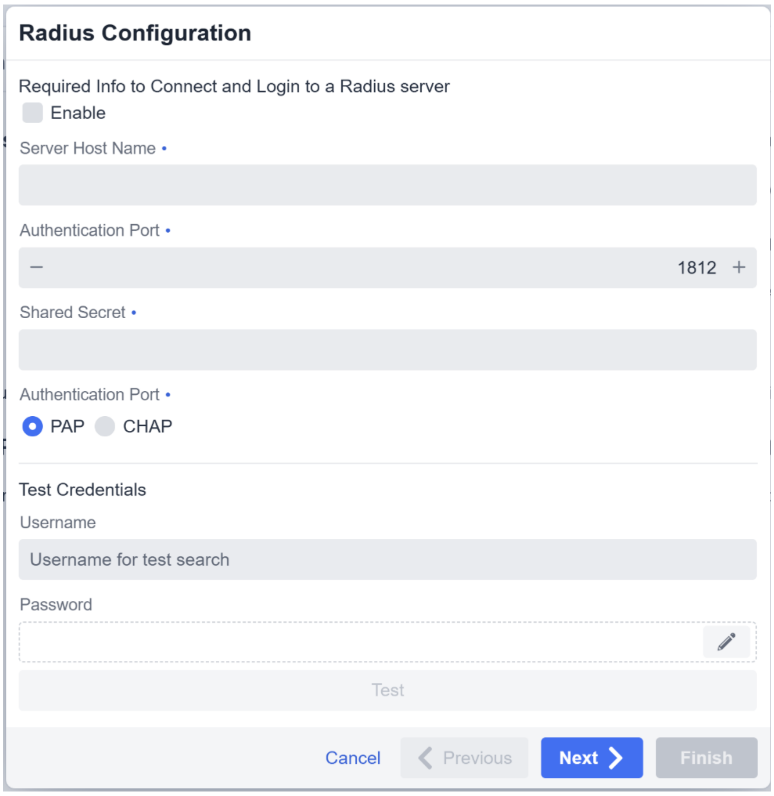
To manage the roles assigned to LDAP User Groups navigate to **Administration > User Management > LDAP** User Groups.

1. Select the LDAP Groups to which roles will be assigned by clicking the checkbox.
2. Click the **Assign** button.
3. In the **Select Role** window, select the role that will be assigned 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 - Enterprise Only

If using "Remote Authentication Dial In User Service" (RADIUS) to manage user access to the network, RADIUS server authentication can be enabled in GE PulseNET. When the GE PulseNET server is configured to access the RADIUS server, it is able to authenticate GE PulseNET users, which allows management of user credentials with RADIUS.

Enable RADIUS Authentication



Radius Configuration

Required Info to Connect and Login to a Radius server

□ Enable

Server Host Name •

Authentication Port •
− 1812 +

Shared Secret •

Authentication Port •
● PAP ○ CHAP

Test Credentials

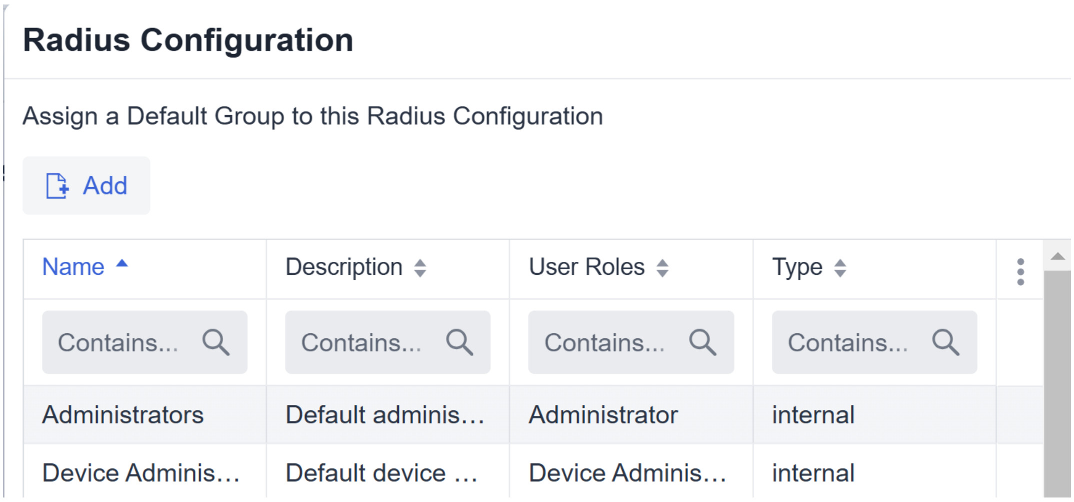
Username
Username for test search

Password

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 Port** — PAP (Password Authentication Protocol) and CHAP (Challenge-Handshake Authentication Protocol) are both supported.
7. To ensure that all values are correct, 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, default roles for users can be defined.

Define User Roles

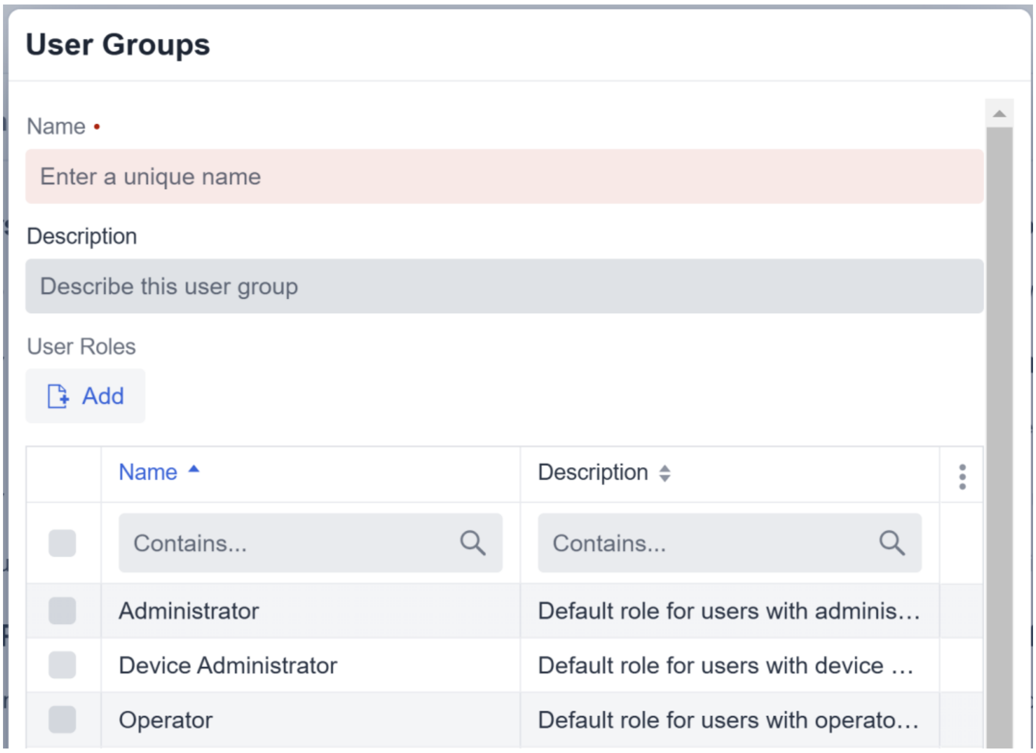


Radius Configuration

Assign a Default Group to this Radius Configuration

Name	Description	User Roles	Type
Contains...	Contains...	Contains...	Contains...
Administrators	Default adminis…	Administrator	internal
Device Adminis…	Default device …	Device Adminis…	internal

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.



User Groups

Name •

Enter a unique name

Description

Describe this user group

User Roles

	Name ▲	Description ⬍
□	Contains...	Contains...
□	Administrator	Default role for users with adminis…
□	Device Administrator	Default role for users with device …
□	Operator	Default role for users with operato…

2. Alternatively, 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 to efficiently monitor the devices on the 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 outages occur or defined thresholds are broken in the monitored environment. Once a performance rule has been enabled, GE PulseNET will send an alert ✖ fatal, ◆ critical, or ⚠ warning when 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.

Email notifications based on GE PulseNET rules — Email notifications can be configured and sent if problems arise in the monitored environment. These notifications can be enabled by checking the Enable Email checkbox for the desired severity levels within each rule.

SMS - Text Alerts
Support for SMS is handled using the email addresses that are routed by the carrier to the SMS of the device. For example: an SMS text to a Verizon user, the email address is formatted as phone number + vtext.com
i.e. 55535437532@vtext.com.

Click here for the explanation page for Verizon. Other carriers have similar capabilities.

Predefined Rules

GE PulseNET contains a number of predefined rules for device monitoring. These rules can be enabled, and thresholds configure so that notifications will be sent. The option is also available to select specific recipient users, roles, or groups to be notified when rule thresholds are exceeded. 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.**

The following table provides a description of some predefined rules:

Rule	Description	Severity
AP Change for Remote	Monitors remote devices for migration to different access points.	N/A
Bad Access Point Health	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.	Warning, Critical, Fatal
Bad Remote Health	Monitors the percentage of remote devices that are in a particular alert state or worse.	Warning, Critical, Fatal
Bad Repeater Health	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.	Warning, Critical, Fatal
Device Unavailable	Monitors the availability of the device.	Fatal
DLINK Alert Notification	Monitors whether a DLINK alarm has been received from a narrowband radio.	N/A
PA Temperature	Generates alerts for DLINK devices when Power Amplifier temperatures reach defined limits.	Warning, Critical, Fatal
Poor Response Time	Monitors the ICMP round trip time for a device.	Warning, Critical, Fatal
RSSI Change	Monitors values of RSSI that are outside the two-day moving average.	Warning, Critical, Fatal

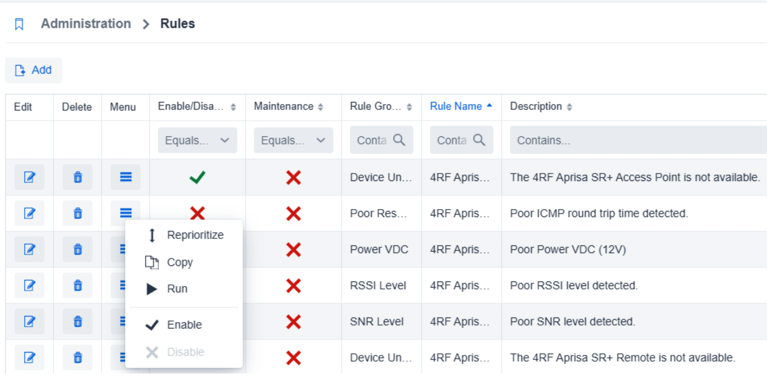
RSSI Level	Monitors the levels of Received Signal for devices.	Warning, Critical, Fatal
SD Master Station Failover	Monitors whether a radio failover has occurred between redundant radio modules.	N/A
Serial Number Unrecognizable	Generates an alert when the serial number of a DLINK access point is unrecognizable	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
Database Health	Monitors attached database performance.	Warning, Critical, Fatal
JVM	Monitors system memory.	Warning, Critical, Fatal
Orbit Cert Update	Every Midnight - checks device for certificate.	Fatal
Orbit Cert Renewal	This rule checks to see if a reboot is required or if the cert renewal failed.	Fatal
Orbit Cert Expiry	This rule checks for if the certificate is expiring or expired.	Fatal

NOTE: Some of the predefined rules are disabled by default. Ensure all required rules have been enabled.

Enable/Disable/Delete - Enterprise Only

To enable rules

1. Navigate to **Administration > Rules**
2. On the **Rules** dashboard, find the row for the rule that will be enabled.
3. On the row(s) for the desired rule, select the Menu icon then click **Enable**



Edit	Delete	Menu	Enable/Disa...	Maintenance	Rule Gro...	Rule Name	Description
			Equals...	Equals...	Conta	Conta	Contains...
			✓	✗	Device Un...	4RF Apris...	The 4RF Aprisa SR+ Access Point is not available.
			✗	✗	Poor Res...	4RF Apris...	Poor ICMP round trip time detected.
				✗	Power VDC	4RF Apris...	Poor Power VDC (12V)
				✗	RSSI Level	4RF Apris...	Poor RSSI level detected.
				✗	SNR Level	4RF Apris...	Poor SNR level detected.
				✗	Device Un...	4RF Apris...	The 4RF Aprisa SR+ Remote is not available.

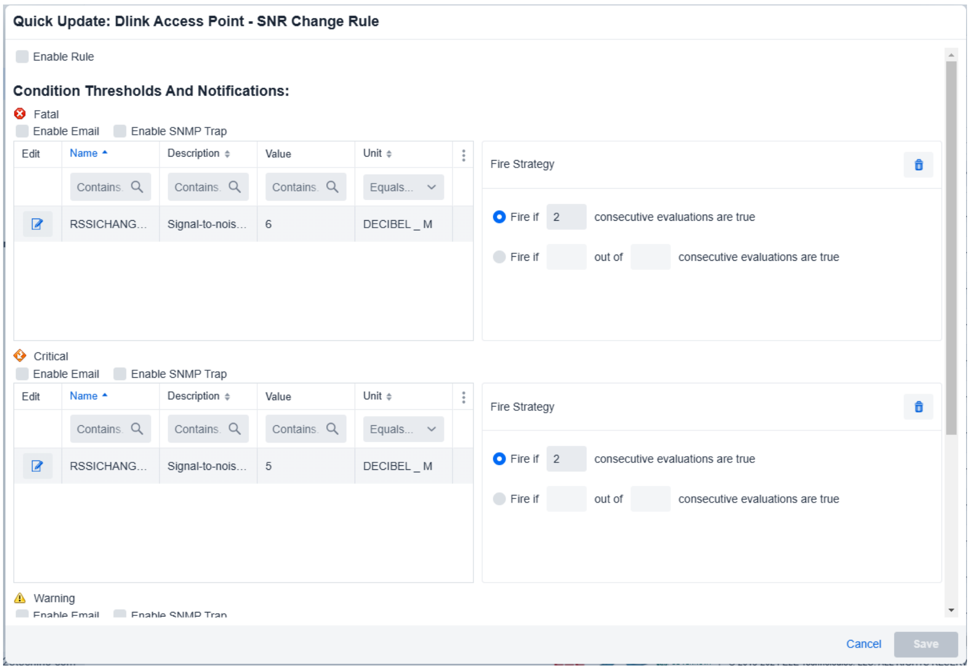
Multiple severity rules can have different conditions defined so that notifications are sent when increasing or decreasing thresholds are met. Once a rule is enabled, define the required threshold values and enable email notifications if desired.

Quick Update for Rule Settings

Most GE PulseNET Multiple Severity Rules have four thresholds: ⊗ fatal, ◆ critical, ⚠ warning, and ✓ normal. Define threshold values for the rule so that GE PulseNET sends alerts when the required condition is met.

Configure thresholds for a rule

1. Navigate to **Administration > Rules**.
2. Click the **Edit** icon for the rule that will be modified and select **Quick Update**.
3. Click the **Edit** icon for any value that will be edited.
4. Type the new value and click **Save**.



Quick Update: Dlink Access Point - SNR Change Rule

□ Enable Rule

Condition Thresholds And Notifications:

Fatal

□ Enable Email □ Enable SNMP Trap

Edit	Name	Description	Value	Unit
	Contains	Contains	Contains	Equals...
	RSSICHANG...	Signal-to-nois...	6	DECIBEL _ M

Fire Strategy

● Fire if 2 consecutive evaluations are true

○ Fire if out of consecutive evaluations are true

Critical

□ Enable Email □ Enable SNMP Trap

Edit	Name	Description	Value	Unit
	Contains	Contains	Contains	Equals...
	RSSICHANG...	Signal-to-nois...	5	DECIBEL _ M

Fire Strategy

● Fire if 2 consecutive evaluations are true

○ Fire if out of consecutive evaluations are true

Warning

□ Enable Email □ Enable SNMP Trap

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. To smooth out any “flapping” conditions for a device on the borderline of this threshold, set the strategy to fire an alert only if GE PulseNET detects the threshold has been breached on three consecutive polls. The strategy can also be set to fire an alert if GE PulseNET detects the threshold has been breached on three of the last five consecutive polls.

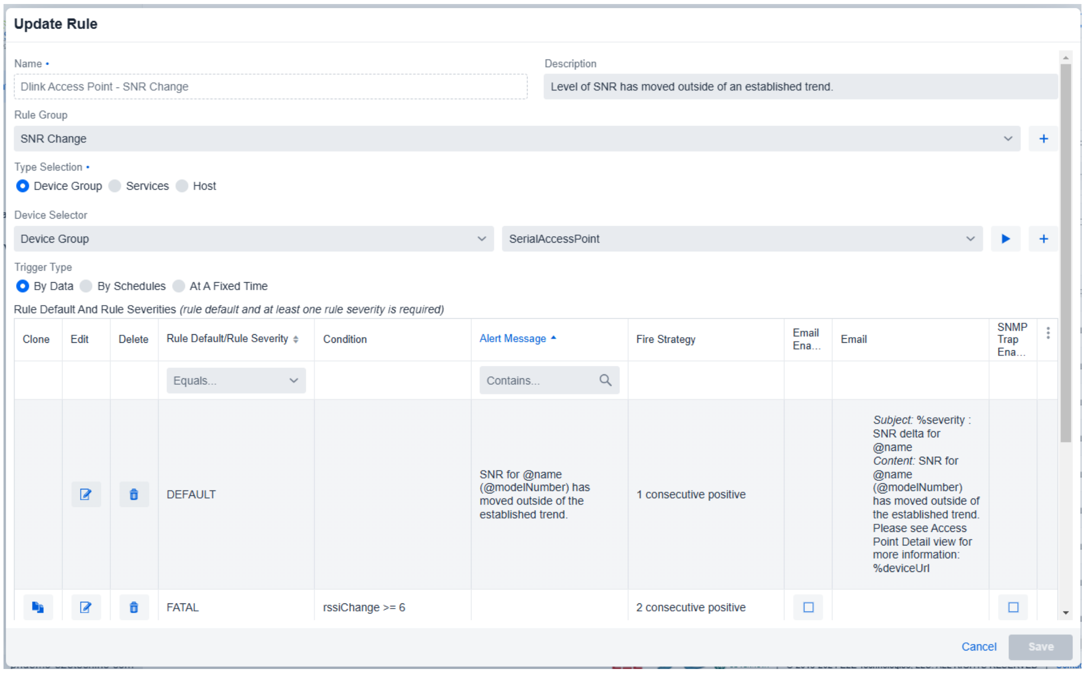
Enabling Email for Rules

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 editing a specific rule, as shown in the image above. Simply check the box to **Enable Email**.

Full Update for Rule Settings - Enterprise Only

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

Select the **Rule Group** to which this rule is assigned by choosing one from the dropdown menu. If the appropriate Rule Group is not found in the list, click the **Add** icon to add a new Rule Group to the list. Change the rule **Name** and **Description** if needed.



Update Rule

Name •
Dlink Access Point - SNR Change

Description
Level of SNR has moved outside of an established trend.

Rule Group
SNR Change

Type Selection •
● Device Group ○ Services ○ Host

Device Selector
Device Group
SerialAccessPoint

Trigger Type
● By Data ○ By Schedules ○ At A Fixed Time

Rule Default And Rule Severities *(rule default and at least one rule severity is required)*

Clone	Edit	Delete	Rule Default/Rule Severity	Condition	Alert Message	Fire Strategy	Email Ena...	Email	SNMP Trap Ena...
			Equals...		Contains...				
			DEFAULT		SNR for @name (@modelNumber) has moved outside of the established trend.	1 consecutive positive		*Subject:* %severity : SNR delta for @name *Content:* SNR for @name (@modelNumber) has moved outside of the established trend. Please see Access Point Detail view for more information: %deviceUrl	
			FATAL	rssiChange >= 6		2 consecutive positive	□		□

In the Device Selector section, 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.

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

In the **Rule Default and Rule Severities** table 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.

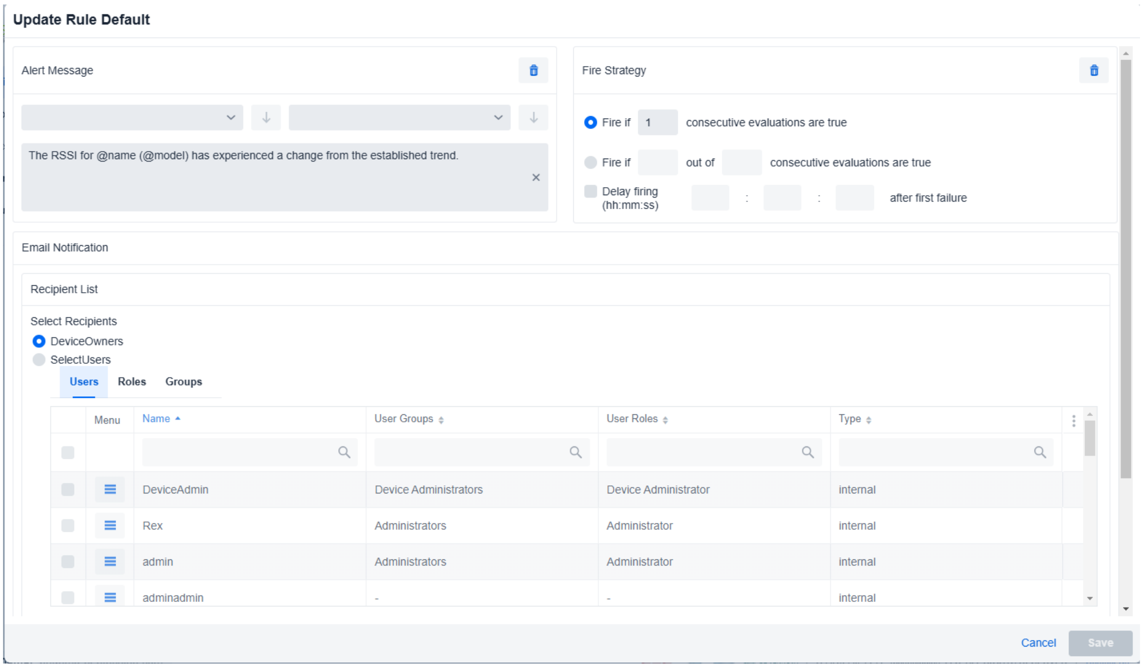
In the example below, the **Rule Default** contains the event message and fire strategy, as well as the subject and content for the email alerts. The Fatal, Critical, and Warning severities will inherit all of those defaults, but each of them will trigger the rule on a slightly different condition or 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 Alert Message section allows creation of alert messages 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.



Update Rule Default

Alert Message

The RSSI for @name (@model) has experienced a change from the established trend.

Fire Strategy

● Fire if 1 consecutive evaluations are true

○ Fire if out of consecutive evaluations are true

□ Delay firing (hh:mm:ss) : : after first failure

Email Notification

Recipient List

Select Recipients

● DeviceOwners

○ SelectUsers

Users Roles Groups

	Menu	Name	User Groups	User Roles	Type
□					
□	≡	DeviceAdmin	Device Administrators	Device Administrator	internal
□	≡	Rex	Administrators	Administrator	internal
□	≡	admin	Administrators	Administrator	internal
□	≡	adminadmin	-	-	internal

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)

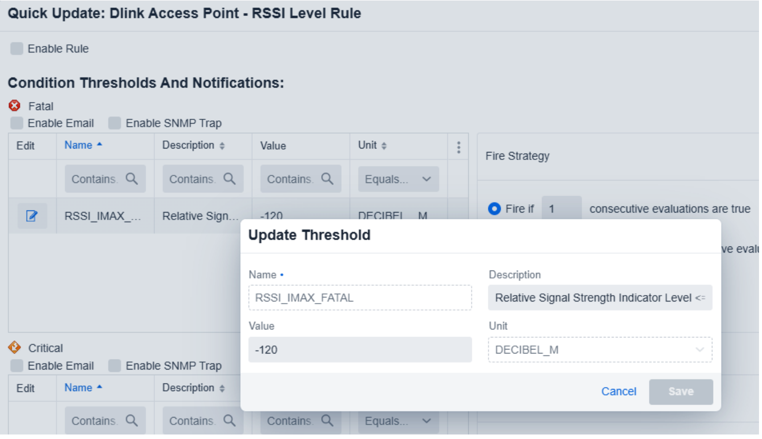
The Fire Strategy works the same as described above in the **Quick Update** section. It is also possible to Delay Firing of a rule by a custom time - if accounting for a known network delay, etc…

Alerts are sent to Device Group owners by default. Checking the **Select Users** option will allow selection of one or more users or user groups to send the alerts to instead.

In the Notification section, define the email recipient list, 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.



Quick Update: Dlink Access Point - RSSI Level Rule

□ Enable Rule

Condition Thresholds And Notifications:

Fatal

□ Enable Email □ Enable SNMP Trap

Edit	Name	Description	Value	Unit
	Contains	Contains	Contains	Equals...
	RSSI_IMAX_...	Relative Sign...	-120	DECIBEL_M

Fire Strategy

● Fire if 1 consecutive evaluations are true

Update Threshold

Name: RSSI_IMAX_FATAL

Description: Relative Signal Strength Indicator Level <=

Value: -120

Unit: DECIBEL_M

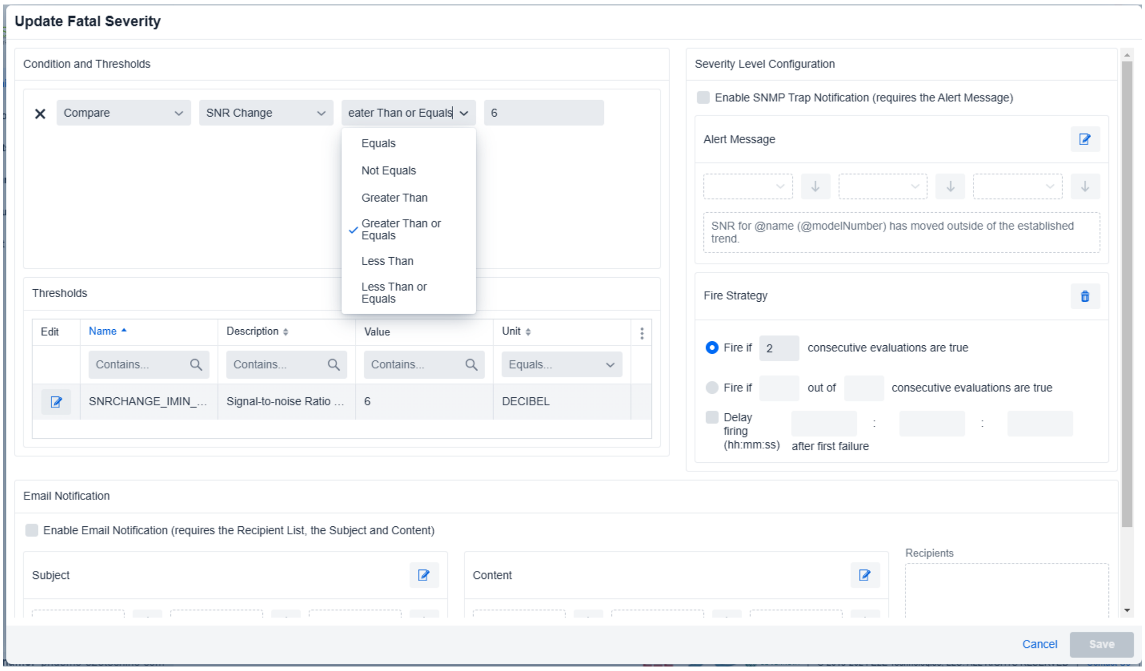
Cancel Save

Critical

□ Enable Email □ Enable SNMP Trap

Edit	Name	Description	Value	Unit
	Contains	Contains	Contains	Equals...

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



Update Fatal Severity

Condition and Thresholds

Compare | SNR Change | eater Than or Equals | 6

Thresholds

Edit	Name	Description	Value	Unit
	Contains...	Contains...	Contains...	Equals...
	SNRCHANGE_IMIN_...	Signal-to-noise Ratio ...	6	DECIBEL

Severity Level Configuration

□ Enable SNMP Trap Notification (requires the Alert Message)

Alert Message

SNR for @name (@modelNumber) has moved outside of the established trend.

Fire Strategy

● Fire if 2 consecutive evaluations are true

○ Fire if out of consecutive evaluations are true

□ Delay firing (hh:mm:ss) after first failure

Email Notification

□ Enable Email Notification (requires the Recipient List, the Subject and Content)

Subject

Content

Recipients

Cancel Save

Comparisons can include the following operators:

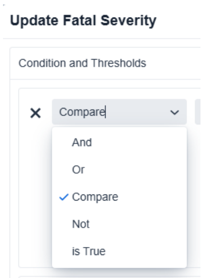
- **Equals:** The search string in the third field must exactly match the value of the chosen parameter. For example, if a device’s IP address EQUALS “10.0.0.54” it will be listed.

- **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 inclusion of devices which have *all* of the specific parameters and matching values that are included in the filter. For example, selecting devices whose IP address Starts With "10.10." AND whose "Firmware Version" Equals "3.0.3"

The OR operator allows inclusion of devices which have *any* of the specific parameters and matching values that are included in the filter. For example, selecting devices whose IP address Starts With "10.10." OR whose IP address Starts With "10.11."

The NOT operator allows exclusion of devices which have the specific parameters and matching values in the filter. For example, selecting devices whose IP address does NOT Start With “10.20.”


Update Fatal Severity

Condition and Thresholds

Once an operation (And/Or/Not/Compare) is chosen, specify a property that exists on the type of devices selected in the **Device Selector**. To see which properties are supported on the devices, click the **play** icon in the Device Selector section, which will display the list of devices that match the device filter or group. On that list, click any of the **Information** icons to see a detailed list of device properties. When defining the severity condition, choose any of the listed properties for the filter criteria.

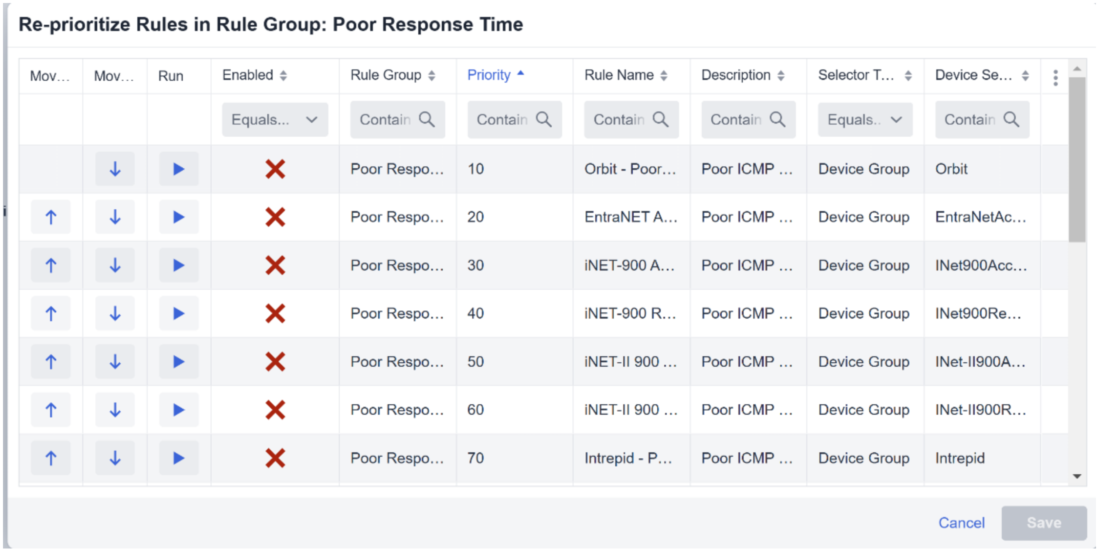
When editing the rule severity conditions and thresholds, it is also possible to edit other values inherited from the Rule Default (if desired).

Action Icons for Rules - Enterprise Only

For each rule in the **Rules Table** there is a set of Action icons used 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 **Menu** icon and select re-prioritize. Use the up/down arrow icons to adjust the order of rule evaluation. Click **Save** to save changes.



Re-prioritize Rules in Rule Group: Poor Response Time

Mov…	Mov…	Run	Enabled	Rule Group	Priority	Rule Name	Description	Selector T…	Device Se…
			Equals…	Contain	Contain	Contain	Contain	Equals..	Contain
	↓	▶	✗	Poor Respo…	10	Orbit - Poor…	Poor ICMP …	Device Group	Orbit
↑	↓	▶	✗	Poor Respo…	20	EntraNET A…	Poor ICMP …	Device Group	EntraNetAc…
↑	↓	▶	✗	Poor Respo…	30	iNET-900 A…	Poor ICMP …	Device Group	INet900Acc…
↑	↓	▶	✗	Poor Respo…	40	iNET-900 R…	Poor ICMP …	Device Group	INet900Re…
↑	↓	▶	✗	Poor Respo…	50	iNET-II 900 …	Poor ICMP …	Device Group	INet-II900A…
↑	↓	▶	✗	Poor Respo…	60	iNET-II 900 …	Poor ICMP …	Device Group	INet-II900R…
↑	↓	▶	✗	Poor Respo…	70	Intrepid - P…	Poor ICMP …	Device Group	Intrepid

Copy Rule Definitions

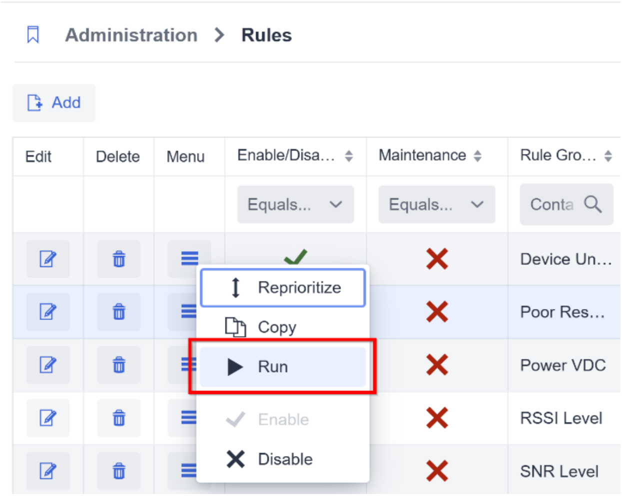
Existing rules can be copied and modified, which provides a shortcut for creating new rules that have similar features. To copy an existing rule, click the **Menu** icon on the row which lists the rule that will be duplicated and select **Copy**. Once the rule is copied, remember to give the new rule 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 that will be modified. It may require a **Quick Edit** or a **Full Update**, as described in the previous sections. Click **Save** to save any changes made to the rule.

Show Device Selector List

To view the list of devices on which an individual rule will operate, click **Run** under the **Menu** icon. A popup window will appear containing the full list of existing devices to which the rule applies.



Edit	Delete	Menu	Enable/Disa…	Maintenance	Rule Gro…
			Equals...	Equals...	Conta
			✓	✗	Device Un…
				✗	Poor Res…
				✗	Power VDC
				✗	RSSI Level
				✗	SNR Level

Service Rules

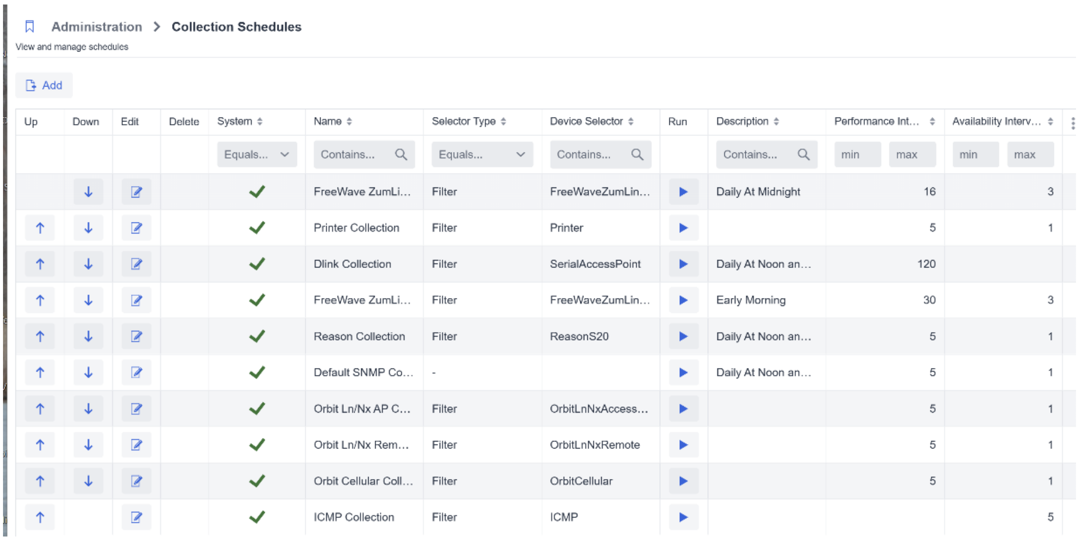
The **Select Services** box is used if the rule in question is NOT associated with a Device Group. For example, DB Health and JVM Monitoring. Checking this box will allow selection of a Service (rather than devices) to which the rule will apply.

COLLECTION SCHEDULES

PulseNET Standard includes only the default collection schedules for Dlink and SNMP.

Scheduling Device Data Collection - Enterprise Only

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, 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.



Administration > Collection Schedules
View and manage schedules
Add

Up	Down	Edit	Delete	System	Name	Selector Type	Device Selector	Run	Description	Performance Int...	Availability Interv...
				Equals...	Contains...	Equals...	Contains...		Contains...	min max	min max
	↓	✎		✓	FreeWave ZumLi...	Filter	FreeWaveZumLin...	▶	Daily At Midnight	16	3
↑	↓	✎		✓	Printer Collection	Filter	Printer	▶		5	1
↑	↓	✎		✓	Dlink Collection	Filter	SerialAccessPoint	▶	Daily At Noon an...	120	
↑	↓	✎		✓	FreeWave ZumLi...	Filter	FreeWaveZumLin...	▶	Early Morning	30	3
↑	↓	✎		✓	Reason Collection	Filter	ReasonS20	▶	Daily At Noon an...	5	1
↑	↓	✎		✓	Default SNMP Co...	-		▶	Daily At Noon an...	5	1
↑	↓	✎		✓	Orbit Ln/Nx AP C...	Filter	OrbitLnNxAccess...	▶		5	1
↑	↓	✎		✓	Orbit Ln/Nx Rem...	Filter	OrbitLnNxRemote	▶		5	1
↑	↓	✎		✓	Orbit Cellular Coll...	Filter	OrbitCellular	▶		5	1
↑		✎		✓	ICMP Collection	Filter	ICMP	▶			5

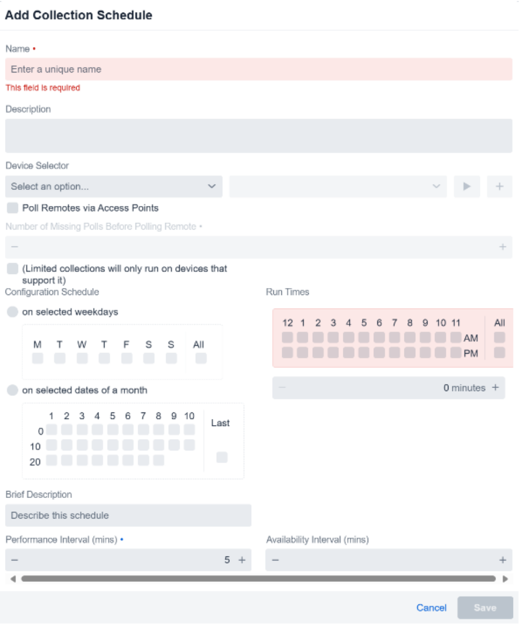
Configure a Data Collection Schedule

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. Click the **Add** button to create a new collection schedule.

On the **Add** or **Update Collection Schedule** display, 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. 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 **play** icon. If an existing device filter or group that meets the need is not found, click the **Add** icon to add a new device filter or group.
3. The **Poll Remotes via Access Points** checkbox can be used to include any downstream Orbit remotes in the scheduled action. [Orbit devices only.]
4. In the **Number of Missed Polls Before Polling Remote** field, enter the number of times the schedule will poll the Master device(s) for the remote data before it will send the request to the remote directly. [Orbit devices only.]
5. Select the **Limited Collection** checkbox if the scheduled action will only poll limited registers from the device. This is useful for high-traffic networks, and is explained in greater detail below.
6. Choose whether GE PulseNET will collect device configuration information on selected days of the week or on 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 GE PulseNET will use for configuration collection.
7. In the **Run Times** box, select one or more times of day (hours) that GE PulseNET will use for configuration collections. Or enter a specific time during each hour that GE PulseNET will use when it collects configuration data from each device.
8. Update the description text for this configuration collection as needed.
9. Enter a new value (minutes) in the field.
10. Click **Save** to apply the settings to the collection schedule.



Add Collection Schedule

Name •
Enter a unique name
This field is required

Description

Device Selector
Select an option...

□ Poll Remotes via Access Points

Number of Missing Polls Before Polling Remote •

□ (Limited collections will only run on devices that support it)

Configuration Schedule

○ on selected weekdays

○ on selected dates of a month

Run Times

0 minutes

Brief Description
Describe this schedule

Performance Interval (mins) •
5

Availability Interval (mins)

Explanation of Limited SNMP Collection (Orbit Only):
Currently, Orbit is the only device that supports limited SNMP polling. AP collection is ONLY what can be collected from the AP and does not communicate with the remote. Limited polling applies to both scheduled collections and on-demand (triggers) collections.
Note: Special collection schedules have been put in place for Orbit LN/NX devices which limit the collection to serial protocol, or one device at a time. On an LN AP, ten remotes will be polled one at a time before moving on.

Explanation of Metric Data Averaging:

PulseNET rolls-up the raw data to averages over time to reduce the amount of data stored. Here's our default policy:

- Every 15 minutes we roll the raw data up to 15-minute intervals, and store these 15-minute intervals for 3 days.
- After 3 days, we roll the 15-minute intervals up to hourly intervals and store hour intervals for 14 days.
- After 14 days, we roll hourly data up to daily intervals and store daily data for one year.

As an example, if data has been graphed for one month (e.g. 30 days)

- for days 30-14: display data points for daily averages
- for days 14-3: display data points for hourly averages
- for days 1-3, display data points for 15 minute averages
- for the last 15 minutes, display raw data

The goal is to provide a simple and consistent way of aggregating all metrics, so that the data will be interpreted in the same way for all.

To calculate custom values, however, the option remains to export the data to a spreadsheet and calculate any averages required.

Keep in mind, the percentage shown will always be the last value in the time range. Modify the time range as needed.

Due to the aggregating process, it is possible for unexpected percentage values to appear. Let's use **Availability** as an example:

A 66% or 75% Available value can happen when 3-4 "15 minute" values (e.g. 100, 0, 100, 100) are rolled up to an "hour" value (75).

The average availability is calculated when values are rolled up to create a new data point (15, hour, day, etc). They are not averaged across the entire time range, and are not averaged based on the polling intervals.

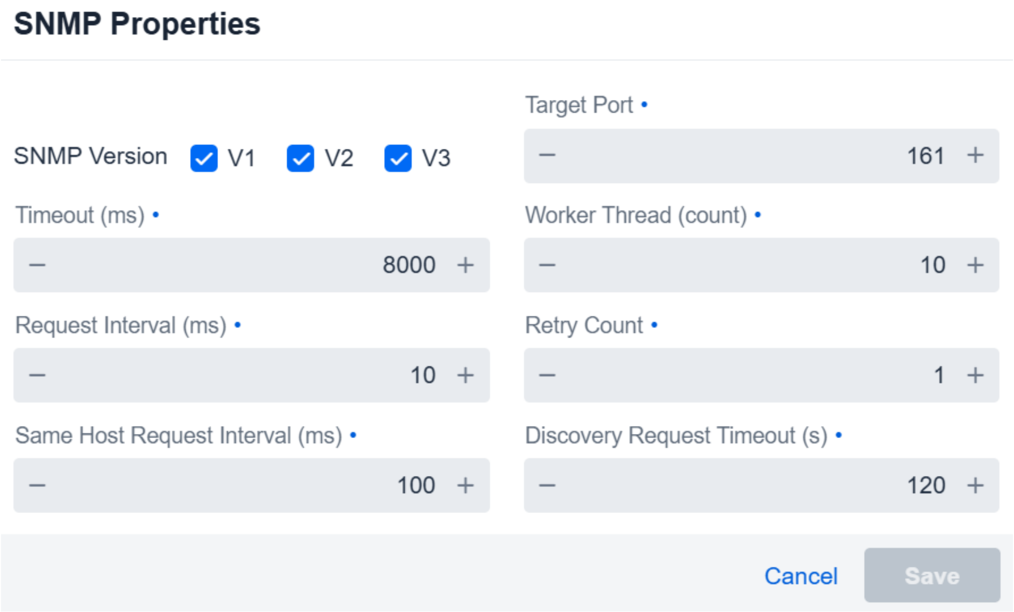
MONITORING CONFIGURATION

The Monitoring Configuration dashboard allows configuration of GE PulseNET settings for several network protocols used 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**.



SNMP Properties

SNMP Version ☑ V1 ☑ V2 ☑ V3

Target Port • 161

Timeout (ms) • 8000

Worker Thread (count) • 10

Request Interval (ms) • 10

Retry Count • 1

Same Host Request Interval (ms) • 100

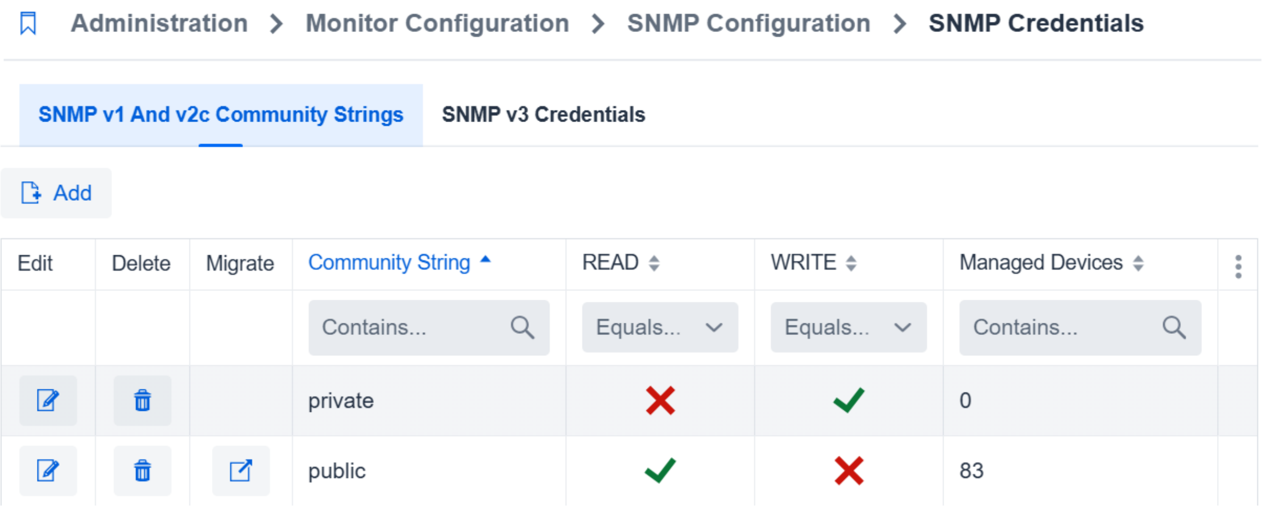
Discovery Request Timeout (s) • 120

The SNMP Properties display allows configuration of 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. Here 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.



Administration > Monitor Configuration > SNMP Configuration > **SNMP Credentials**

SNMP v1 And v2c Community Strings | **SNMP v3 Credentials**

Add

Edit	Delete	Migrate	Community String ▲	READ ⇕	WRITE ⇕	Managed Devices ⇕
			Contains...	Equals...	Equals...	Contains...
✎	🗑		private	✗	✓	0
✎	🗑	↗	public	✓	✗	83

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

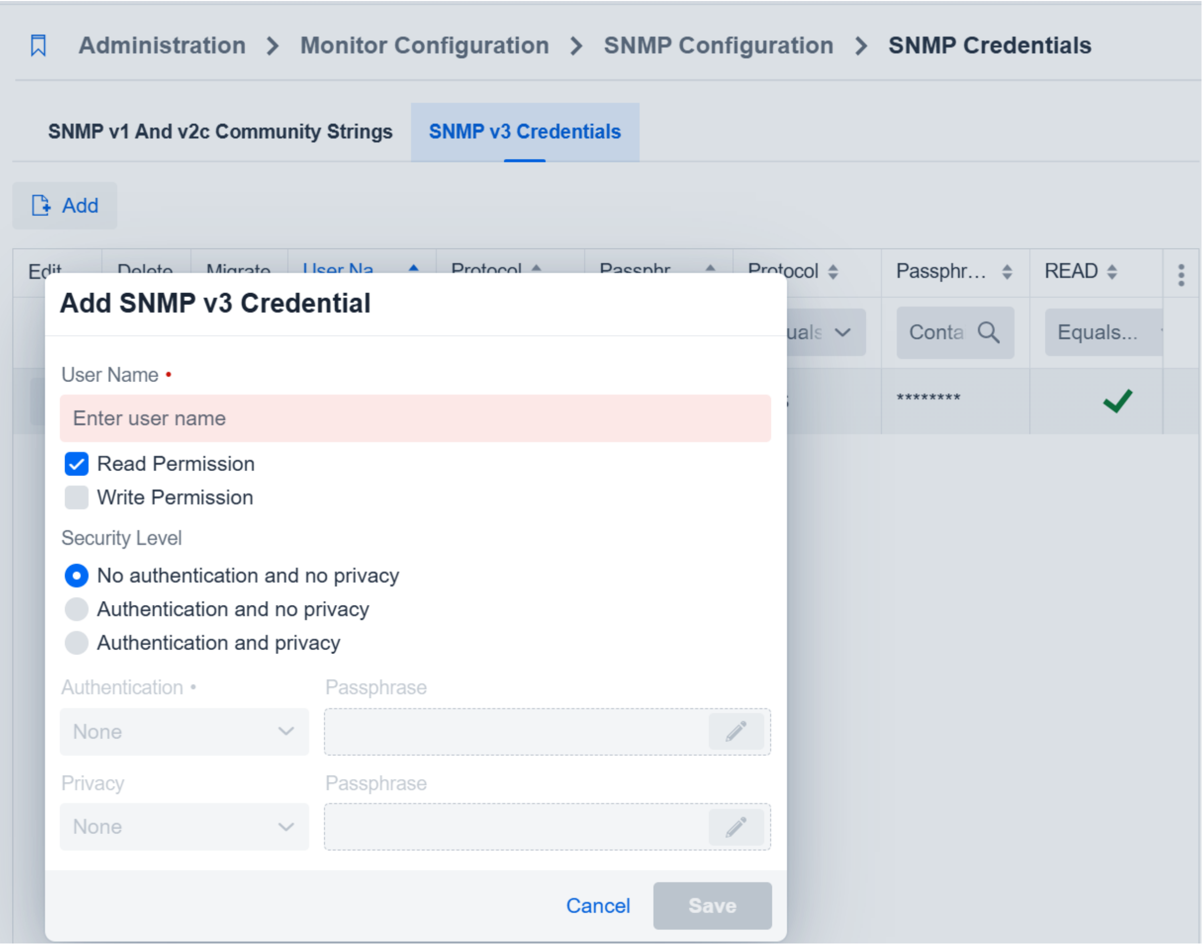
- Click the **Edit** icon on the row displaying the credential that will be edited.
- Change the values as desired, and click **Save** to save the changes.

Delete an SNMP Community String

- Click the **Edit** icon on the row displaying the credential that will be deleted.
- Click the **Delete** button to confirm deletion of 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



Administration > Monitor Configuration > SNMP Configuration > SNMP Credentials

SNMP v1 And v2c Community Strings | SNMP v3 Credentials

Add

Add SNMP v3 Credential

User Name •

Enter user name

☑ Read Permission
□ Write Permission

Security Level

● No authentication and no privacy
○ Authentication and no privacy
○ Authentication and privacy

Authentication • None | Passphrase

Privacy None | Passphrase

Cancel | Save

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, 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 selected **Security Level** requires authentication, specify the authentication protocol and passphrase (i.e., the password for the specified user name).
9. If the selected **Security Level** requires privacy, specify a privacy protocol and passphrase. The passphrase is the encryption key.
10. Click **Save**.

Edit SNMP v3 Credentials

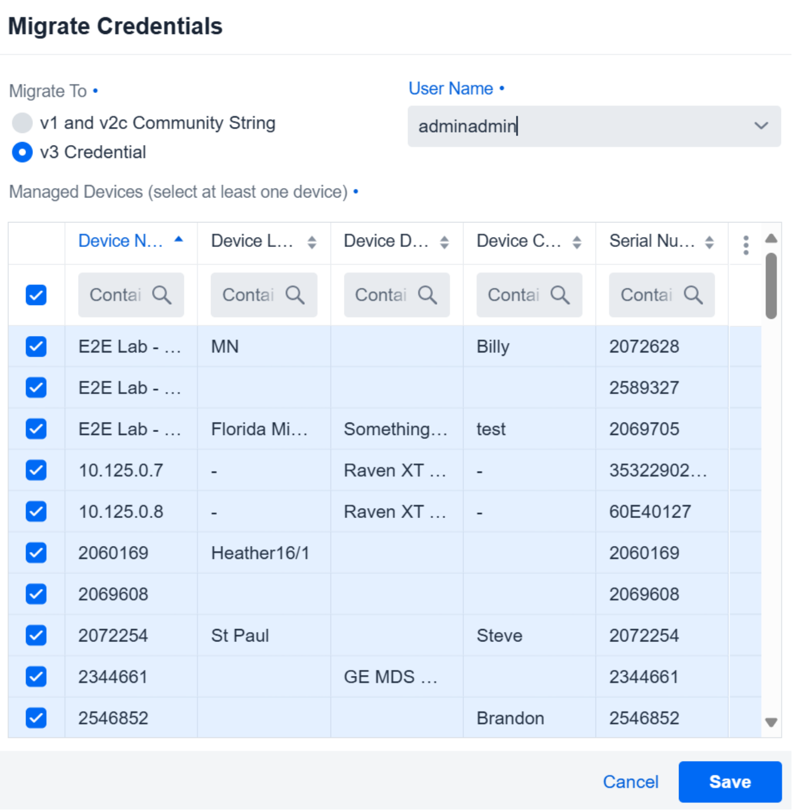
- In the SNMP v3 Credentials table, click the Edit icon for the SNMP v3 credential that will be edited.
- Edit the settings for the credential as desired.
- Click **Save**.

Delete SNMP v3 Credentials

- Click the **Delete** icon on the row displaying the credential that will be deleted.
- Click the **Delete** button to confirm deletion of 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** and beside of the SNMP community string there is a migrate column click on the community string in which needs to be migrated



Migrate Credentials

Migrate To •
○ v1 and v2c Community String
● v3 Credential

User Name •
adminadmin

Managed Devices (select at least one device) •

☑	Device N... ▲	Device L...	Device D...	Device C...	Serial Nu...
☑	Contai	Contai	Contai	Contai	Contai
☑	E2E Lab - ...	MN		Billy	2072628
☑	E2E Lab - ...				2589327
☑	E2E Lab - ...	Florida Mi...	Something...	test	2069705
☑	10.125.0.7	-	Raven XT ...	-	35322902...
☑	10.125.0.8	-	Raven XT ...	-	60E40127
☑	2060169	Heather16/1			2060169
☑	2069608				2069608
☑	2072254	St Paul		Steve	2072254
☑	2344661		GE MDS ...		2344661
☑	2546852			Brandon	2546852

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

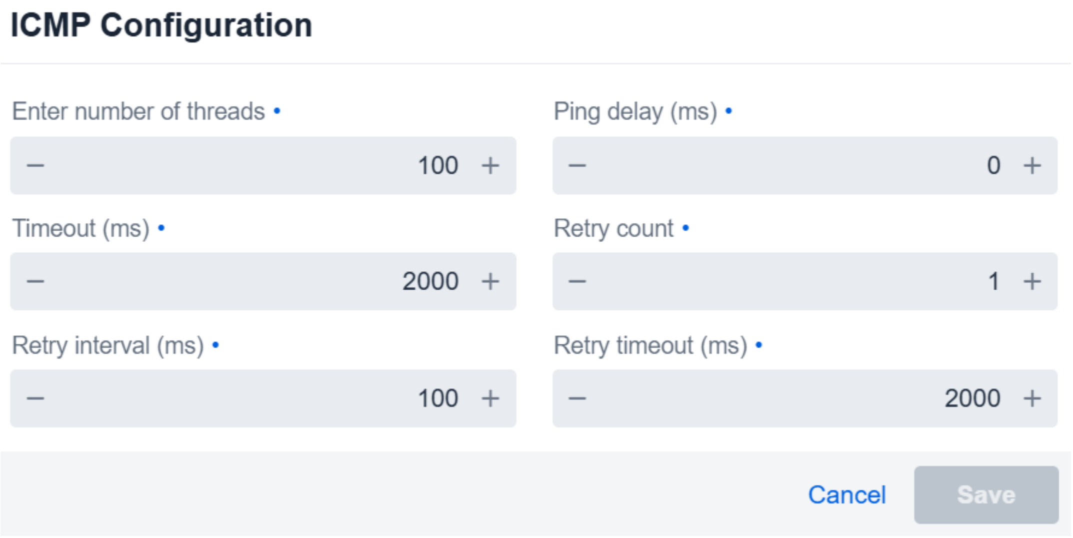
- Find the community string or credential from which devices will be migrated; and click the migrate icon in the migrate column.
- In the **Migrate Credential Wizard**, choose the type of SNMP credential to which the selected devices will be migrated (v1/v2c or v3), then select the SNMP credential that will be used to communicate with these devices in the future.
- Check the specific devices that will be migrated 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.



ICMP Configuration

Enter number of threads • 100

Ping delay (ms) • 0

Timeout (ms) • 2000

Retry count • 1

Retry interval (ms) • 100

Retry timeout (ms) • 2000

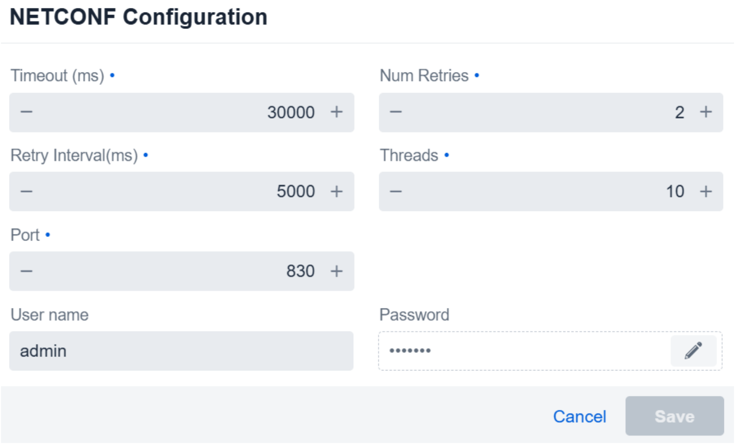
- **Number of threads** sets the number of simultaneous parallel ICMP queries that GE PulseNET will be capable of generating.
- **Ping Delay** sets the amount of time between successive ICMP requests.
- **Timeout** sets the amount of time that GE PulseNET will wait before marking a device as unreachable 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 - Enterprise Only

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.



NETCONF Configuration

Timeout (ms) • 30000

Num Retries • 2

Retry Interval(ms) • 5000

Threads • 10

Port • 830

User name admin

Password •••••••

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

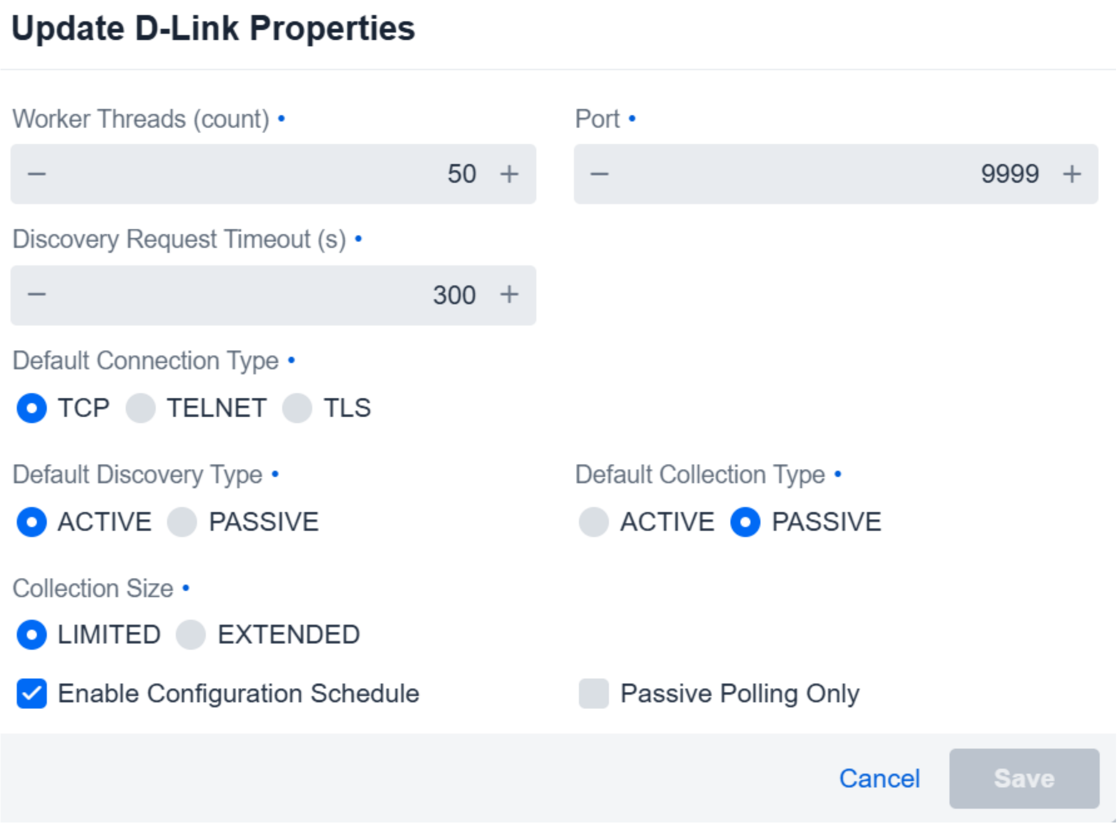
Configuring DLINK Properties

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.



Update D-Link Properties

Worker Threads (count) • 50

Port • 9999

Discovery Request Timeout (s) • 300

Default Connection Type • ● TCP ○ TELNET ○ TLS

Default Discovery Type • ● ACTIVE ○ PASSIVE

Default Collection Type • ○ ACTIVE ● PASSIVE

Collection Size • ● LIMITED ○ EXTENDED

☑ Enable Configuration Schedule

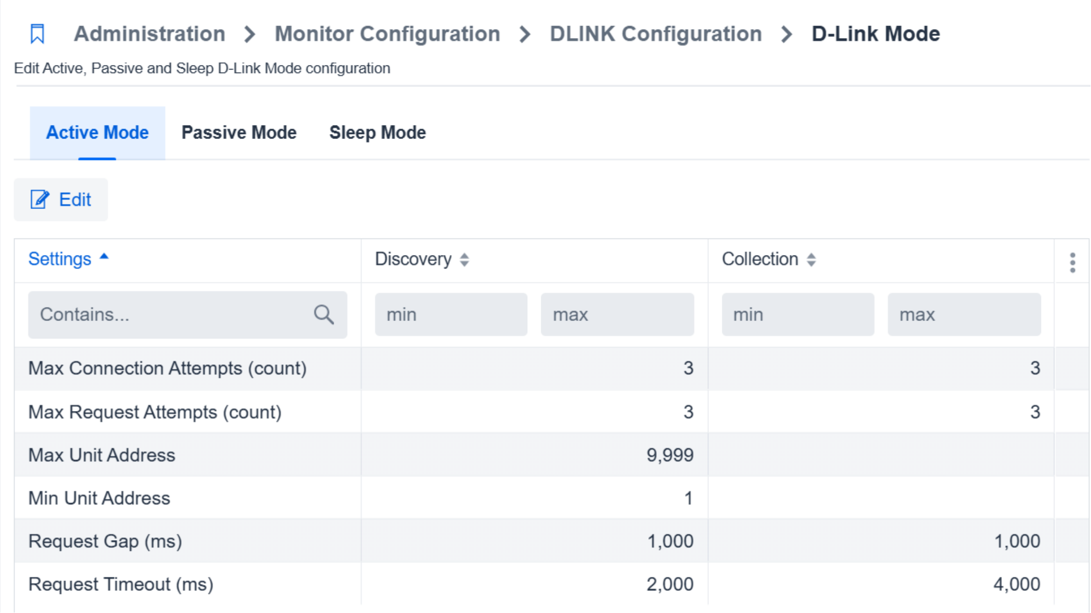
□ Passive Polling Only

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 increasing 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.


Administration > Monitor Configuration > DLINK Configuration > D-Link Mode
Edit Active, Passive and Sleep D-Link Mode configuration
Active Mode
Passive Mode
Sleep Mode
Edit

Settings	Discovery		Collection	
Contains...	min	max	min	max
Max Connection Attempts (count)	3		3	
Max Request Attempts (count)	3		3	
Max Unit Address	9,999			
Min Unit Address	1			
Request Gap (ms)	1,000		1,000	
Request Timeout (ms)	2,000		4,000	

Active Mode Properties

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

- **Request Timeout** sets the time GE PulseNET waits for a response to an active DLINK request.
- **Request Gap** sets the length of time GE PulseNET waits between making active requests for data.
- **Max Attempts** sets the maximum number of DLINK retries before timing out.
- **Max Connection Attempts** sets the maximum number of connection attempts before timing out.
- **Min Unit Address** sets the lowest diagnostic unit ID of a range of IDs to be queried.
- **Max Unit Address** sets the highest diagnostic unit ID of a range of IDs to be queried.

Sleep Mode Properties

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

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

Passive Mode Properties

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

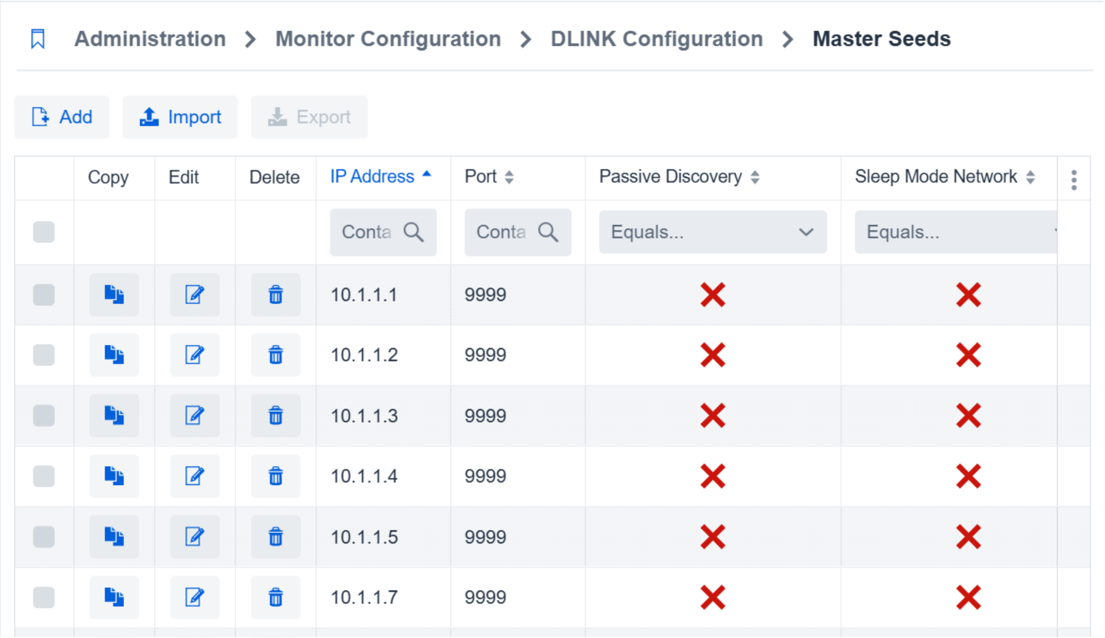
- **Request Timeout** sets the time GE PulseNET waits for a response to an passive DLINK request.
- **Response Gap** sets the minimum time between collecting one metric and querying for the next metric.
- **Repeats** sets the maximum number of DLINK retries.
- **Repeat Interval** sets the time GE PulseNET 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

A Master Seed can be set up for any DLINK master device, and is used to perform initial discovery, as well as subsequent discovery of associated remotes. IP and Port settings must be defined so that GE PulseNET knows how to send DLINK protocol queries to the diagnostic interface on the Master device. This process is similar to the IP Range discovery menu just below, but allows for the parameters of the discovery to be set ahead of time, so that it will not follow the DLINK global defaults. In addition, the Master Seed list can be exported/imported to another GE PulseNET instance, allowing easy rediscovery of the network if needed.

Note: The default Port and Unit ID for SD devices at 9999 is shown in examples, but the Port may vary, and unit ID range can cover up to 65000.

In order to monitor DLINK devices via a master seed, 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.


Administration > Monitor Configuration > DLINK Configuration > Master Seeds
Add
Import
Export

	Copy	Edit	Delete	IP Address ▲	Port ⇕	Passive Discovery ⇕	Sleep Mode Network ⇕
□				Conta	Conta	Equals...	Equals...
□	⧉	✎	🗑	10.1.1.1	9999	✗	✗
□	⧉	✎	🗑	10.1.1.2	9999	✗	✗
□	⧉	✎	🗑	10.1.1.3	9999	✗	✗
□	⧉	✎	🗑	10.1.1.4	9999	✗	✗
□	⧉	✎	🗑	10.1.1.5	9999	✗	✗
□	⧉	✎	🗑	10.1.1.7	9999	✗	✗

Add a DLINK Master Seed

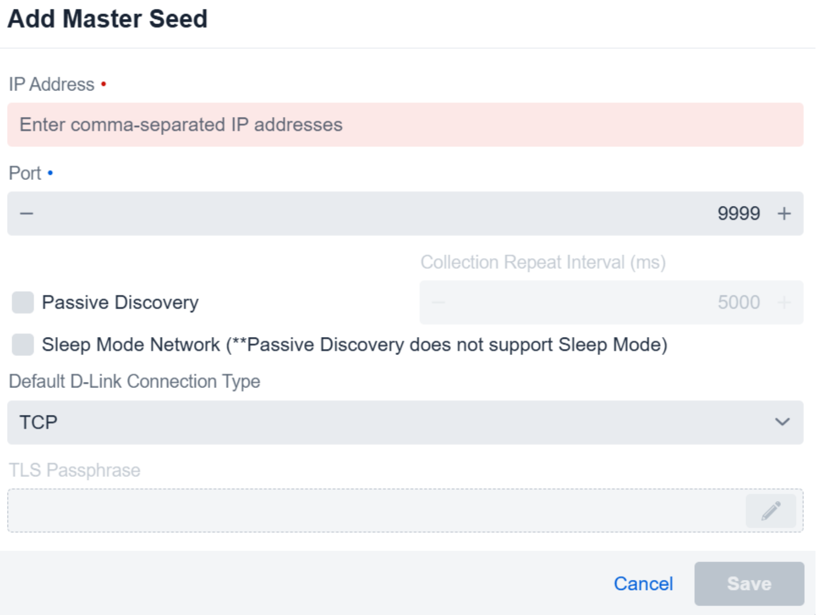
- Enter one or more IP addresses which have common settings.
- Enter the port on the terminal server which connects to the diagnostic interface on the Master.
- If passive discovery will be the default method, leave the **Passive Discovery**

checkbox selected. Clear the checkbox if Active discovery will 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 the network. For more information about passive and active discovery, see **Device Discovery**.

- In the **Collection Repeat Interval** field, enter the default value to be used 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.



Add Master Seed

IP Address •

Enter comma-separated IP addresses

Port •

– 9999 +

Collection Repeat Interval (ms)

□ Passive Discovery – 5000 +

□ Sleep Mode Network (**Passive Discovery does not support Sleep Mode)

Default D-Link Connection Type

TCP

TLS Passphrase

Copying a Master Seed Setting

In the **Master Seeds** table, click the **Copy** icon on the row which will be copied. 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 will be edited. 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 will be removed. Click **Yes** to confirm deletion.

Planning Data Collection on DLINK Networks

There are a number of factors that should be considered when planning data collections for monitored DLINK networks. The physical arrangement of the devices in the environment and their relationships to each other must be understood. 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. 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 the 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 data collection is being configured using the frequency technique, a larger request gap may be needed.

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 using 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 the 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 the network. Timeouts that are too short results in incomplete data collection and the devices may be marked as unavailable. If using 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 the application polling frequency.
- **Forgive Missed Polls** — The value of this parameter determines how quickly a device is marked as unavailable. If a device misses the specified number of consecutive data collection requests, it is considered unavailable.

Sleep Mode Networks

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

Passive collection can be used if the sleep mode network is awake at regular intervals, for example if devices are scheduled to be awake for 10 seconds and then sleep for 20 seconds. If using 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 application polling and the schedule for GE PulseNET data collection. Also, consider how the power is consumed for monitoring the devices. Ensure that enough power is 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 report as unavailable. If the parameter value is too long, it may be consuming more power than necessary when monitoring data.

MANAGING DEVICE FILTERS - Enterprise Only

The Filters dashboard allows for management of 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 view, copy, edit, or delete filters, or add new filter definitions.

View Device List for a Filter

Click the **play** icon in the **Actions** section of the row for the filter that will be examined. A popup list will show the devices captured by this filter. Click the **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 that will be copied. 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 **Information** icon to the right of the filter **Name** on the row for the filter that will be examined.

Edit a Custom Filter Definition

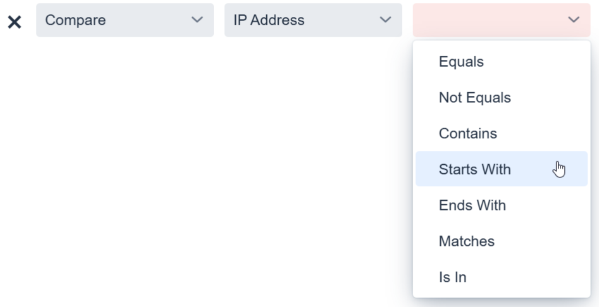
If using a custom filter definition, edit its settings by clicking the **Edit** icon on the row for the filter that will be edited. **Note:** Predefined filters delivered with GE PulseNET cannot be edited.

Delete a Custom Filter Definition

If using a custom filter definition, delete it by clicking the **Delete** icon on the row for the filter that will be removed. **Note:** 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 selection devices that have a specific parameter that matches a chosen value. For example, comparing 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.
- **Not Equals:** The comparison will return a match if the parameter’s value contains anything except the literal search string.
- **Contains:** The comparison will return a match if the search string is contained anywhere within the parameter’s value.
- **Starts With:** The comparison will return a match if the parameter’s value begins with the literal search string.
- **Ends With:** The comparison will return a match if the parameter’s value ends with the literal search string.
- **Matches:** Allows the use of regular expression wildcards to form the search string. **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.

The **AND** operator allows inclusion of devices which have *all* of the specific parameters and matching values that are included in the filter.
The **OR** operator allows inclusion of devices which have *any* of the specific parameters and matching values that are included in the filter.

The **NOT** operator allows exclusion of devices which have the specific parameters and matching values in the filter.
At any time while defining the filter, click the **Run Query** button to see the list of devices that match the settings. When satisfied that the filter definition is correct, click **Run Query** to view the list of devices that match the filter. In the device table at the bottom of the display, refine the device list even further by deselecting any matching devices that will not be included. This gives the Administrator complete control of the final device list that will become part of this filter.

The final filter can be saved in two different ways. If the filter will contain *all* the devices that matched the search criteria, click **Create From Query**. If the filter will contain *only* the devices selected from the device list at the bottom of the display, click **Create From Selected Devices**. Either of these options will result in a new filter that is displayed in the **Manage Filters** table.

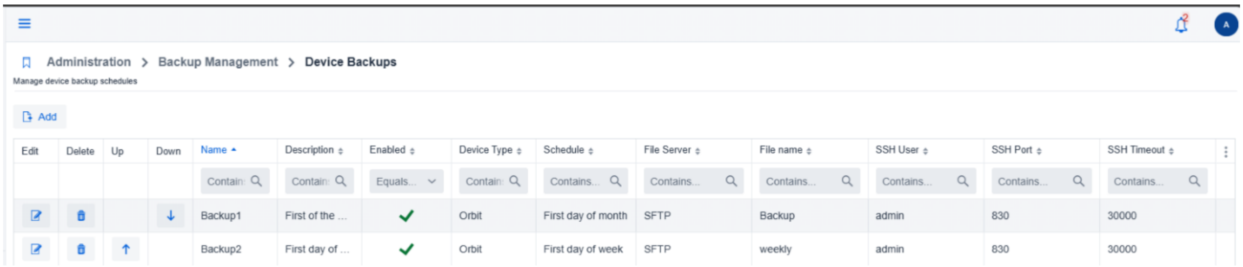
Backup Management - Enterprise Only

GE MDS strongly recommends that configuration backup files be created 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 GEMDS Orbit and GE Reason S20 devices.

The Backup Management dashboard becomes available exclusively for Orbit devices once valid GEMDS PulseNET Enterprise licenses are applied to the system. Additionally, when managing GE Reason devices, a GE Reason license is required. This dashboard enables Administrators to initiate and schedule regular configuration backups for supported GEMDS Orbit and GE Reason S20 devices.

To manage device backup settings, navigate to **Administration > Backup Management**. Click on Backup Schedules. From the Device Backup table view, copy, edit, or delete device backups, as well as schedule new backup configurations.

If an error occurs during a scheduled device configuration backup, an alert will be sent. To manage the alerts, see the **Working with Rules** section.



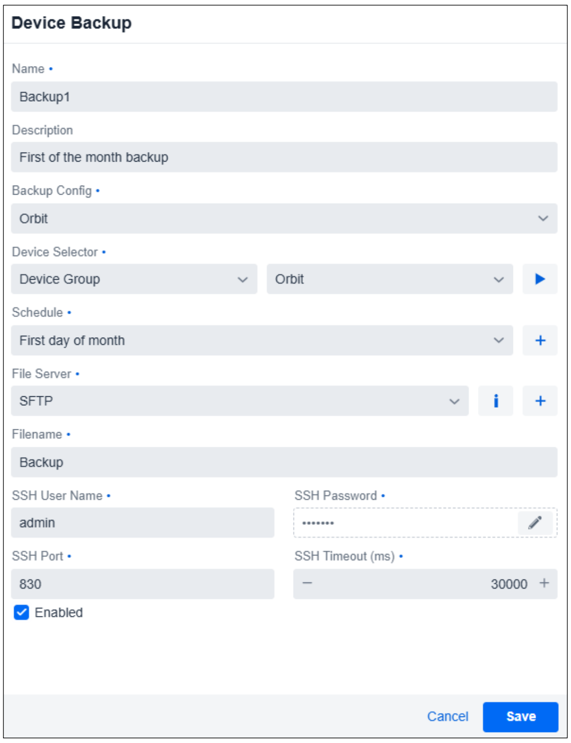
Administration > Backup Management > Device Backups

Manage device backup schedules

Edit	Delete	Up	Down	Name	Description	Enabled	Device Type	Schedule	File Server	File name	SSH User	SSH Port	SSH Timeout
				Contain:	Contain:	Equals...	Contain:	Contains...	Contains...	Contains...	Contains...	Contains...	Contains...
			↓	Backup1	First of the ...	✓	Orbit	First day of month	SFTP	Backup	admin	830	30000
		↑		Backup2	First day of ...	✓	Orbit	First day of week	SFTP	weekly	admin	830	30000

Add a Device Configuration Backup

To schedule a new backup, click the **Add** button from Administration > Backup Management > Device Backups



Device Backup

Name •
Backup1

Description
First of the month backup

Backup Config •
Orbit

Device Selector •
Device Group | Orbit

Schedule •
First day of month

File Server •
SFTP

Filename •
Backup

SSH User Name •
admin

SSH Password •
•••••••

SSH Port •
830

SSH Timeout (ms) •
30000

☑ Enabled

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. Use the **Backup Config** drop-down menu to select the model of device either Orbit or GE Reason.
3. Next, use the device Selector to select a device group from the drop-down menu. Click the play icon to view a list of the devices that will be included in the device group.
4. Select the frequency of the Device Backup configuration from the **Schedule** drop-down menu.
5. In the **File Server** drop-down menu, select where the device should send its backup configuration. *NOTE: The current GE Reason MIB does not support the / character.*

6. In the **File name** field, type the name of the file that will be used to save the configuration.
7. The **Device Credentials** will vary depending on the type of backup config. Orbit will use SSH over NETCONF (830) and the GE Reason device will use the SNMP Credentials from the SNMP Properties.
8. Click the **Enable** checkbox to run the configuration.
9. Click **Save** to create the new Device Configuration Backup.

⚠ **NOTE:** The SFTP site where the Device Configuration Backups are stored may need to be manually cleaned up from time to time.

Backup Configuration Read Scheduling

The GE Reason S20 and the GEMDS Orbit both have a backup feature that provides the ability to capture the configuration and setting of the device for archiving.

To utilize the configuration backup feature it is important to understand that it is designed to operate on a recurring schedule. That is, the backup task will operate every 15 minutes or once a month – but always in a recurring operation. A one time backup is not currently supported.

Note: Schedules that have a recurrence pattern of “Once” are not supported for device backups – even though it is in the drop-down selection.

When creating backup tasks, the order they appear in the “Device Backup” table indicates the priority of tasks with tasks “above” the others being a higher priority. Devices should ONLY appear in one backup task. If a device is in a higher priority backup task is duplicated, then the lower priority task will not run – even if there are other devices along with the duplicated device.

MANAGING DEVICE GROUPS - Enterprise Only

The Device Groups dashboard allows for management of 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 view, edit, or delete existing device groups, or add 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 play icon in the **Actions** section of the row for the group that will be examined. A popup list will show the devices included in this group. Click the **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 that will be edited. See **Adding Device Groups** for an explanation of the components that can be edited in a device group.

Delete Device Group

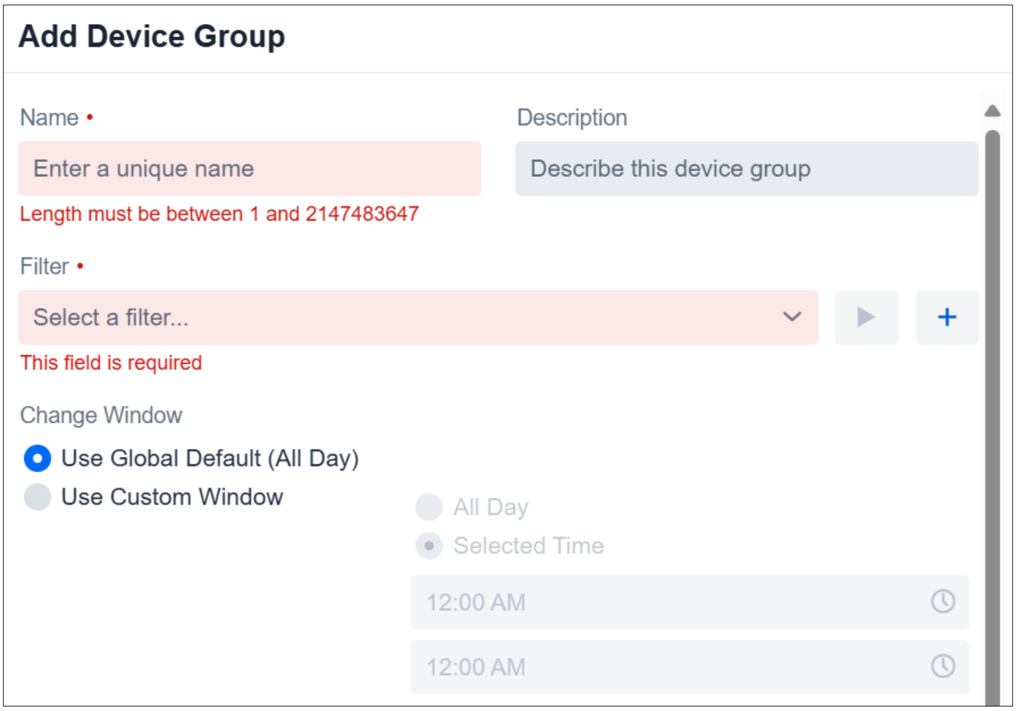
Click the **Delete** icon on the row for the group that will be removed. Click **Yes** to confirm the deletion, or **Cancel** to cancel this action.

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 **Add** icon to add a new filter. See the **Managing Device Filters** section for more information. Once a filter is selected, click the play icon to view a list of the devices that will be included in this device group.

Next select the **Change Window**, which is the period of time during which changes will be allowed on this group of devices. The global default change window setting can be used, or a custom time range can be defined. Finally, select the GE PulseNET users who are the owners for any change requests on this group of devices. Click **Save** to save the new device group.



Add Device Group

Name •
Enter a unique name
Length must be between 1 and 2147483647

Description
Describe this device group

Filter •
Select a filter...
This field is required

Change Window
● Use Global Default (All Day)
○ Use Custom Window
○ All Day
● Selected Time
12:00 AM
12:00 AM

Batch Device Management

Device Maintenance Management

This menu provides the option to enable or disable Maintenance Mode for multiple devices at once. Select required devices, then click the "Enter Maintenance" or "Exit Maintenance" button as needed.

Device Staging & Production Management

This menu provides the option to Move devices into Staging and/or Production mode as a bulk action. Select required devices, then click the "Move Devices to Staging" or "Move Devices to Production" button as needed.

Device Decommission Management

This menu provides the option to Decommission multiple devices simultaneously as a batch action. Select the required devices and click "Decommission" to remove them from monitoring.

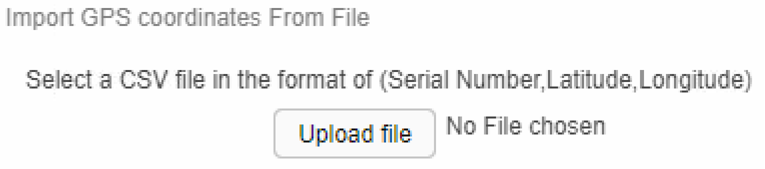
Note: The devices will still be holding the original license they were discovered under and will appear under the **Administration - Licensing - Manage License** menu. Click into the monitoring license and the decommissioned devices will be listed here under the **Decommissioned** column. From this menu it is also possible to **Delete** the device, which will free up the license. That specific device serial number will not be authorizable again in the future.

GPS Coordinate Import

This option will update the GPS Coordinates of multiple devices. It requires the Serial Number, Latitude and Longitude placed in a .csv or .txt file, similar to the below example:

```
2560646,51.499390,-0.127465
3588862,34.101803,-118.341507
2320301,43.397503,40.359585
```

Once the formatting is correct, save the .csv or .txt file, and upload the file via the IMS UI with the Upload file button.



Import GPS coordinates From File

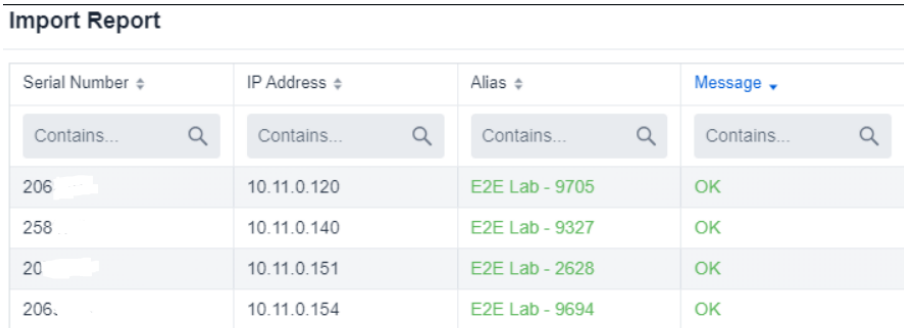
Select a CSV file in the format of (Serial Number,Latitude,Longitude)

Device Alias Import

This option will update the Alias name of multiple devices as a batch action. It requires the “Serial Number, Alias” to be placed in a .csv or .txt file, like the below example:

```
2560646, Site ABC
3588862, Site DEF
2320301, Site GHI
```

Once the file has been uploaded, click Import to proceed with the action – an Import Report will display the changed items, and the Message column will denote any unreachable devices that failed to update.



Import Report

Serial Number ⇕	IP Address ⇕	Alias ⇕	Message ▾
Contains...	Contains...	Contains...	Contains...
206[redacted]	10.11.0.120	E2E Lab - 9705	OK
258[redacted]	10.11.0.140	E2E Lab - 9327	OK
20[redacted]	10.11.0.151	E2E Lab - 2628	OK
206[redacted]	10.11.0.154	E2E Lab - 9694	OK

CHANGE MANAGEMENT - Enterprise Only

GE PulseNET includes a change management feature which automates specified configuration changes on individual devices or on bulk groups of devices. 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. (Note: some devices may require a special license).

GE MDS Orbit: (Cell Firmware Change, Certificate Firmware Change, Device Firmware Change, Password Change, Device Restart(s), SSH Configuration Change, Configuration Change)
GE MDS SD: (Device Firmware Change, Passphrase Change, Configuration Change)
GE MDS iNET: (Device Firmware Change, Configuration Change)
GE MDS Mercury: (Device Firmware Change, Configuration Change)
GE Reason S20/S24: (Device Firmware Change, Push Configuration Change, Configuration Change)*****
4RF AprisaSR+ (Firmware Change, Configuration Change)
Freewave ZumLink: (Configuration Change)

*****Requires GE Reason License

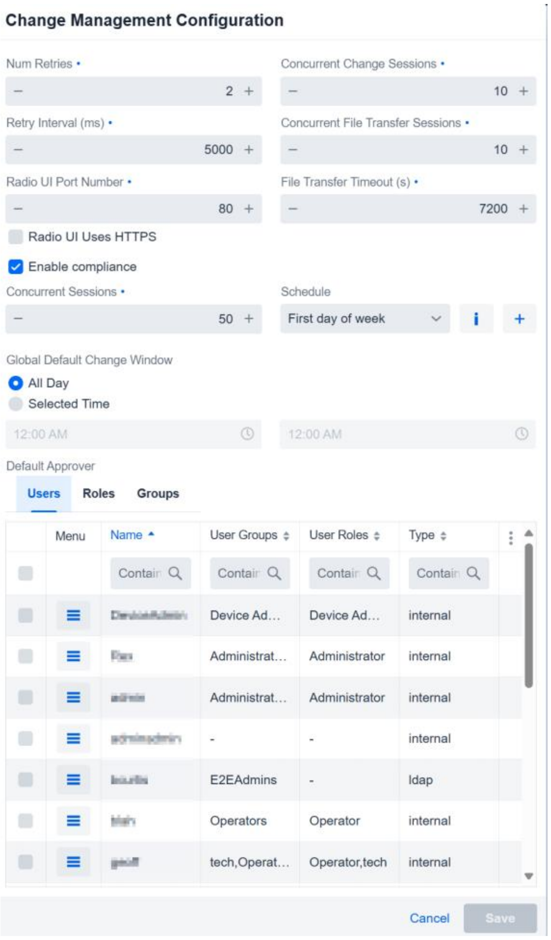
GE PulseNET allows an Administrator to specify the exact change to be made, the specific set of devices on which the change must be made, the time window during which the change will be allowed, and escalation for change approval to the users who are device owners. GE PulseNET uses the SNMP or NETCONF protocol to communicate securely with the remote radios.

The processes described below work in conjunction to create the final change request, and some initial configuration is required. For example, to create a Cell Modem Firmware Upgrade request, the following steps are required:

1. Upload the Cell Modem Firmware to an external SFTP server.
2. Configure PulseNET to point to that SFTP server under **System Configuration > File Servers.**
3. Create a Firmware Change **Template** in PulseNET for the Orbit Device (It will ask if device or cellular firmware.)
4. Then create the Change **Request** as described below.

Configuring Change Management - Enterprise Only

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.



Change Management Configuration

Num Retries •: 2
Concurrent Change Sessions •: 10
Retry Interval (ms) •: 5000
Concurrent File Transfer Sessions •: 10
Radio UI Port Number •: 80
File Transfer Timeout (s) •: 7200

☐ Radio UI Uses HTTPS
☑ Enable compliance

Concurrent Sessions •: 50
Schedule: First day of week

Global Default Change Window
● All Day
○ Selected Time

12:00 AM 12:00 AM

Default Approver

	Menu	Name	User Groups	User Roles	Type
☐		Contain	Contain	Contain	Contain
☐	≡	[redacted]	Device Ad...	Device Ad...	internal
☐	≡	[redacted]	Administrat...	Administrator	internal
☐	≡	[redacted]	Administrat...	Administrator	internal
☐	≡	[redacted]	-	-	internal
☐	≡	[redacted]	E2EAdmins	-	ldap
☐	≡	[redacted]	Operators	Operator	internal
☐	≡	[redacted]	tech,Operat...	Operator,tech	internal

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.

Click **Save** to save these parameters.

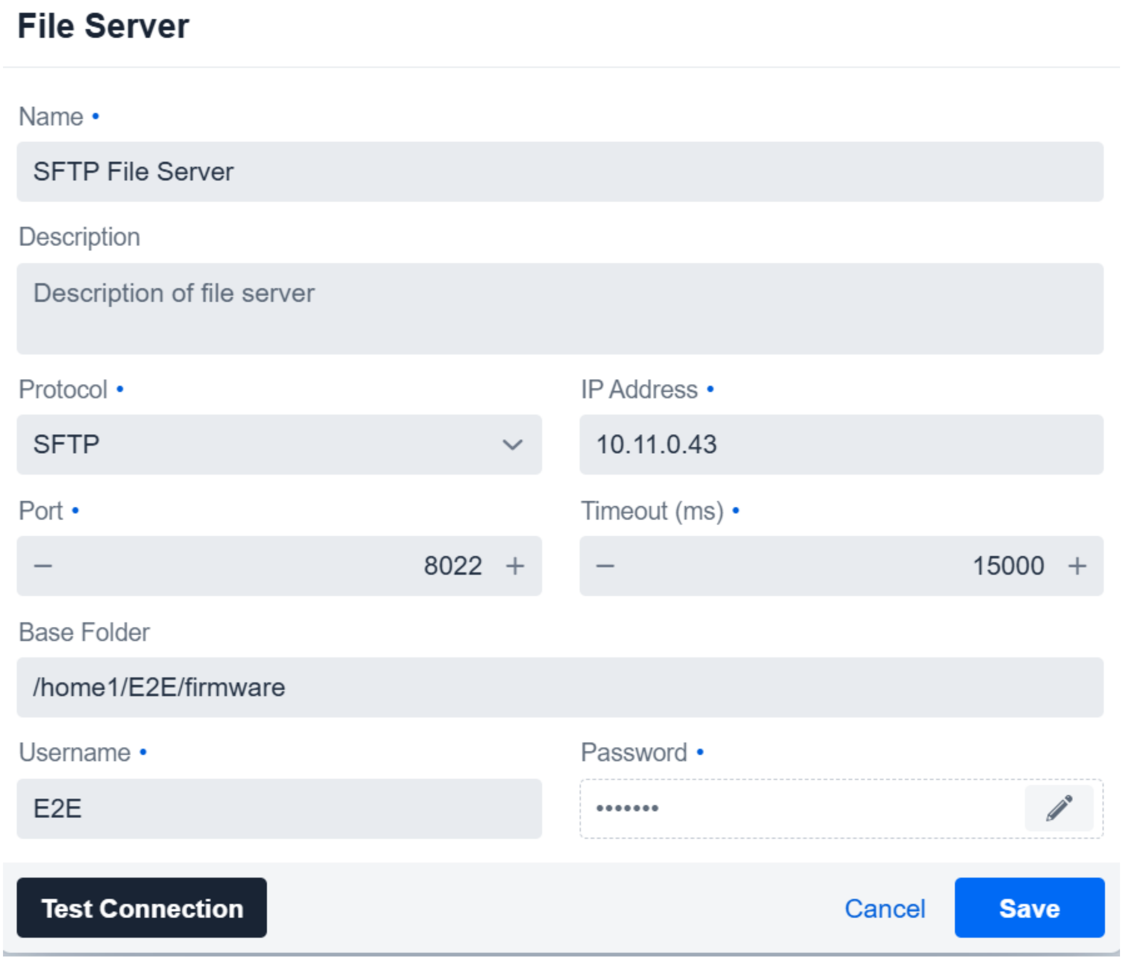
Managing Firmware Servers - Enterprise Only

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. Select a Firmware Server which supports SFTP or TFTP and contains the firmware images.

File Servers must be added via **Administration > System Configuration > File Servers**



File Server

Name •
SFTP File Server

Description
Description of file server

Protocol •
SFTP

IP Address •
10.11.0.43

Port •
8022

Timeout (ms) •
15000

Base Folder
/home1/E2E/firmware

Username •
E2E

Password •
•••••••

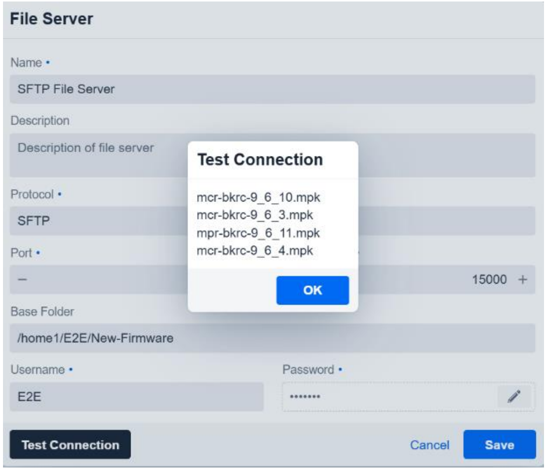
To add, enter a unique name to identify the firmware server, as well as a description of the services provided. This is a good place to describe the server's location or the reason why some devices may need to retrieve their firmware images from this file repository.

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.
- **Base 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.



File Server

Name • SFTP File Server

Description: Description of file server

Protocol • SFTP

Port • 15000

Base Folder: /home1/E2E/New-Firmware

Username • E2E

Password • •••••••

Test Connection

mcr-bkrc-9_6_10.mpk
mcr-bkrc-9_6_3.mpk
mpr-bkrc-9_6_11.mpk
mcr-bkrc-9_6_4.mpk

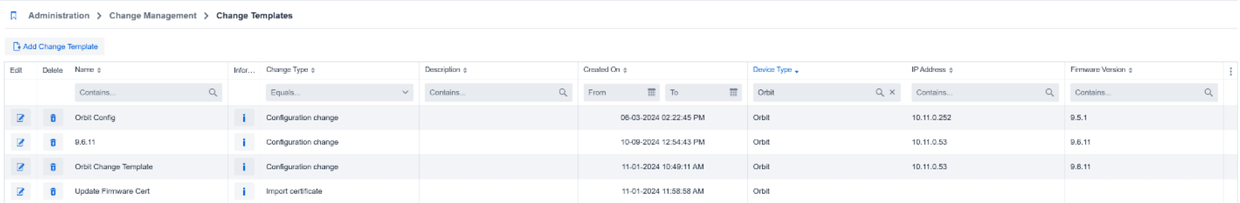
Once the Firmware Server connection settings have been entered, test the connection by clicking the **Test Connection** button. A new dialog box that contains the list of firmware images (SFTP only) will appear in the designated folder on this specific file server. If unsuccessful, an error message will indicate why the connection failed. **Note:** The SFTP/TFTP server must use the root path. Sub-folders cannot be used.

Managing Change Templates - Enterprise Only

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.



Administration > Change Management > Change Templates

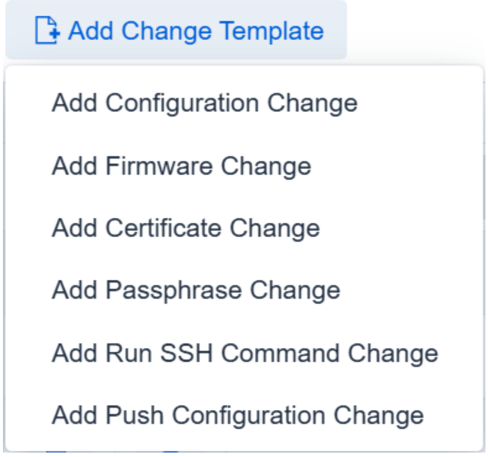
Add Change Template

Edit	Delete	Name	Infor...	Change Type	Description	Created On		Device Type	IP Address	Firmware Version
		Contains...		Equals...	Contains...	From	To	Orbit	Contains...	Contains...
✎	🗑	Orbit Config	i	Configuration change		06-03-2024 02:22:45 PM		Orbit	10.11.0.252	9.5.1
✎	🗑	9.6.11	i	Configuration change		10-09-2024 12:54:43 PM		Orbit	10.11.0.53	9.6.11
✎	🗑	Orbit Change Template	i	Configuration change		11-01-2024 10:49:11 AM		Orbit	10.11.0.53	9.6.11
✎	🗑	Update Firmware Cert	i	Import certificate		11-01-2024 11:58:58 AM		Orbit		

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 an **Information** icon that will display a brief summary of any change requests which are using the change template. The Change Type column shows the type of change that will be performed (Configuration, Password, or Firmware). The **Device Type** column lists the type of device that will be targeted by the change. Configuration change templates require the Administrator 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.

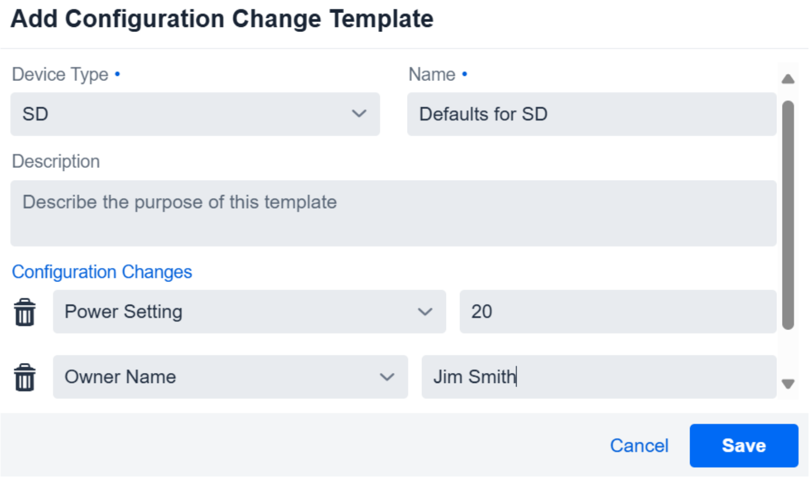
Add a Configuration Change Template

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 the device user manual. Click the **Add** icon to add additional properties. Click the **Save** button.



Add Configuration Change Template

Device Type • SD

Name • Defaults for SD

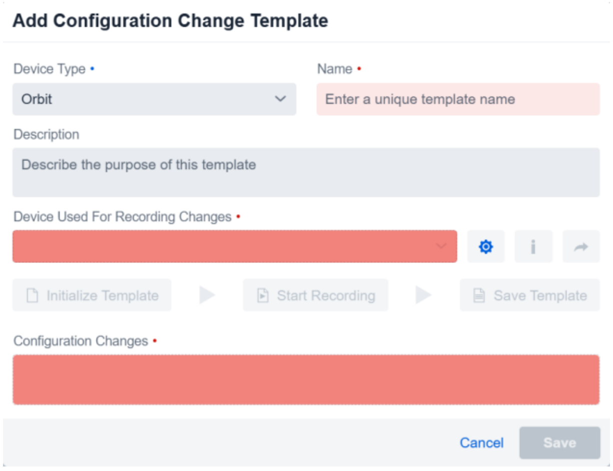
Description: Describe the purpose of this template

Configuration Changes

Power Setting: 20

Owner Name: Jim Smith

For Orbit devices, enter a unique template **Name** and **Description** of the template. It is usually best practice to include the reason for this change in the description field. Next select a device that will be used for recording the changes to be made on similar device models. Any device can be selected, but a device with a known good configuration should be used as the basis for changes to be made on other devices in the network.



Add Configuration Change Template

Device Type • Orbit

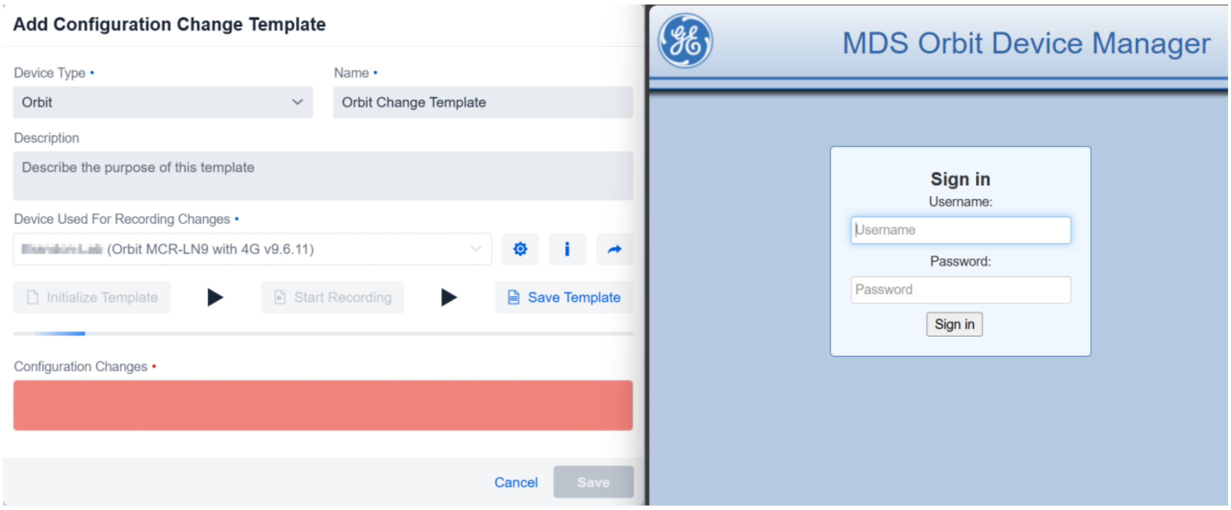
Name • Enter a unique template name

Description: Describe the purpose of this template

Device Used For Recording Changes •

Under Device used for Recording Changes click the **Device Selector** gear icon to view the devices that can be used for recording.

After clicking the **Initialize Template** button, GE PulseNET opens a communication channel to the recording device and makes a snapshot of that device’s configuration settings. The first gray arrow will then become, indicating that it is ready to proceed to the next button in the row.



Add Configuration Change Template

Device Type • Orbit

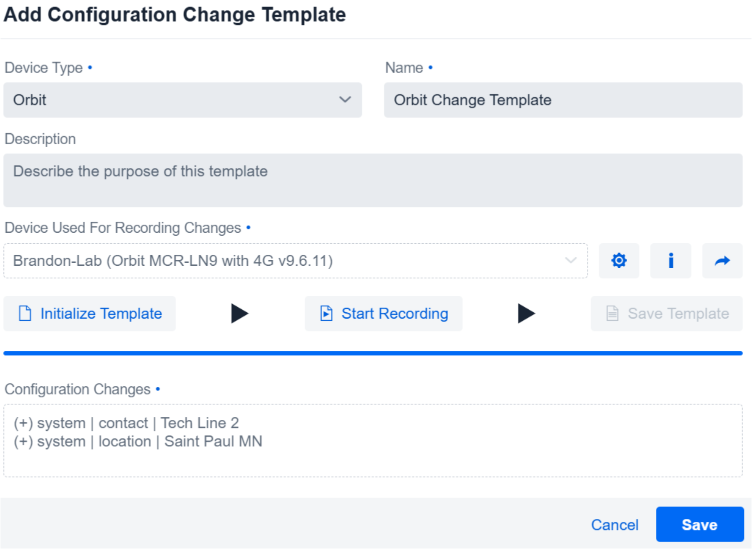
Name • Orbit Change Template

Description: Describe the purpose of this template

Device Used For Recording Changes • [redacted] (Orbit MCR-LN9 with 4G v9.6.11)

Configuration Changes •

Clicking **Start Recording** will open the web interface and establish an interactive login session to the recording device. During the interactive session with the recording device, make any desired changes to the configuration and then commit or save those changes on the device itself. The second gray arrow in GE PulseNET will then become, indicating that it is ready to proceed to the final step.



Add Configuration Change Template

Device Type • Orbit

Name • Orbit Change Template

Description: Describe the purpose of this template

Device Used For Recording Changes • Brandon-Lab (Orbit MCR-LN9 with 4G v9.6.11)

Configuration Changes •

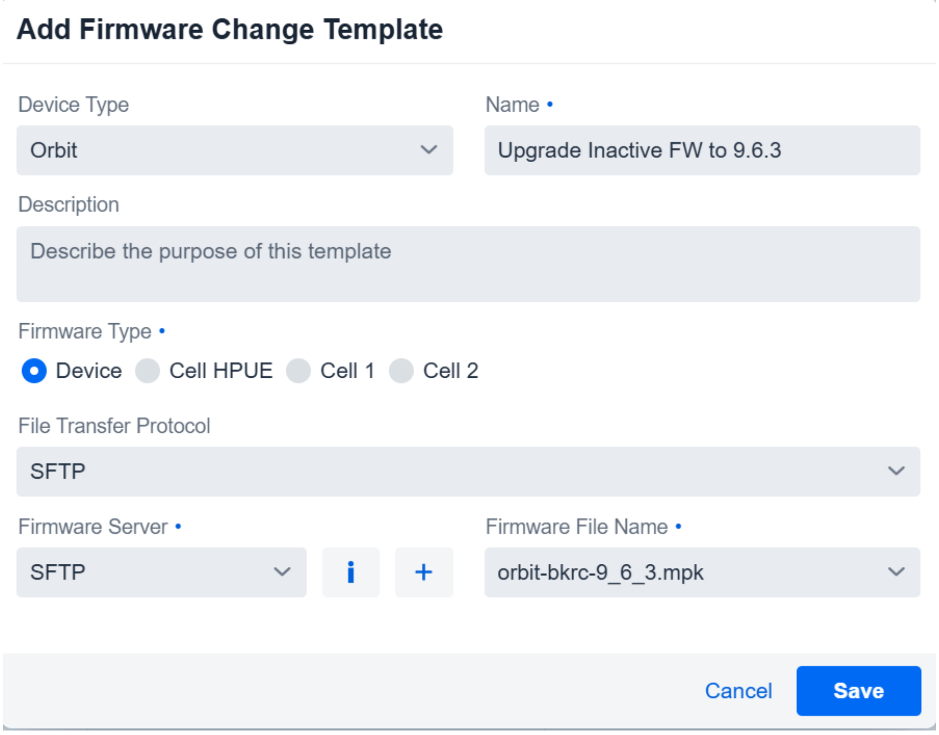
```
(+) system | contact | Tech Line 2
(+) system | location | Saint Paul MN
```

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 will be included in the template.

Click the **Save** button at the bottom of the screen in order to save the completed template.

Add a Firmware Change Template

A firmware push is supported for iNET, Mercury, Orbit, SD Master Station dlink remote devices, 4RF Aprisa SR+, and GE Reason devices. After choosing to add a firmware change template, select a device type. Enter a unique template name and a description of the changes that will be included in the template. Next, select the firmware type Device, Cell HPUE, Cell 1 or Cell 2. Then select a File Transfer Protocol and a **Firmware Server** from which the device will retrieve its image. If an appropriate firmware server is not shown in the dropdown list, click the **Add** icon to add another firmware server. See the **Manage Firmware Servers** section for more information. Note: this view and the File Transfer Protocols will change based on the Device Type.



Add Firmware Change Template

Device Type: Orbit

Name •: Upgrade Inactive FW to 9.6.3

Description: Describe the purpose of this template

Firmware Type •: ● Device ○ Cell HPUE ○ Cell 1 ○ Cell 2

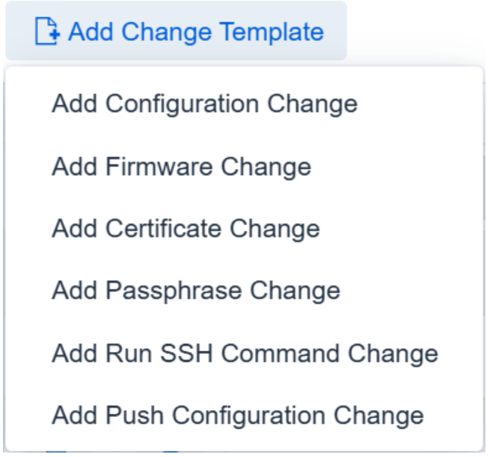
File Transfer Protocol: SFTP

Firmware Server •: SFTP

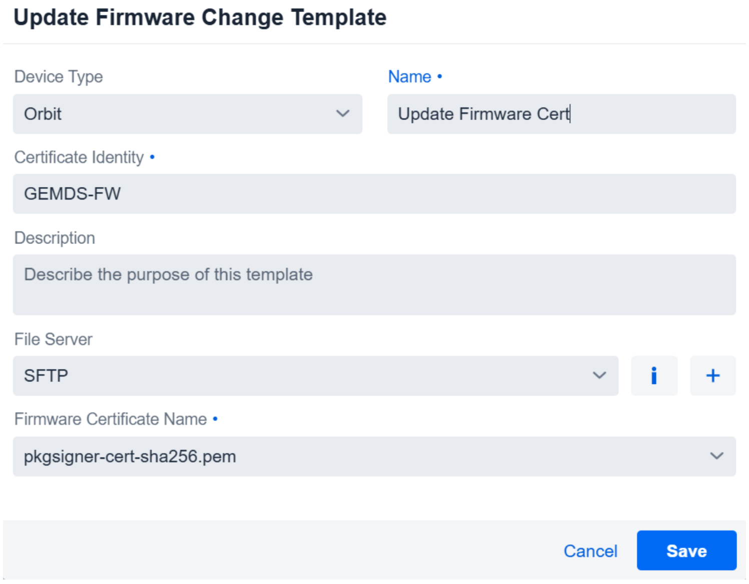
Firmware File Name •: orbit-bkrc-9_6_3.mpk

Once the firmware server is selected, click the **Information** icon to see the connection settings for that server. Next, select or input the exact name of a Firmware File that will be uploaded to the devices. The dropdown list of firmware files only contains images that are currently available on a selected SFTP server. Click **Save to** save the 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, click the **Add** icon to add another firmware server. See the **Manage Firmware Servers** section for more information.



Update Firmware Change Template

Device Type	Orbit
Name •	Update Firmware Cert
Certificate Identity •	GEMDS-FW
Description	Describe the purpose of this template
File Server	SFTP
Firmware Certificate Name •	pkgsigner-cert-sha256.pem

Once the firmware server is selected, click the **Information** icon to see the connection settings for that server. Next, select or input the exact name of the Firmware Certificate that will be uploaded Click **Save** to save the completed Certificate Import Change Template.

Add Passphrase Change

Applies only to SD Access Points. This allows the DLINK passphrase and Data passphrase to be updated from the AP. The call will be sent to the AP, which in turn tells the remotes to update their passphrases.

Add SSH Command Change

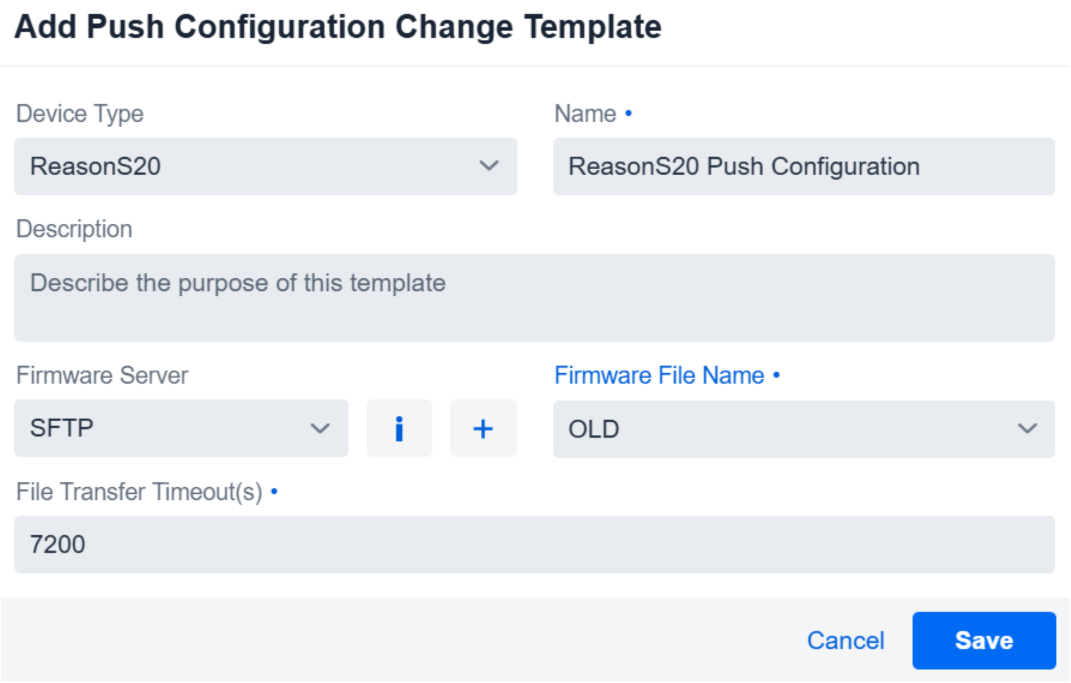
Users can use the "Add SSH Command Change" to apply the following types of changes via SSH.

- INET
  - Enable SNMP v2c
  - Change Password
- Orbit
  - Change Admin, Tech, and Oper passwords
  - Generate One Time Password
  - Set current time and date
  - Enable SNMP v2c
  - Set Engine ID from MAC
  - Set Engine ID from MAC as Text
- SD
  - Change Password To change password on SD devices - use telnet port 23.
- Mercury
  - Change Guest Password
  - Change Admin Password
  - Enable SNMP v2c
- 4RF Aprisa SR+
  - Add New User
  - Set Admin Password
  - Set SNMP Read/Write Community
  - Delete User
- Sierra Wireless
  - Change Password
- Ubiquiti
  - Change Password
- Cambium
  - Change Password
- Freewave
  - Enable SNMP v2c
  - Change Password To change password on Freewave - under SSH Change Management use Port 80

Add Push Configuration Change - REASON Only

This feature will allow for selection of a ReasonS20 backup file from a TFTP/SFTP server - this template will then be used in a Push Configuration Change Request targeting specific ReasonS20 devices to which this backup configuration will be deployed.

See section on File Servers for more information.



Add Push Configuration Change Template

Device Type: ReasonS20

Name •: ReasonS20 Push Configuration

Description: Describe the purpose of this template

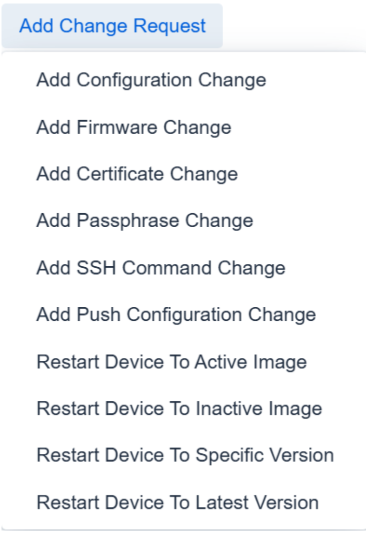
Firmware Server: SFTP

Firmware File Name •: OLD

File Transfer Timeout(s) •: 7200

Managing Change Requests - Enterprise Only

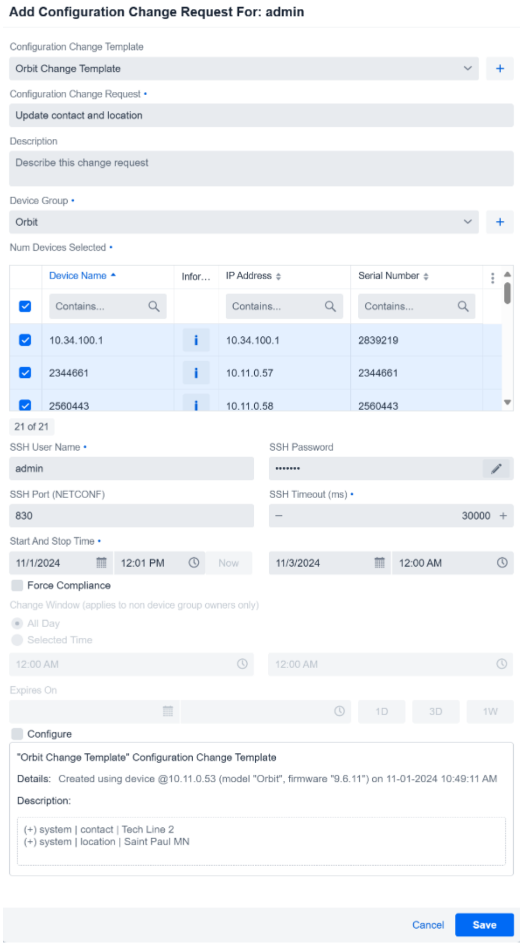
From the **Change Management** dashboard, select **Change Requests**. The Change Requests view allows creation of change requests as well as checking the status of existing requests.



Add Change Request
Add Configuration Change
Add Firmware Change
Add Certificate Change
Add Passphrase Change
Add SSH Command Change
Add Push Configuration Change
Restart Device To Active Image
Restart Device To Inactive Image
Restart Device To Specific Version
Restart Device To Latest Version

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



Add Configuration Change Request For: admin

Configuration Change Template: Orbit Change Template

Configuration Change Request •: Update contact and location

Description: Describe this change request

Device Group •: Orbit

Num Devices Selected •

☑	Device Name	Infor…	IP Address	Serial Number
☑	Contains...		Contains...	Contains...
☑	10.34.100.1	i	10.34.100.1	2839219
☑	2344661	i	10.11.0.57	2344661
☑	2560443	i	10.11.0.58	2560443

21 of 21

SSH User Name •: admin

SSH Password: ••••••••

SSH Port (NETCONF): 830

SSH Timeout (ms) •: 30000

Start And Stop Time •: 11/1/2024 12:01 PM Now — 11/3/2024 12:00 AM

□ Force Compliance

Change Window (applies to non device group owners only)

● All Day

○ Selected Time

12:00 AM — 12:00 AM

Expires On

1D 3D 1W

□ Configure

"Orbit Change Template" Configuration Change Template

Details: Created using device @10.11.0.53 (model "Orbit", firmware "9.6.11") on 11-01-2024 10:49:11 AM

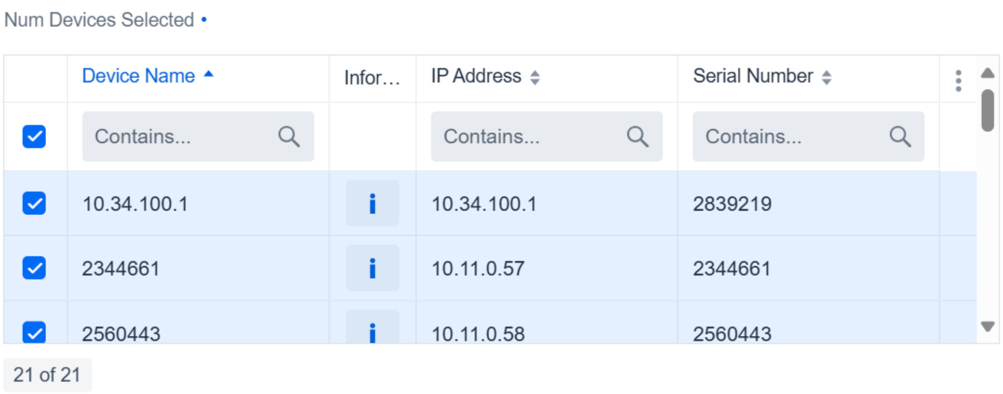
Description:

(+) system | contact | Tech Line 2
(+) system | location | Saint Paul MN

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.

- First select the Configuration Change Template to use for this change request. If an appropriate configuration change template has already been defined, select it from the dropdown menu. If a predefined configuration change template does not yet exist for this change request, click the Add icon to add a new configuration change template. See the Managing Change Templates section for additional details.
- Enter a Unique Name for the Configuration Change Request

- Enter a description of the request (optional)
- Select a **Device Group** to which the changes will be applied. If device groups have already been defined, select the appropriate group from the dropdown menu. If a predefined device group is not yet available for this change request, click the **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. Narrow the selection further by clicking the device icon to the right of the device count. Deselect any devices in the group that should not receive this change.



Num Devices Selected •

	Device Name ▲	Infor...	IP Address ⇕	Serial Number ⇕
☑	Contains...		Contains...	Contains...
☑	10.34.100.1	i	10.34.100.1	2839219
☑	2344661	i	10.11.0.57	2344661
☑	2560443	i	10.11.0.58	2560443

21 of 21

- Next Enter the credentials that will be used to make the change on the device.
- Select the **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, the change window can be adjusted as needed for this specific change request.
- Clicking the **Calendar** icon allows configuration of the start or end time by selecting the day and time on the calendar widget. Clicking in the **Timestamp** field will allow direct editing to 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 a user with “write” access (via Access Control) to the 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 Writer or Default Approver for the group of devices 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. A user with “Write” access to the device group 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-writer (for example, an operator) can re-execute a change request. If the non-writer 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 the compliance service to be enabled. Under compliance, there is no alert, and the service itself determines which requests need to be run, and runs them. If selected, the compliance service will run against all devices in the Change Request. It is also possible to run an individual device compliance check from the Summary Device Detail view rather than as a change request.
- Once the **Configuration Change Template** is selected, the description and change details for the device configuration items that will be changed in this request will appear.

- Click the **Save** button to submit the new Change Request.
- Once the Configuration Change is running the progress will be tracked for each device. This can be found under the Menu item on the Change Request view. Select "Device Update Status" then total, Updated, Or Not Updated.

Adding a Firmware Change Request

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

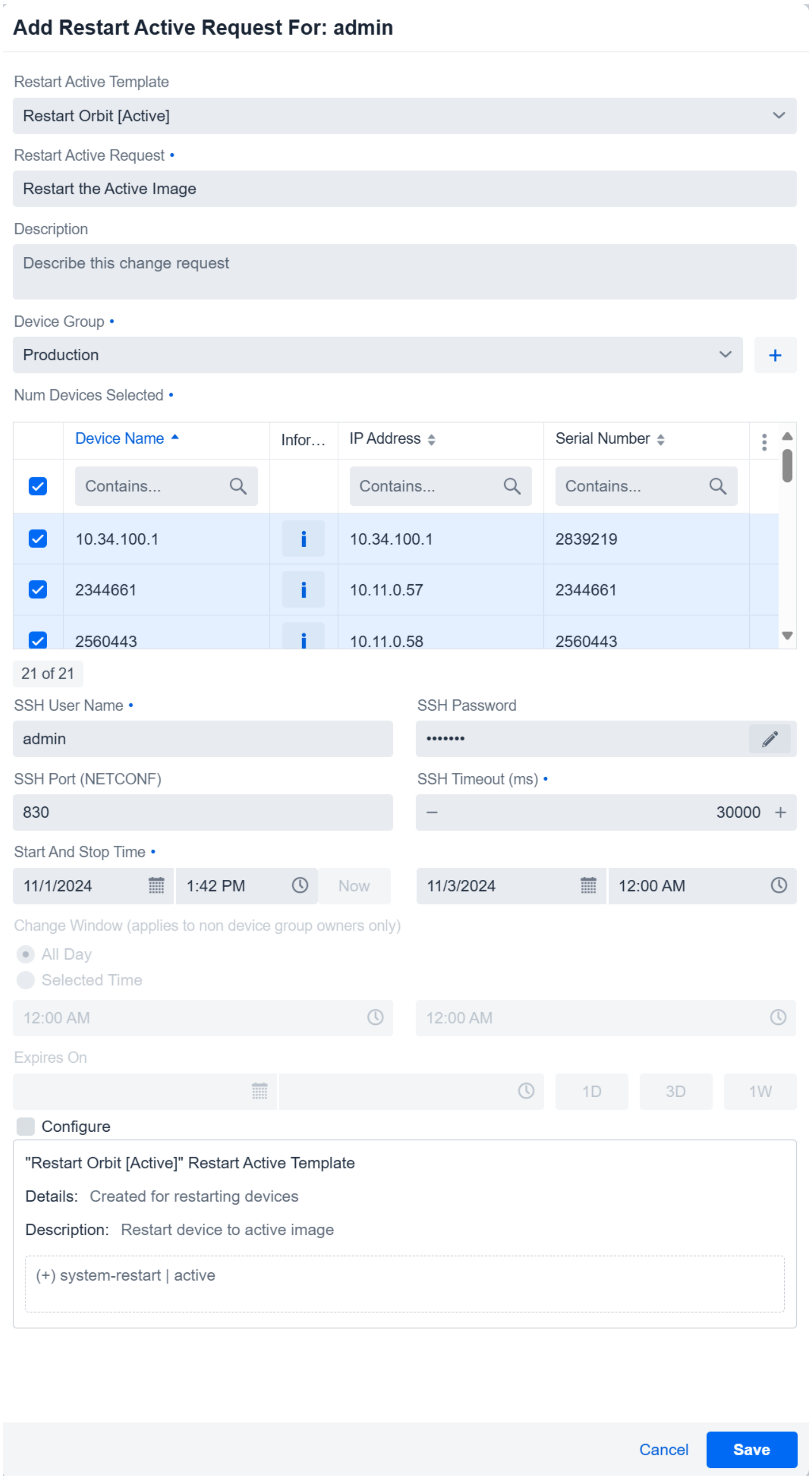
- Select a **Device Group** to which this Firmware Change Request will apply.
- Select the **Start** and **Stop** times during which this change will be allowed. Set the Change Window, if required.
- Choose a **Firmware Change Template** from the dropdown list. If a predefined template is not available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

- Click the **Save** button to submit the new Change Request.
- Once the Firmware Change is running the progress will be tracked for each device. This can be found under the Menu item on the Change Request view. Select “Device Update Status” then total, Updated, Or Not Updated.

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.



Add Restart Active Request For: admin

Restart Active Template: Restart Orbit [Active]

Restart Active Request •: Restart the Active Image

Description: Describe this change request

Device Group •: Production

Num Devices Selected •

☑	Device Name ▲	Infor…	IP Address	Serial Number
☑	Contains...		Contains...	Contains...
☑	10.34.100.1	i	10.34.100.1	2839219
☑	2344661	i	10.11.0.57	2344661
☑	2560443	i	10.11.0.58	2560443

21 of 21

SSH User Name •: admin

SSH Password: •••••••

SSH Port (NETCONF): 830

SSH Timeout (ms) •: 30000

Start And Stop Time •: 11/1/2024 1:42 PM Now 11/3/2024 12:00 AM

Change Window (applies to non device group owners only)

● All Day

○ Selected Time

12:00 AM 12:00 AM

Expires On

1D 3D 1W

□ Configure

"Restart Orbit [Active]" Restart Active Template

Details: Created for restarting devices

Description: Restart device to active image

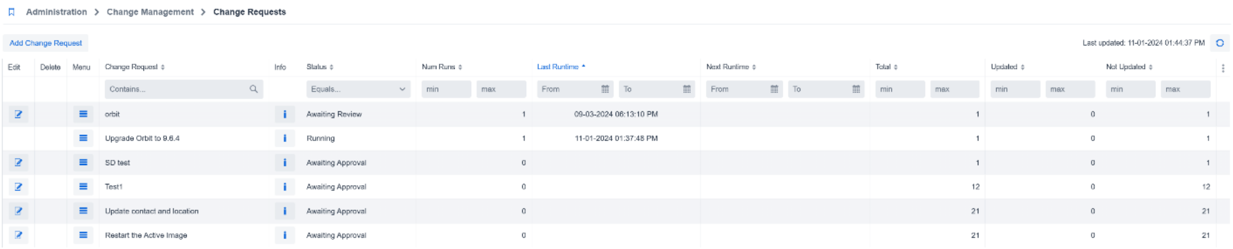
(+) system-restart | active

- Choose a **Restart Device Template** from the dropdown list. The available templates will be limited to those available for the type of **Restart Request** 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 the option 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, the description and details that will be sent to the remote radios as part of this request will appear.
- 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.

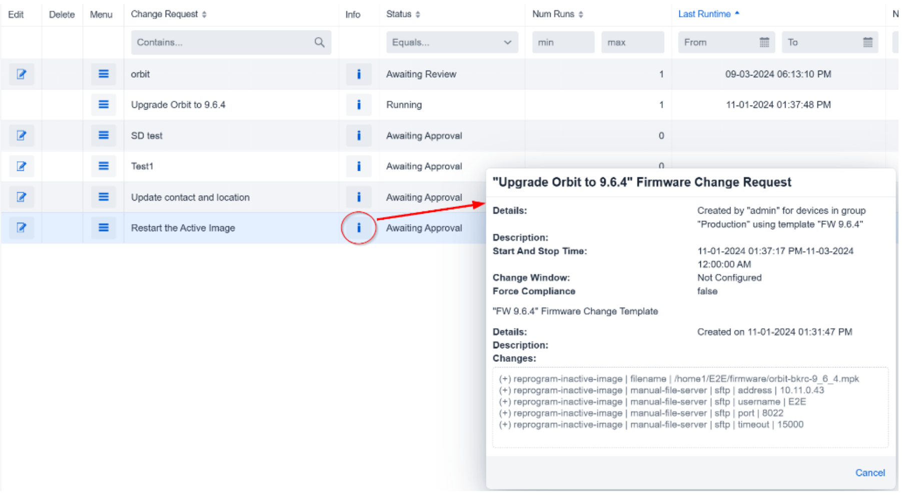


Last updated: 11-01-2024 01:44:37 PM

Edit	Delete	Menu	Change Request	Info	Status	Num Runs	Last Runtime	Next Runtime	Total	Updated	Not Updated
			Contains...		Equals...	min max	From To	From To	min max	min max	min max
✎		≡	orbit	i	Awaiting Review	1	09-03-2024 06:13:10 PM		1	0	1
		≡	Upgrade Orbit to 9.6.4	i	Running	1	11-01-2024 01:37:48 PM		1	0	1
✎		≡	SD test	i	Awaiting Approval	0			1	0	1
✎		≡	Test1	i	Awaiting Approval	0			12	0	12
✎		≡	Update contact and location	i	Awaiting Approval	0			21	0	21
✎		≡	Restart the Active Image	i	Awaiting Approval	0			21	0	21

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, Running, awaiting approval is eligible to be Canceled.

Clicking the **Information** icon will display a brief summary of the change request.



Edit	Delete	Menu	Change Request ⇕	Info	Status ⇕	Num Runs ⇕		Last Runtime ▴		N
			Contains...		Equals...	min	max	From	To	
✎		≡	orbit	i	Awaiting Review	1		09-03-2024 06:13:10 PM		
		≡	Upgrade Orbit to 9.6.4	i	Running	1		11-01-2024 01:37:48 PM		
✎		≡	SD test	i	Awaiting Approval	0				
✎		≡	Test1	i	Awaiting Approval	0				
✎		≡	Update contact and location	i	Awaiting Approval					
✎		≡	Restart the Active Image	i	Awaiting Approval					

"Upgrade Orbit to 9.6.4" Firmware Change Request

Details: Created by "admin" for devices in group "Production" using template "FW 9.6.4"
Description:
Start And Stop Time: 11-01-2024 01:37:17 PM-11-03-2024 12:00:00 AM
Change Window: Not Configured
Force Compliance false

"FW 9.6.4" Firmware Change Template

Details: Created on 11-01-2024 01:31:47 PM
Description:
Changes:

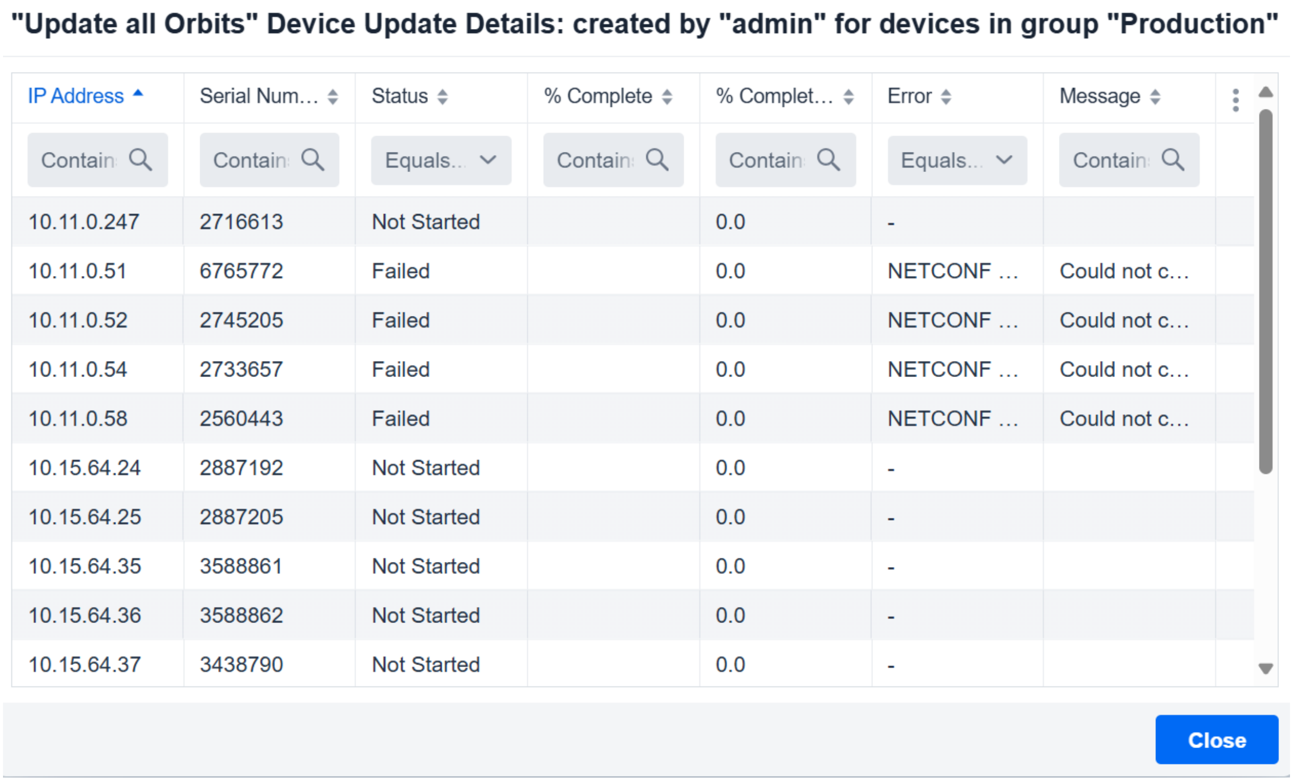
```
(+) reprogram-inactive-image | filename | /home1/E2E/firmware/orbit-bkrc-9_6_4.mpk
(+) reprogram-inactive-image | manual-file-server | sftp | address | 10.11.0.43
(+) reprogram-inactive-image | manual-file-server | sftp | username | E2E
(+) reprogram-inactive-image | manual-file-server | sftp | port | 8022
(+) reprogram-inactive-image | manual-file-server | sftp | timeout | 15000
```

If an **Edit** icon appears in the column next to the **Information** icon, it is possible to edit several of the Change Request fields. Editable fields include the **Description** and the **Change Window** for non-owners of the device group.

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 the next runtime to be customized, if 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.

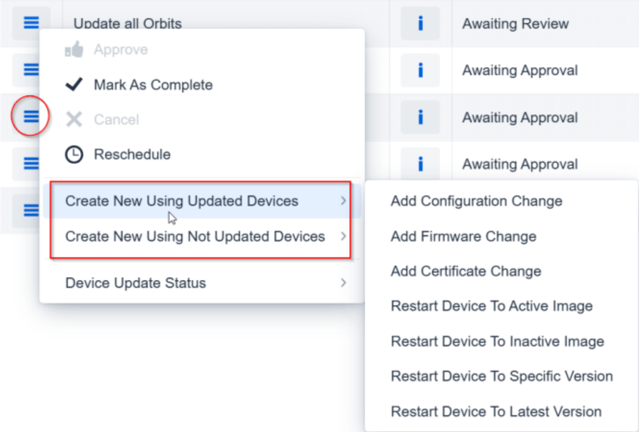
Users can click on the Menu icon from there select “Device Update Status” to see more details of the request. This will also display if there are any errors.



"Update all Orbits" Device Update Details: created by "admin" for devices in group "Production"

IP Address	Serial Num...	Status	% Complete	% Complet...	Error	Message
Contain	Contain	Equals..	Contain	Contain	Equals..	Contain
10.11.0.247	2716613	Not Started		0.0	-	
10.11.0.51	6765772	Failed		0.0	NETCONF ...	Could not c...
10.11.0.52	2745205	Failed		0.0	NETCONF ...	Could not c...
10.11.0.54	2733657	Failed		0.0	NETCONF ...	Could not c...
10.11.0.58	2560443	Failed		0.0	NETCONF ...	Could not c...
10.15.64.24	2887192	Not Started		0.0	-	
10.15.64.25	2887205	Not Started		0.0	-	
10.15.64.35	3588861	Not Started		0.0	-	
10.15.64.36	3588862	Not Started		0.0	-	
10.15.64.37	3438790	Not Started		0.0	-	

After a change request has entered the status of Completed or Awaiting Review. User can create another change request based on the device updated and not updated. This allows users to run a change request based on the results of a previous change request.



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, all fields with the **Edit** icon located to the right in the field can be edited.
- Click the **Edit** icon to make change.

NOTE: If more than one value on an SD Device must be changed, it is recommended that the traditional Change Management menu is used to run the request rather than the Device Detail view (see **Change Management** for more details). If 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 a config change is made 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.

Trigger Force Compliance - Enterprise Only

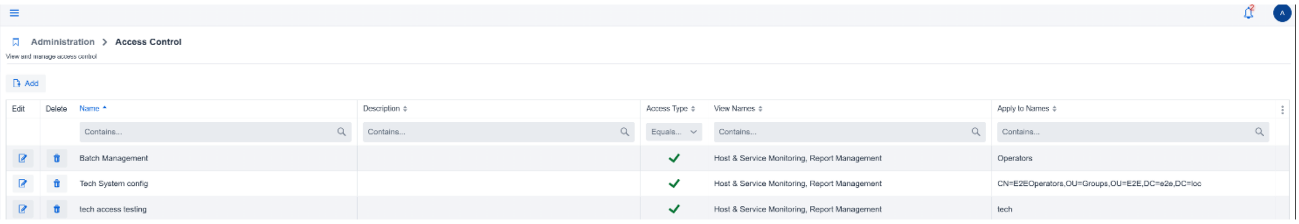
To trigger force compliance per device go to the device from the total summary view and click on the **Gear** icon and select **"Trigger Force Compliance."** This will cause PulseNET to look through the change requests that have Force Compliance enabled and then it will apply those change requests in the sequence in which they were created if the device is accessible.

ACCESS CONTROL - Enterprise Only

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**.



Administration > Access Control

View and manage access control

Add

Edit	Delete	Name	Description	Access Type	View Names	Apply to Names
		Contains...	Contains...	Equals...	Contains...	Contains...
		Batch Management		✓	Host & Service Monitoring, Report Management	Operators
		Tech System config		✓	Host & Service Monitoring, Report Management	CN=E2EOperators,OU=Groups,OU=E2E,DC=e2e,DC=loc
		tech access testing		✓	Host & Service Monitoring, Report Management	tech

Delete Access Control Records

- Select the checkbox on one or more rows which are to be deleted
- Click the **Delete** button and then confirm deletion of 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 will be edited. Any property except the unique Access Control Name can be edited.

Add Access Control Records

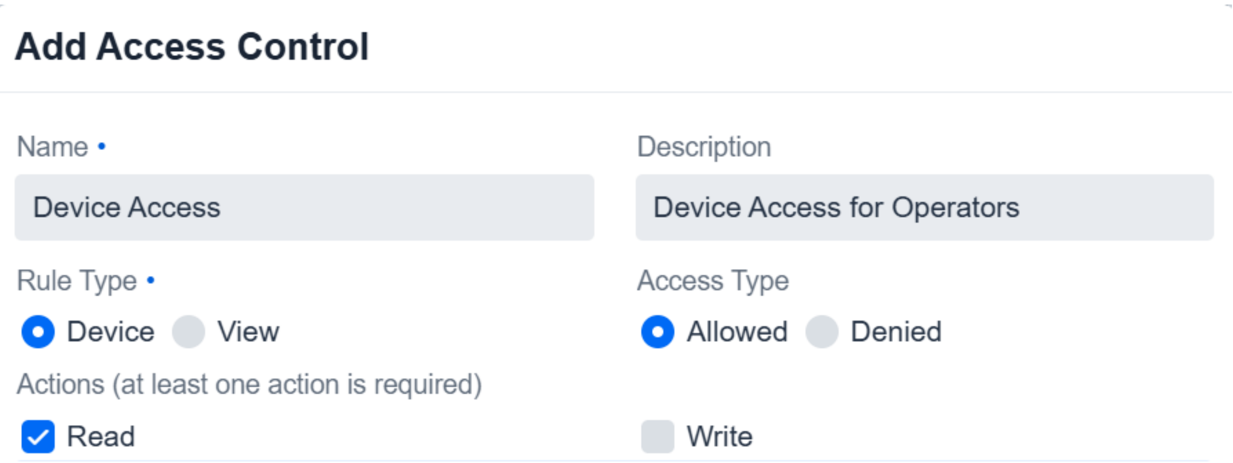
Click the **Add** button and enter the information for the new Access Control

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**.

There are two options under **Rule Type** - **Device** and **View**.



Add Access Control

Name •

Device Access

Description

Device Access for Operators

Rule Type •

● Device ○ View

Access Type

● Allowed ○ Denied

Actions (at least one action is required)

☑ Read

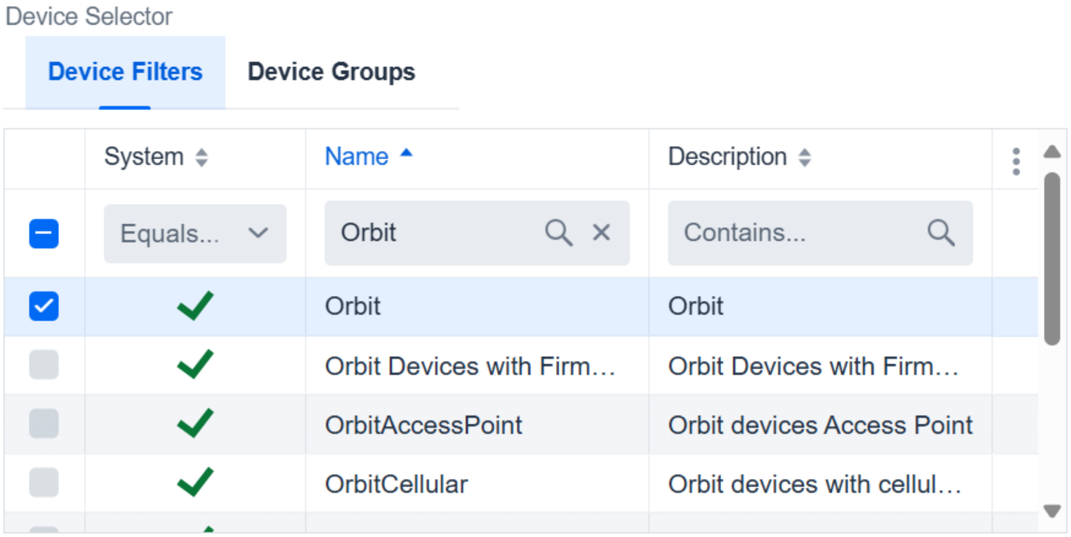
□ Write

Rule Type: Device is used to provide access to specific Devices, or Device Groups

Access Type contains the options Allowed or Denied. **Allowed** will provide device access for the selected users, while **Denied** will prevent the selected users from viewing or managing the device/group. This provides the flexibility to add features for users who need them or remove features for users who should not be allowed to access them.

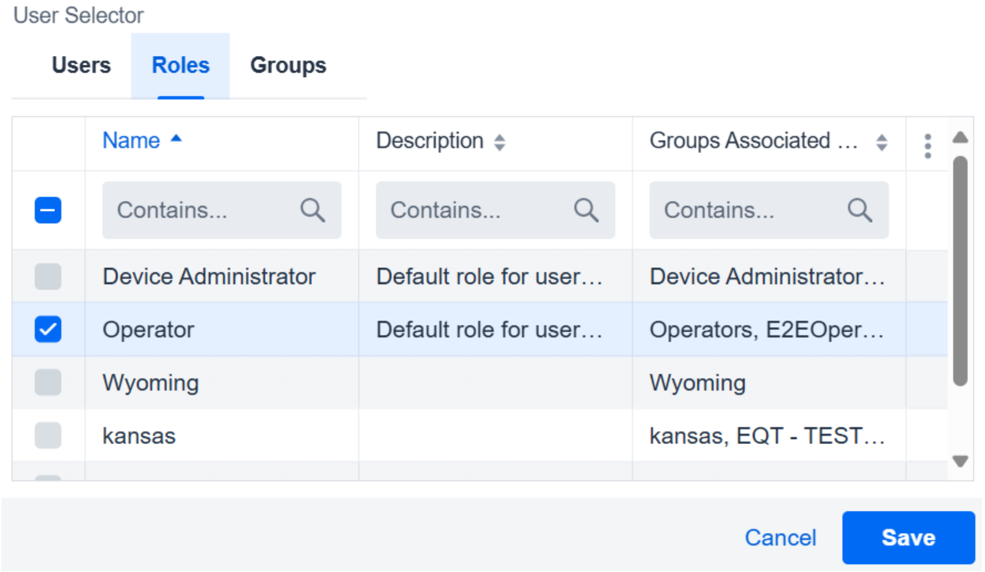
Actions contains the option for Read or Write access. (Write access automatically includes Read.) **Read** access allows the user to view the device but does not allow any changes to be made. **Write** access allows the user to view and make changes to the device. **Note:** Write access to the device/group is required for a user to be able to approve and run a device Change Request.

Once the above has been set, select at least one option from the Device Filters or Device Groups.



	System	Name	Description
▬	Equals...	Orbit	Contains...
☑	✓	Orbit	Orbit
□	✓	Orbit Devices with Firm…	Orbit Devices with Firm…
□	✓	OrbitAccessPoint	Orbit devices Access Point
□	✓	OrbitCellular	Orbit devices with cellul…

Then in the User Selector, check at least one option from the Users, Roles, and groups.

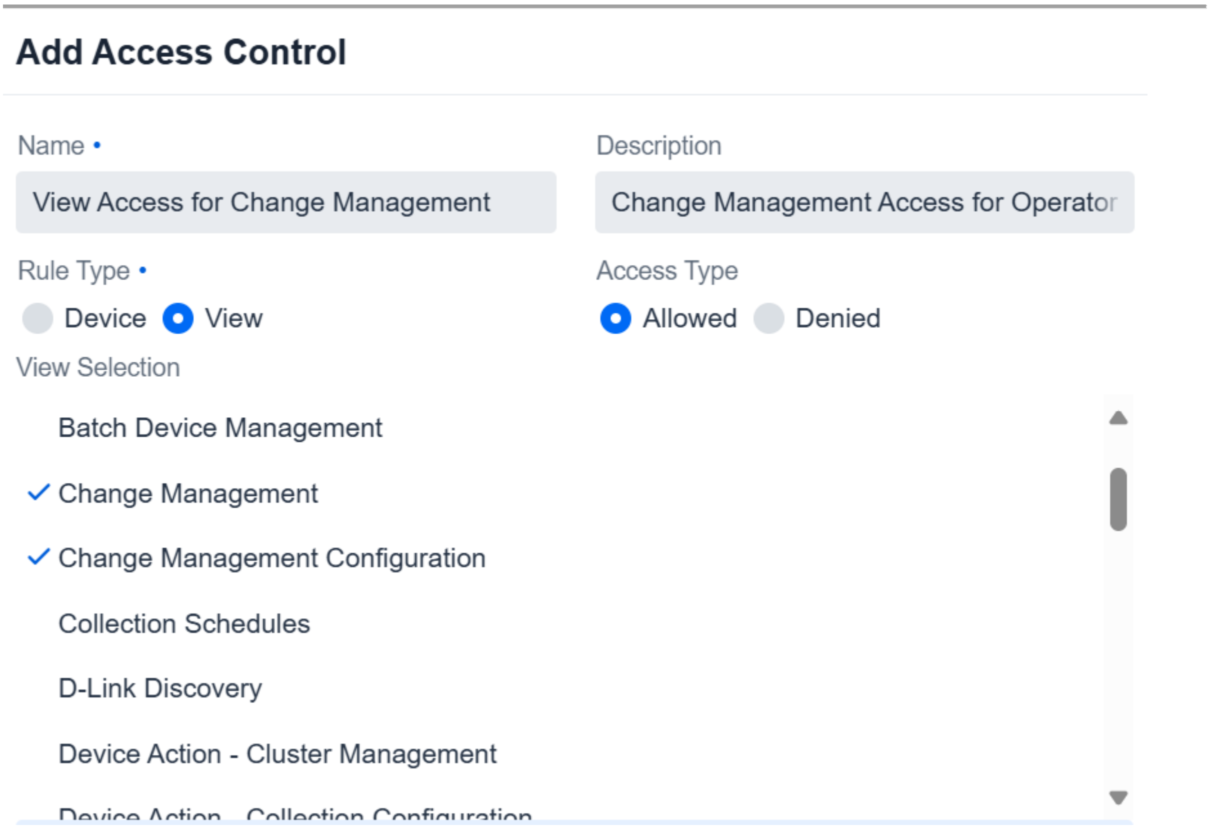


	Name	Description	Groups Associated …
▬	Contains...	Contains...	Contains...
□	Device Administrator	Default role for user…	Device Administrator…
☑	Operator	Default role for user…	Operators, E2EOper…
□	Wyoming		Wyoming
□	kansas		kansas, EQT - TEST…

In this example, any users with the User Role of Operator will be given access to the Orbit Device Group.

When configured correctly, hit **Save** to enact the new Access Control policy.

Rule Type: View is used to provide access to specific dashboards or control features.



Add Access Control

Name • View Access for Change Management

Description: Change Management Access for Operator

Rule Type • ○ Device ● View

Access Type ● Allowed ○ Denied

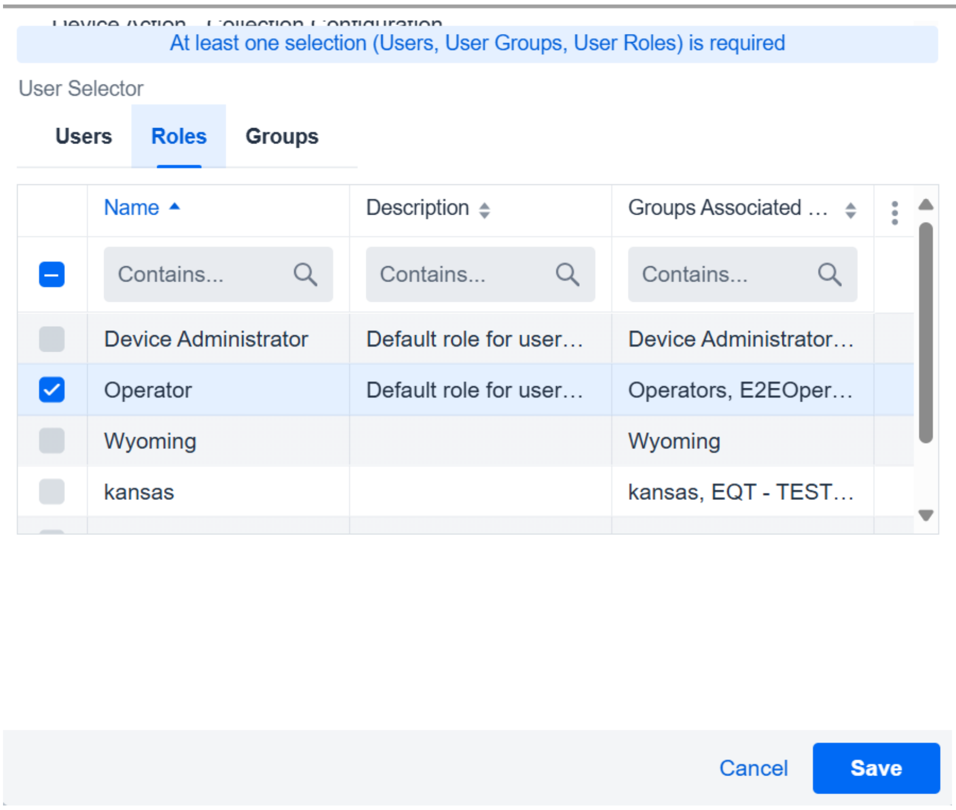
View Selection

- Batch Device Management
- ✓ Change Management
- ✓ Change Management Configuration
- Collection Schedules
- D-Link Discovery
- Device Action - Cluster Management
- Device Action - Collection Configuration

Access Type contains the options Allowed or Denied. **Allowed** will provide view access for the selected users, while **Denied** will prevent the selected users from accessing the selected menu/feature. This provides the flexibility to add features for users who need them, or remove features for users who should not be allowed to access them. Note: administrators cannot be denied access to views.

The **View Selection** menu contains all features that can be allowed or denied for users. Select one or more Views from the left menu, and use the arrows to move desired features over to the right menu, Selected Views. Any feature in the Selected Views menu will be Allowed/Denied.

On the User menu below, select at least one option from the Users, User Roles, or User Groups section to which the Selected Views will be applied.



At least one selection (Users, User Groups, User Roles) is required

User Selector

☐	Name ▲	Description	Groups Associated ...
☐	Contains...	Contains...	Contains...
☐	Device Administrator	Default role for user...	Device Administrator...
☑	Operator	Default role for user...	Operators, E2EOper...
☐	Wyoming		Wyoming
☐	kansas		kansas, EQT - TEST...

When finished, click **Save** to save the 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), several different Access Control records may be required for each dashboard or user group.

DEVICE DISCOVERY

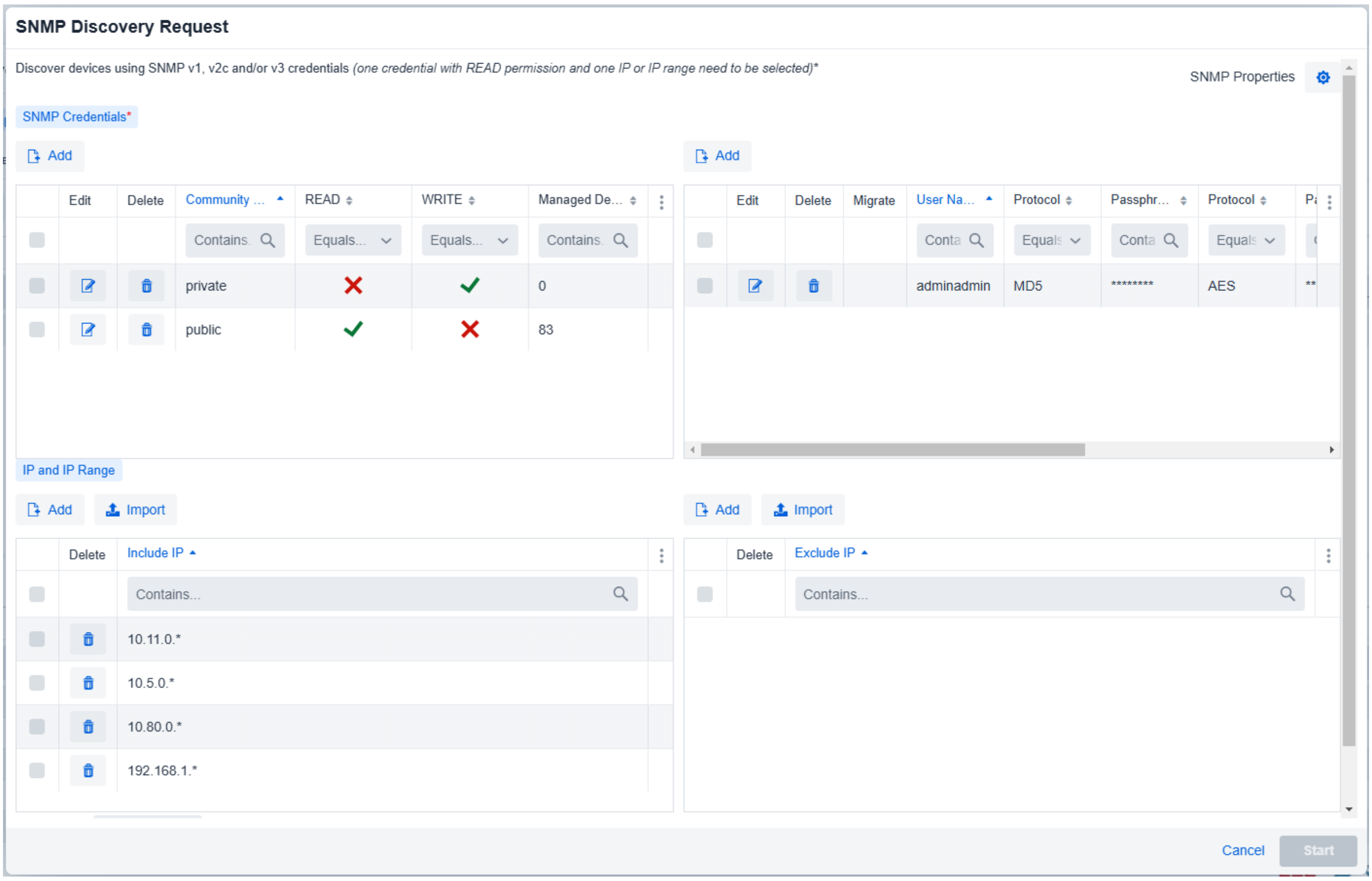
For **Standard** installations, the Device Discovery Menu is located at **Administration > Device Discovery**. For **Enterprise** installations, click the **Gear** icon at the upper right corner of the **Summary** dashboard to select the discovery features from the dropdown list.

Before GE PulseNET can monitor the network devices it must first discover them and provide the option to authorize them for management. Enterprise Device Discovery is a task that could be delegated to non-Administrator users, thus the options for discovering devices appear on the Summary dashboard rather than the Administration dashboard.

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 discovering EntraNet devices, at least one WRITE credential must be selected.
   - The more credentials specified, the longer the discovery typically runs. If the SNMP community strings or credentials needed are not found in the list, 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 more than one Community String to be selected, it is best practice to run discovery with just one SNMP read-only selected at a time. This prevents the discovery action from being flagged by an internal IT system 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 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**.



SNMP Discovery Request

Discover devices using SNMP v1, v2c and/or v3 credentials *(one credential with READ permission and one IP or IP range need to be selected)**

SNMP Credentials*

	Edit	Delete	Community ...	READ	WRITE	Managed De...
□			Contains.	Equals...	Equals...	Contains.
□			private	✗	✓	0
□			public	✓	✗	83

	Edit	Delete	Migrate	User Na...	Protocol	Passphr...	Protocol	P
□				Conta	Equals	Conta	Equals	
□				adminadmin	MD5	********	AES	**

IP and IP Range

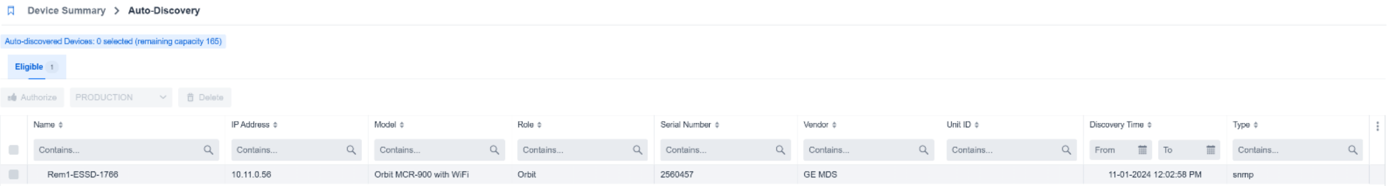
	Delete	Include IP
□		Contains...
□		10.11.0.*
□		10.5.0.*
□		10.80.0.*
□		192.168.1.*

	Delete	Exclude IP
□		Contains...

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

Auto-Discover of SNMP Devices

Auto-Discovery is now available for **Orbit LN and NX radios**. First discover the AP from the Discovering SNMP Devices. For devices to be Auto-Discovered a configuration poll must run on the AP. Once the device shows in the Auto-Discovery view it can be authorized.



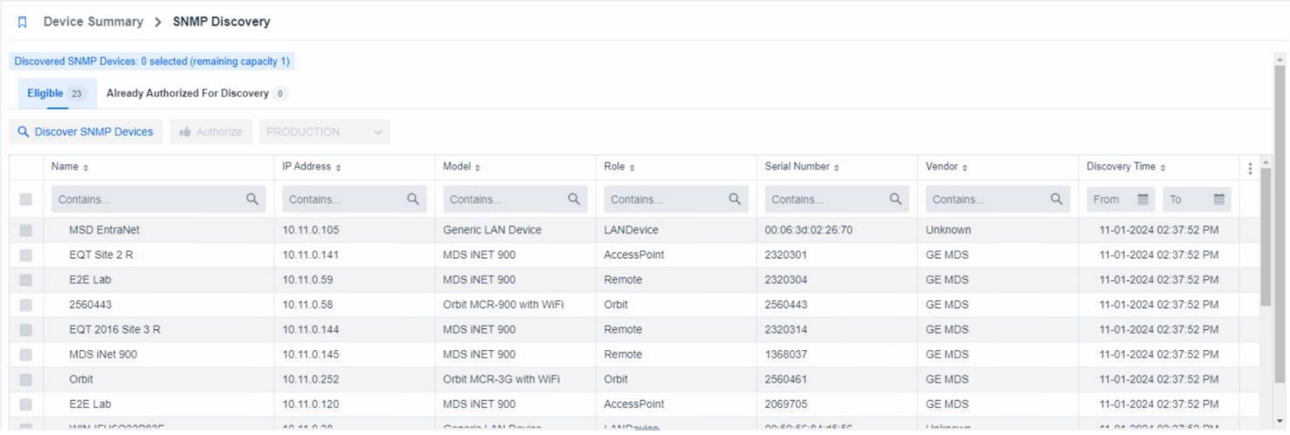
Device Summary > **Auto-Discovery**

Auto-discovered Devices: 0 selected (remaining capacity 165)

	Name	IP Address	Model	Role	Serial Number	Vendor	Unit ID	Discovery Time	Type
□	Contains...	Contains...	Contains...	Contains...	Contains...	Contains...	Contains...	From To	Contains...
□	Rem1-ESSD-1766	10.11.0.56	Orbit MCR-900 with WiFi	Orbit	2560457	GE MDS		11-01-2024 12:02:58 PM	snmp

Note: Other SNMP devices are not supported, only Dlink and Orbit LN/NX. If SNMP device needs to be removed from this view click on the delete button for the selected device(s). SNMP devices will continue to be auto-discovered once a configuration poll is triggered. If a Dlink device is deleted from Auto-Discovery view, the stingdlink service must be restarted. Then the device will be available for Auto-Discovery again.

Discovered Devices



Device Summary > SNMP Discovery

Discovered SNMP Devices: 0 selected (remaining capacity 1)

Eligible 23 | Already Authorized For Discovery 0

Discover SNMP Devices | Authorize | PRODUCTION

Name	IP Address	Model	Role	Serial Number	Vendor	Discovery Time
MSD EntraNet	10.11.0.105	Generic LAN Device	LANDevice	00:06:3d:02:26:70	Unknown	11-01-2024 02:37:52 PM
EQT Site 2 R	10.11.0.141	MDS iNET 900	AccessPoint	2320301	GE MDS	11-01-2024 02:37:52 PM
E2E Lab	10.11.0.59	MDS iNET 900	Remote	2320304	GE MDS	11-01-2024 02:37:52 PM
2560443	10.11.0.58	Orbit MCR-900 with WiFi	Orbit	2560443	GE MDS	11-01-2024 02:37:52 PM
EQT 2016 Site 3 R	10.11.0.144	MDS iNET 900	Remote	2320314	GE MDS	11-01-2024 02:37:52 PM
MDS iNet 900	10.11.0.145	MDS iNET 900	Remote	1368037	GE MDS	11-01-2024 02:37:52 PM
Orbit	10.11.0.252	Orbit MCR-3G with WiFi	Orbit	2560461	GE MDS	11-01-2024 02:37:52 PM
E2E Lab	10.11.0.120	MDS iNET 900	AccessPoint	2069705	GE MDS	11-01-2024 02:37:52 PM

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, it will list any decommissioned devices that may need to be reauthorized, as well as notifications about any monitored devices that have significant configuration changes.

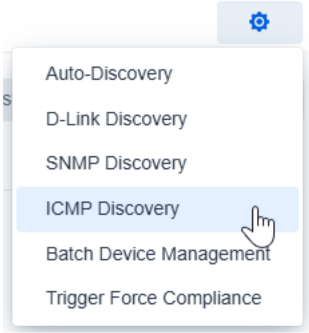
If there are decommissioned devices that must be reauthorized, the option to do so will be listed here. Also, if discovery becomes aware that the configuration for a device has changed, an option to acquire the new configuration information will appear.

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 ICMP Devices (With PulseNET Device Monitor)

If a license for the PulseNET Device Monitor has been deployed, the option for ICMP Discovery will appear in the Summary > Gear Icon dropdown menu.



On the ICMP Discovery Request menu, specify the IP or IP range of the device(s) to be discovered in the left panel. Define IP addresses or ranges to be excluded from the discovery in the right panel. Click Start to begin the discovery attempt. The discovery request is processed and a list of eligible devices will be displayed in the left panel.

NOTE: At least one PulseNET Enterprise license is required to activate. ICMP Ping mode monitors availability and response time. ICMP Properties can be modified by clicking on the gear icon in the top right of the ICMP Discovery Request menu or by navigating to Administration > Monitoring Configuration > ICMP Configuration.

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, which is explained in more detail below. 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 the network.

Active Discovery

During active discovery the master device will immediately return information from the remote devices in the network. This discovery method has the potential to be intrusive on certain networks because of the additional traffic it creates.

If using 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. Appending the request only to existing traffic. This means that discovery may 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 adding 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.

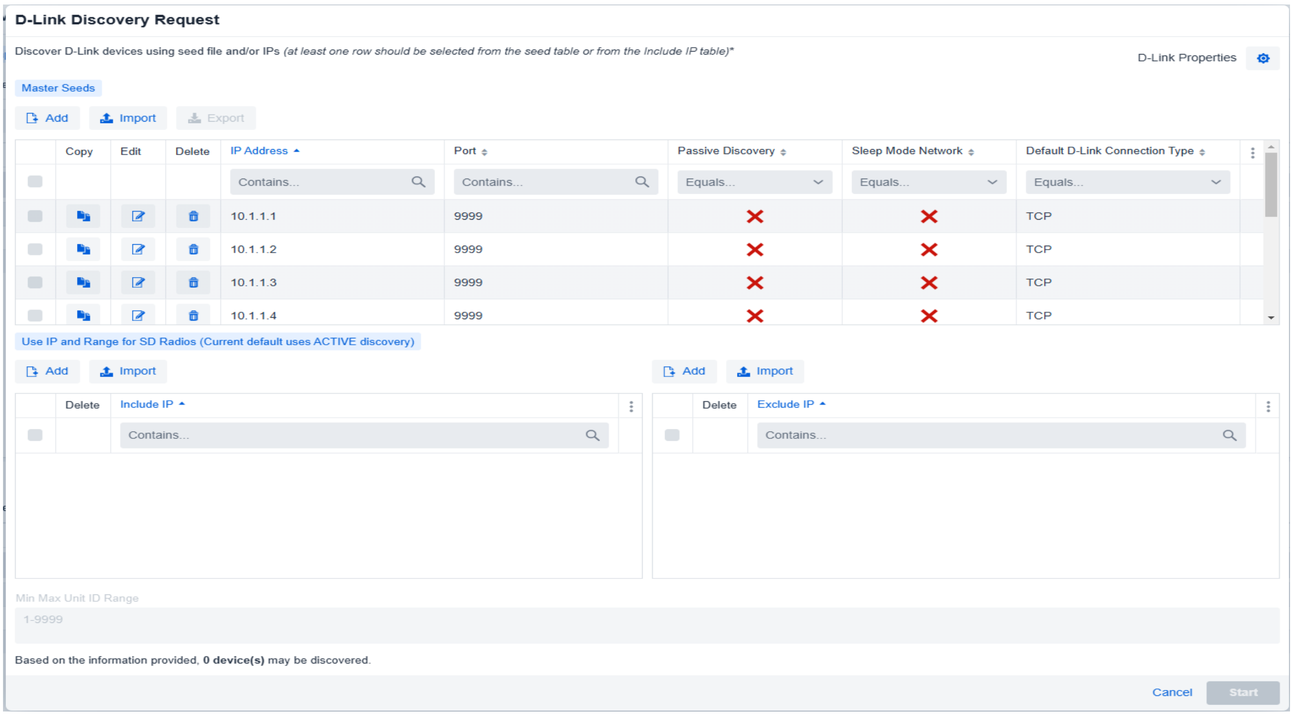
Discover DLINK Devices

1. Click the **Discover DLINK Devices** button and select Master devices for discovery using either a Master Seed definition or by specifying the IP address of an SD Master radio.

   NOTE: If the required DLINK Master Seed(s) are not available, 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 specified, the longer the discovery process is likely to take. A timeout value for both active and passive modes can be set and modified, which will determine how long the discovery is allowed to run.

   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. The required port may vary. CIDR protocol is now supported for IP management.
2. Repeat, adding as many IP addresses and ranges as needed. It is also possible to specify IP addresses or ranges to be excluded from discovery.
3. If using Active Discovery, indicate the specific Unit IDs or a range of target Unit IDs for the set of radios being discovered. 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.



D-Link Discovery Request

Discover D-Link devices using seed file and/or IPs *(at least one row should be selected from the seed table or from the Include IP table)**

D-Link Properties
Master Seeds
Add
Import
Export

	Copy	Edit	Delete	IP Address	Port	Passive Discovery	Sleep Mode Network	Default D-Link Connection Type
□				Contains...	Contains...	Equals...	Equals...	Equals...
□				10.1.1.1	9999	✗	✗	TCP
□				10.1.1.2	9999	✗	✗	TCP
□				10.1.1.3	9999	✗	✗	TCP
□				10.1.1.4	9999	✗	✗	TCP

Use IP and Range for SD Radios (Current default uses ACTIVE discovery)
Add
Import

	Delete	Include IP
□		Contains...

	Delete	Exclude IP
□		Contains...

Min Max Unit ID Range

1-9999

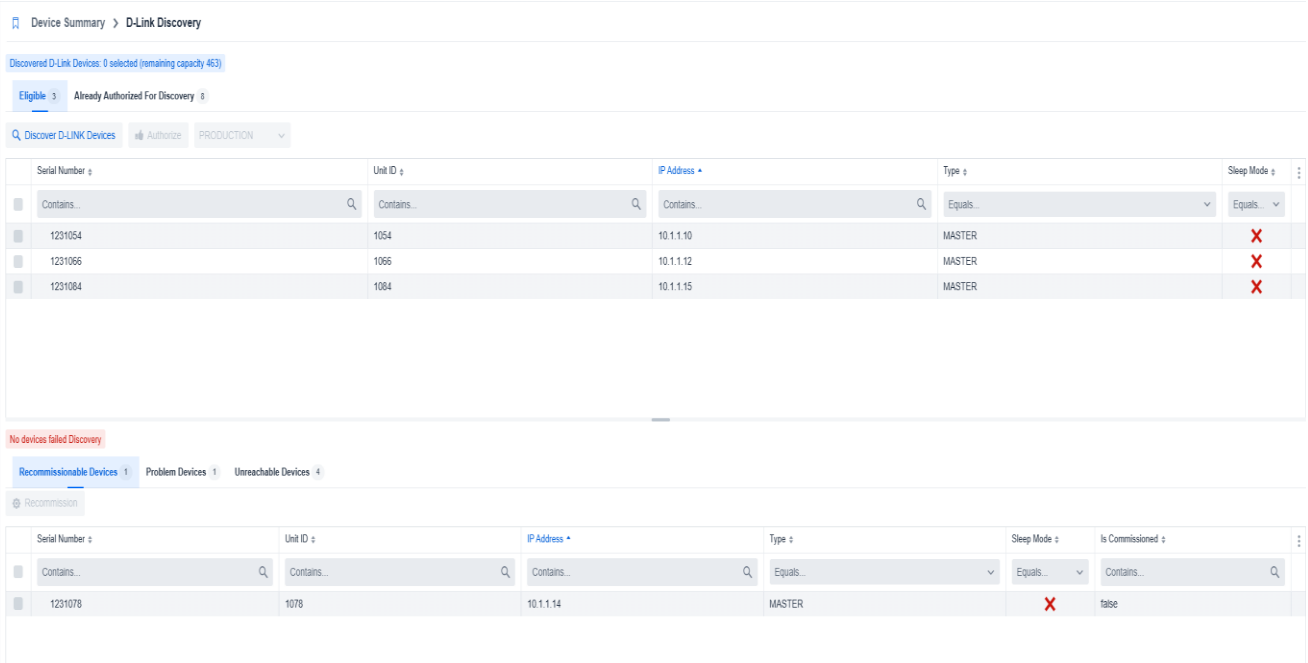
Based on the information provided, **0 device(s)** may be discovered.

The discovery request will be 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.

During discovery the Discovery Progress pane at the top right will list any decommissioned devices that may need to be reauthorized, as well as any monitored devices that have significant configuration changes.



Discovered D-Link Devices: 0 selected (remaining capacity 463)

Serial Number	Unit ID	IP Address	Type	Sleep Mode
Contains...	Contains...	Contains...	Equals...	Equals...
1231054	1054	10.1.1.10	MASTER	✗
1231066	1066	10.1.1.12	MASTER	✗
1231084	1084	10.1.1.15	MASTER	✗

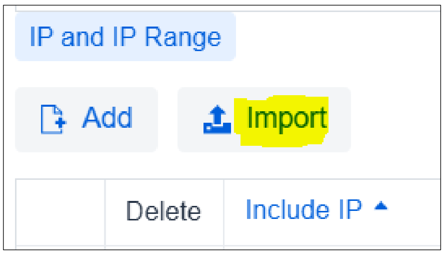
No devices failed Discovery

Serial Number	Unit ID	IP Address	Type	Sleep Mode	Is Commissioned
Contains...	Contains...	Contains...	Equals...	Equals...	Contains...
1231078	1078	10.1.1.14	MASTER	✗	false

If there are decommissioned devices that need to be reauthorized, the option to do so will appear here. Also, if discovery becomes aware that the configuration for a device has changed, the option will appear to acquire the new configuration information.

Import IP or IP Range

A specific list of IPs, or an IP range can be imported directly into the "Include IP" menu of any ICMP, DLink, or SNMP Discovery Request.

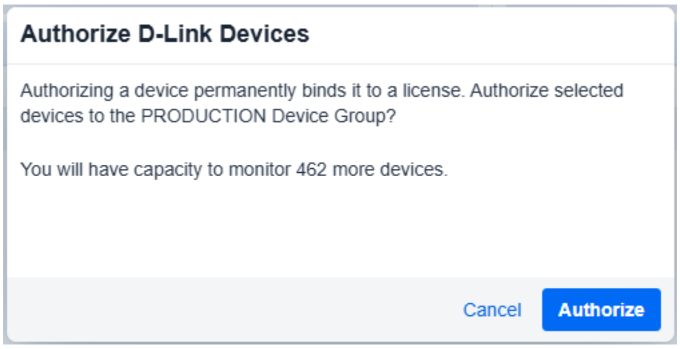


Click the Import button on the IP menu of any discovery request, then select and upload the comma-separated list of IP addresses that will be imported.

Click Import and the list of IPs will be added to the "Include IP" menu where they can be used for discovery requests.

Discovering DLINK Redundant Clusters - Enterprise Only

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 the option of authorizing the devices as members of a redundant cluster. Click Authorize to continue.



Authorize D-Link Devices

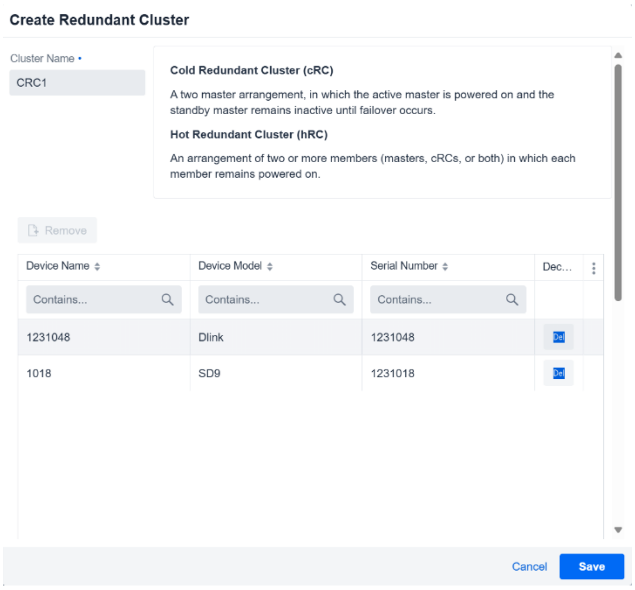
Authorizing a device permanently binds it to a license. Authorize selected devices to the PRODUCTION Device Group?

You will have capacity to monitor 462 more devices.

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. 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.



Create Redundant Cluster

Cluster Name • CRC1

Cold Redundant Cluster (cRC)

A two master arrangement, in which the active master is powered on and the standby master remains inactive until failover occurs.

Hot Redundant Cluster (hRC)

An arrangement of two or more members (masters, cRCs, or both) in which each member remains powered on.

Device Name	Device Model	Serial Number	Dec...
1231048	Dlink	1231048	Del
1018	SD9	1231018	Del

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 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.

Authorizing Devices

After discovering the devices in the network, they must be authorized 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 the selections and click **Authorize**.

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

Note: Each device is authorized based on the unique serial number, and PulseNET does not support re-using the same IP on a different device for this reason. If a device fails and requires replacement, it must be decommissioned in PulseNET to release the IP. License replacements for failed devices can be acquired by contacting GE PulseNET Support.

Working with Redundant Clusters - Enterprise Only

GE PulseNET Enterprise has the ability to associate two or more redundant devices into "clusters." This allows the system 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 the GE MDS support team. To create and work with redundant clusters, the user must be assigned the Failover Configuration permission. When selecting potential members to place in a redundant cluster, they must have the following prerequisites:

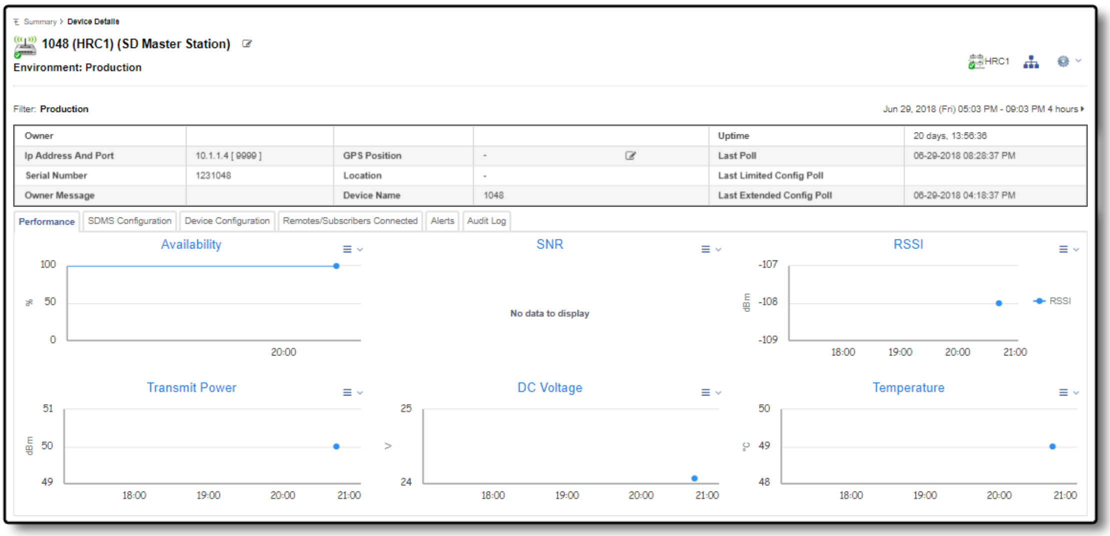
- Cluster devices must not be members of another cluster. If a potential cluster member is already part of another cluster, edit the old cluster to delete the potential member before adding that device to the new cluster. For information on deleting a member of an existing cluster, see **Editing Redundant Clusters**.
- If a potential member has been decommissioned, it must be rediscovered and reauthorized 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.


Summary › Device Details

1048 (HRC1) (SD Master Station)

Environment: Production

HRC1

Filter: Production

Jun 29, 2018 (Fri) 05:03 PM - 09:03 PM 4 hours

Owner				Uptime	20 days, 13:56:36
Ip Address And Port	10.1.1.4 [9999]	GPS Position	-	Last Poll	06-29-2018 08:28:37 PM
Serial Number	1231048	Location	-	Last Limited Config Poll	
Owner Message		Device Name	1048	Last Extended Config Poll	06-29-2018 04:18:37 PM

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 all required candidates have been added, 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 remotes connected to the redundant cluster.

Triggering Config Collection for Redundant Cluster

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

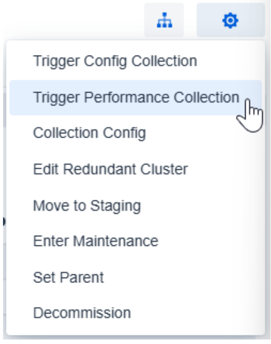
1. Navigate to the **Cluster Administration** menu and click on **Trigger Config**

Collection.

2. In the Trigger Config Collection window, confirm the configuration collection.
3. Click **OK** or **Cancel**.

Triggering Performance Collection for Redundant Cluster

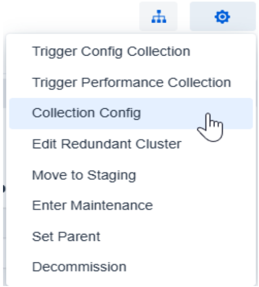
To trigger performance collection for a cold redundant cluster, follow these steps:



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

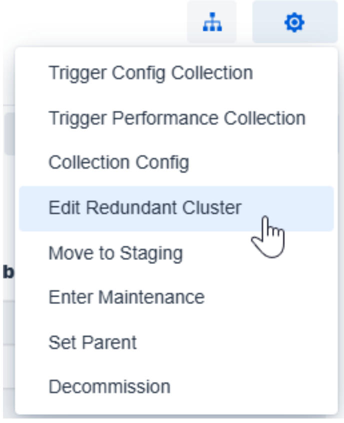
For more details about Collection Configuration of master devices see **Configuring data collection on DLINK master devices**. Editing collection configuration through the Cluster Administration menu will apply the modified collection configuration to all master devices in the redundant cluster.

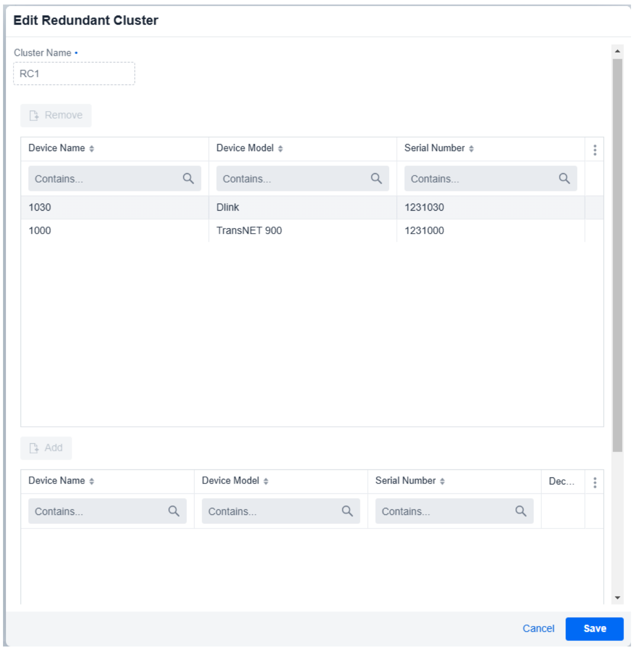


Editing Redundant Clusters

1. Navigate to the detail view of the redundant cluster.

2. Click the gear **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.




Edit Redundant Cluster

Cluster Name • RC1

Remove

Device Name	Device Model	Serial Number
1030	Dlink	1231030
1000	TransNET 900	1231000

Add

Device Name	Device Model	Serial Number	Dec...

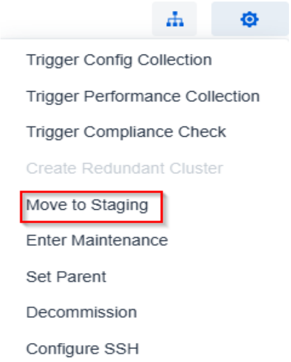
To remove members, in the Cluster Members table, click the **Decommission** icon in the device row. This member will be decommissioned and must be re-discovered and re-authorized. Continue until all desired devices are removed. If devices in a cluster are decommissioned until only one device remains, the cluster itself will be decommissioned.

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

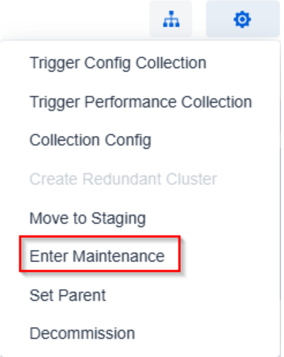


2. In the Change Environment window, confirm the move.
3. Click **OK** or **Cancel**.

Creating Maintenance Windows for Redundant Clusters

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**.



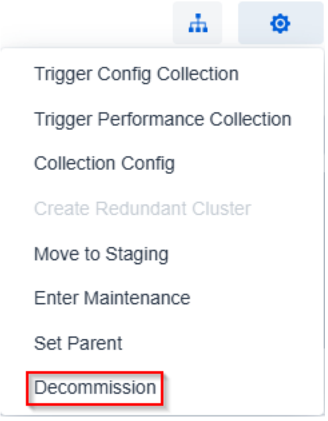
2. In the **Device Maintenance Mode** window, click the checkbox next to Blackout downstream devices.
3. Click the **OK** button. Click the **Cancel** button to cancel.

When creating a maintenance window, all members of the redundant cluster are placed in maintenance mode. A maintenance window cannot be created 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.

Multiple Masters can be put into maintenance mode simultaneously using **Batch Device Management**.

Decommissioning Redundant Clusters

In the Cluster Detail Page, navigate to the **Cluster Administration** menu. Click **Decommission** to decommission the whole cluster. The **Decommission Devices** window will list all 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 Devices

If a monitored device has been removed from service, decommission the device. Decommissioning must also be used if needing to swap devices located at the same IP address. The new device must have the same credentials as the monitored device that is being decommissioned. After decommissioning a 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 will also be decommissioned at the same time. To select all downstream devices, click the checkbox in the table header. Be aware that when decommissioning a DLINK master, all downstream devices are automatically decommissioned along with it.
3. Click **Yes** to confirm decommission.

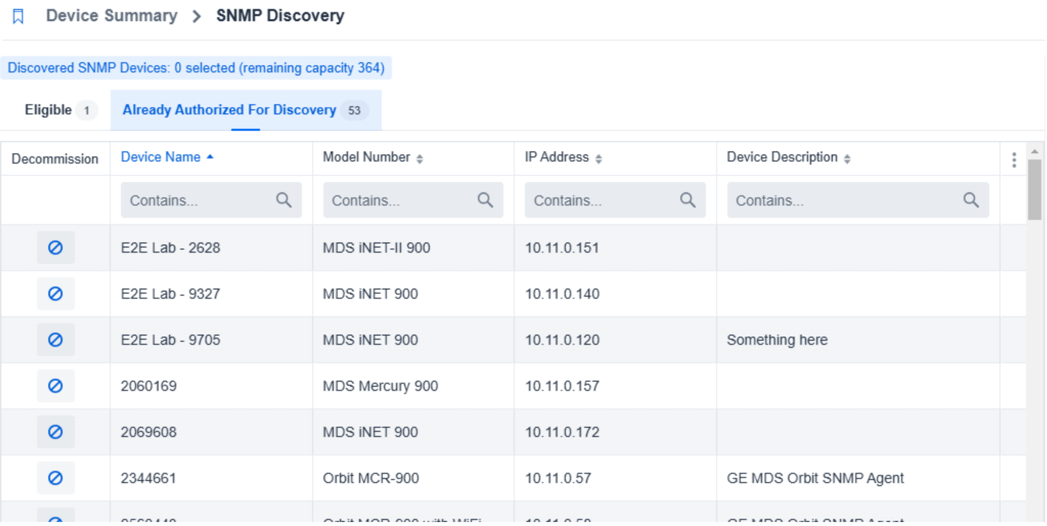
The device will be immediately decommissioned and removed from monitoring. Multiple Masters can be decommissioned simultaneously using **Batch Device Management**.

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.


Device Summary > SNMP Discovery
Discovered SNMP Devices: 0 selected (remaining capacity 364)
Eligible 1
Already Authorized For Discovery 53

Decommission	Device Name	Model Number	IP Address	Device Description
	Contains...	Contains...	Contains...	Contains...
⊘	E2E Lab - 2628	MDS iNET-II 900	10.11.0.151	
⊘	E2E Lab - 9327	MDS iNET 900	10.11.0.140	
⊘	E2E Lab - 9705	MDS iNET 900	10.11.0.120	Something here
⊘	2060169	MDS Mercury 900	10.11.0.157	
⊘	2069608	MDS iNET 900	10.11.0.172	
⊘	2344661	Orbit MCR-900	10.11.0.57	GE MDS Orbit SNMP Agent
⊘	[illegible]	Orbit MCR-900 with WiFi	10.11.0.58	GE MDS Orbit SNMP Agent

Click the **Delete** icon and confirm the decommission by clicking the **Yes** button.

Configuring data collection on DLINK master devices

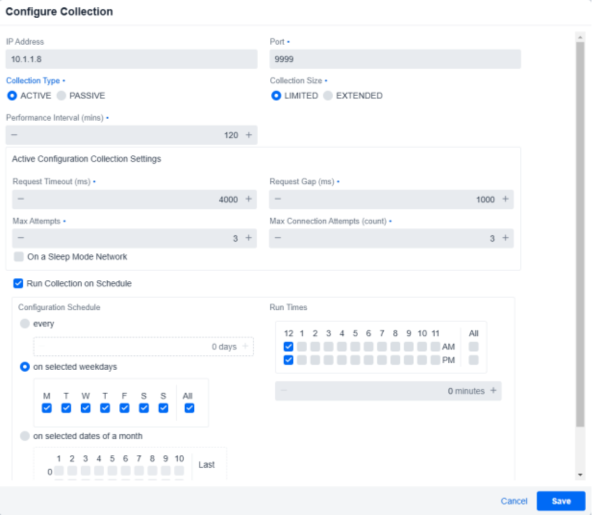
Use the **Configure Collection** option to define the collection type and scope of data collected on an individual DLINK master and its downstream devices. Global default settings are defined in the DLINK Properties section (see **Configuring DLINK Properties**).

Define Settings for an Individual Master Device

1. On the Detail view for the master, click the **Gear** ⚙ icon and select **Collection Config** from the list.
2. In the Configure Collection display, 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. The DLINK Request Timeout, Request Gap, Max Attempts, or Max Connection Attempts, as well as whether the network has been configured in Sleep Mode may need to be adjusted based on the radio performance and frequency of SCADA polling.



Configure Collection

IP Address: 10.1.1.8

Port •: 9999

Collection Type •: ● ACTIVE ○ PASSIVE

Collection Size •: ● LIMITED ○ EXTENDED

Performance Interval (mins) •: 120

Active Configuration Collection Settings

Request Timeout (ms) •: 4000

Request Gap (ms) •: 1000

Max Attempts •: 3

Max Connection Attempts (count) •: 3

□ On a Sleep Mode Network

☑ Run Collection on Schedule

Configuration Schedule

○ every 0 days

● on selected weekdays

M	T	W	T	F	S	S	All
☑	☑	☑	☑	☑	☑	☑	☑

○ on selected dates of a month

	1	2	3	4	5	6	7	8	9	10	Last
0	□	□	□	□	□	□	□	□	□	□	

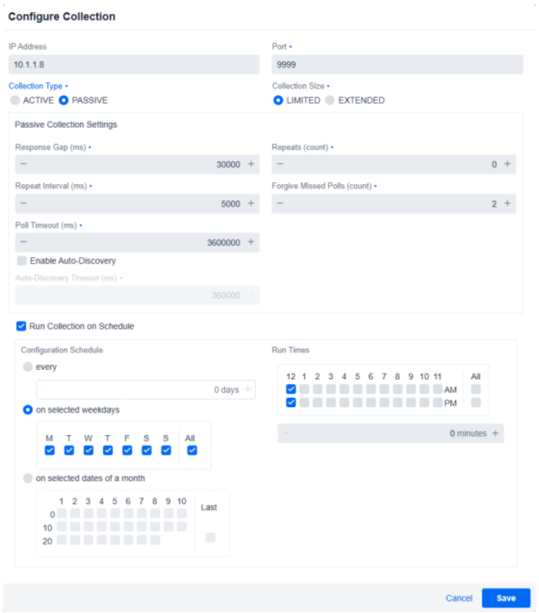
Run Times

12	1	2	3	4	5	6	7	8	9	10	11		All
☑	□	□	□	□	□	□	□	□	□	□	□	AM	□
☑	□	□	□	□	□	□	□	□	□	□	□	PM	□

0 minutes

Passive Collection Settings

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



Configure Collection

IP Address: 10.1.1.8

Port •: 9999

Collection Type •: ○ ACTIVE ● PASSIVE

Collection Size •: ● LIMITED ○ EXTENDED

Passive Collection Settings

Response Gap (ms) •: 30000

Repeats (count) •: 0

Repeat Interval (ms) •: 5000

Forgive Missed Polls (count) •: 2

Poll Timeout (ms) •: 3600000

□ Enable Auto-Discovery

Auto-Discovery Timeout (ms) •: 360000

☑ Run Collection on Schedule

Configuration Schedule

○ every 0 days

● on selected weekdays

M	T	W	T	F	S	S	All
☑	☑	☑	☑	☑	☑	☑	☑

○ on selected dates of a month

Run Times

	12	1	2	3	4	5	6	7	8	9	10	11	All
AM	☑	□	□	□	□	□	□	□	□	□	□	□	□
PM	☑	□	□	□	□	□	□	□	□	□	□	□	□

0 minutes

The DLINK Response Gap, Repeat Count, Repeat Interval, Forgive Missed Polls, and Poll Timeout may need to be adjusted based on the radio performance and frequency of SCADA polling

The Continuous Passive Auto-discovery option can be selected for a Master and any 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**).

1. Choose the Collection Size for configuration data. To minimize the impact of GE PulseNET's configuration collection, 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.

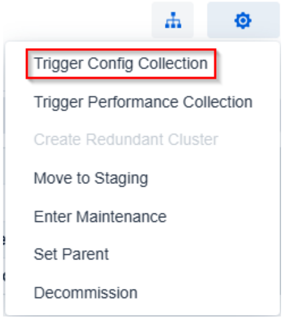
   Extended — all available configuration parameters are requested and returned for masters and remote devices. The total time to complete an extended collection will be greater than for a limited collection.

2. Next specify whether GE PulseNET should ask the devices for their configuration information. If Run Collection on Schedule is checked, then enter the collection schedule GE PulseNET will use for obtaining configuration data. For more information about using the scheduling tool, see **Scheduling Device Data Collection**.
3. Finally, set the collection interval on which GE PulseNET will ask devices for their Performance information.
4. Click **Save** to save the updated Collection Configuration for this Master.

Triggering Data Collections - Enterprise Only

Trigger an On-demand Configuration Collection

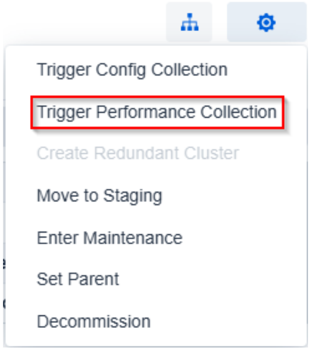
1. On the Device Detail display for any radio, click the **Gear** icon near the top right corner and select Trigger Config Collection.



2. Confirm 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.

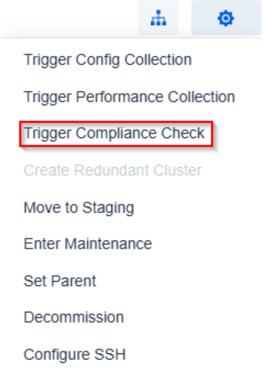


2. Confirm to trigger an on-demand configuration collection for this device (**Yes/Cancel**).

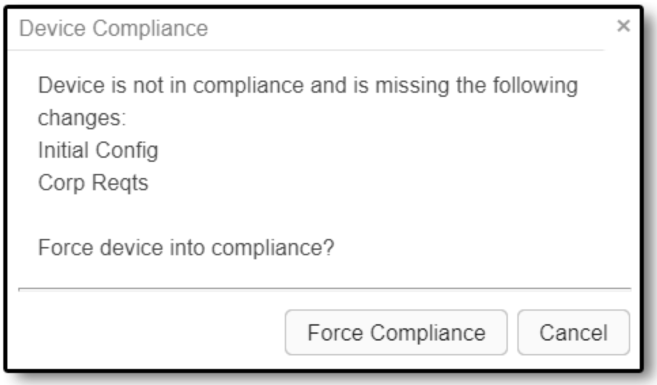
Trigger Compliance Checks

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 to immediately force compliance for the missing changes on that device by clicking on **Force Compliance.**



Device Compliance

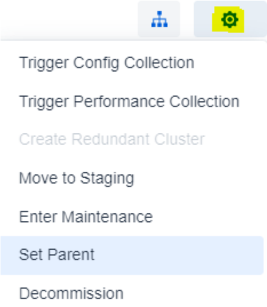
Device is not in compliance and is missing the following changes:
Initial Config
Corp Reqts

Force device into compliance?

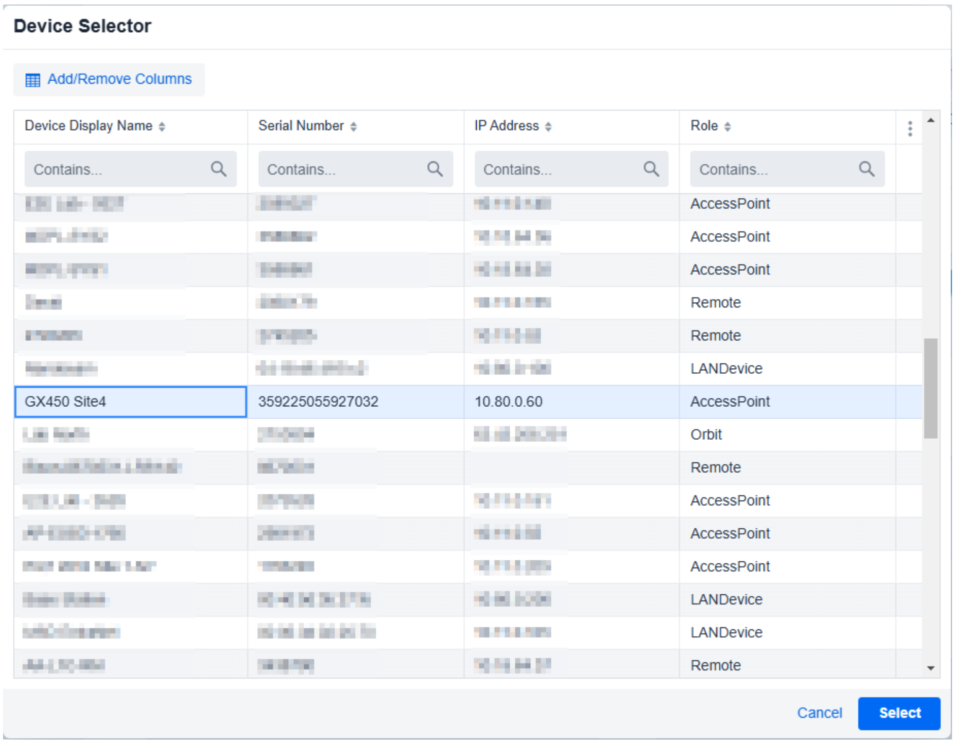
Setting Device Parent

Any device can be added as a parent device. This allows manual control over topology and connected remotes.

1. On the Device Detail display for any device, click the **Gear** icon near the top right corner and select **Set Parent.**



2. In the **Device Selector** window, select the parent device for the current device.

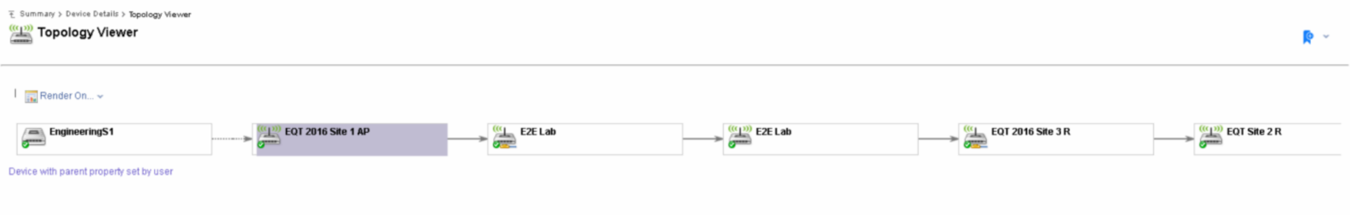


Device Selector

Add/Remove Columns

Device Display Name	Serial Number	IP Address	Role
Contains...	Contains...	Contains...	Contains...
[redacted]	[redacted]	[redacted]	AccessPoint
[redacted]	[redacted]	[redacted]	AccessPoint
[redacted]	[redacted]	[redacted]	AccessPoint
[redacted]	[redacted]	[redacted]	Remote
[redacted]	[redacted]	[redacted]	Remote
[redacted]	[redacted]	[redacted]	LANDevice
GX450 Site4	359225055927032	10.80.0.60	AccessPoint
[redacted]	[redacted]	[redacted]	Orbit
[redacted]	[redacted]		Remote
[redacted]	[redacted]	[redacted]	AccessPoint
[redacted]	[redacted]	[redacted]	AccessPoint
[redacted]	[redacted]	[redacted]	AccessPoint
[redacted]	[redacted]	[redacted]	LANDevice
[redacted]	[redacted]	[redacted]	LANDevice
[redacted]	[redacted]	[redacted]	Remote

3. Once the device is set as the parent, it will be shown in the connected remotes tab and the Topology View. The link will have a dotted line and the endpoint will be purple.



Note: Best practice is to allow PulseNET to programmatically connect endpoints. In certain cases this cannot be done through PulseNET this option allows you to manage those devices.

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. 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**.

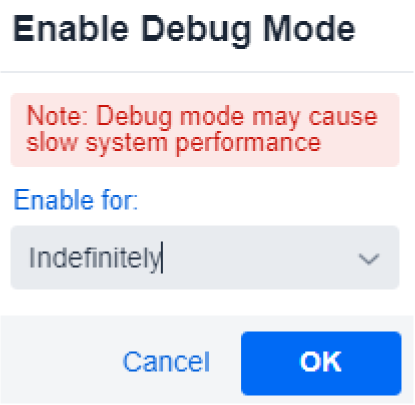
3. The **Include Observations** checkbox is an optional field this option gathers data for only those devices (limit 10 devices).
4. When prompted, either view the support bundle using a local archive manager or download it to the local machine.

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

Note: If the user interface of PulseNET is unable to be reached. An offline support bundle can be generated from running the support_log_bundle.bat from the PulseNET home directory where PulseNET is installed.

Enabling Debug Mode

Click on the **Toggle Debug Mode** button to enable. 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 system performance.



Enable Debug Mode

Note: Debug mode may cause slow system performance

Enable for:

Indefinitely

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:

Variable Binding	Field
1.3.6.1.4.1.4130.9.1.1	MESSAGE
1.3.6.1.4.1.4130.9.1.4	SERVICE
1.3.6.1.4.1.4130.9.1.6	RULE
1.3.6.1.4.1.4130.9.1.7	OBJECT_ID
1.3.6.1.4.1.4130.9.1.8	OBJECT_NAME
1.3.6.1.4.1.4130.9.1.9	SEVERITY
1.3.6.1.4.1.4130.9.1.10	HOST_NAME
1.3.6.1.4.1.4130.9.1.11	HOST_IP
1.3.6.1.4.1.4130.9.1.13	URL
1.3.6.1.4.1.4130.9.1.14	DATE_TIME

Operating System Updates - Safe Order to Stop all PulseNET Services

Stopping/Starting Services for Single Server Configuration:

1. Run the stop.bat/sh file located in \GE_MDS\PulseNET\ directory.
2. Once system updates have completed run the start.bat/sh from the same directory as in the first step.

Stopping/Starting Services for Multi-Server Configuration

1. Run the stop.bat/sh file located in \GE_MDS\PulseNET\ directory on the Primary Application Server.
2. Confirm the application services have stopped successfully. Then on the Primary Database Server run the stop.bat/sh file located in \GE_MDS\PulseNET\ directory.
3. Once system updates have completed run the start.bat/sh in from the above directory on the Primary Database Server and then on the Primary Application Server.

   (During step 2 stingmongo-log may not stop, it is safe to manually end/kill this process to make the service stop if needed.)

Stopping/Starting Services for 3 Server Configuration

1. Run the stop.bat/sh file located in \GE_MDS\PulseNET\ directory on the Application Server.
2. Confirm the application services have stopped successfully. Then on the next Application Server run the stop.bat/sh file located in \GE_MDS\PulseNET\ directory.
3. Run the stop.bat/sh file located in \GE_MDS\PulseNET\ directory on the Arbiter Server.
4. Once system updates have completed, run the start.bat/sh from the above directory on the Arbiter Server, then each of the other two Application Servers.

   (During step 3 **stingmongo-log** may not stop, it is safe to manually end/kill this process to make the service stop if needed.)

Stopping HA Configuration for OS patching:

1. Run the stop.bat/sh file located in \GE_MDS\PulseNET\ directory on the secondary application.
2. Run the stop.bat/sh file located in \GE_MDS\PulseNET\ directory on the primary application server.
3. Run the stop.bat/sh file located in \GE_MDS\PulseNET\ directory on the secondary database.
4. Run the stop.bat/sh file located in \GE_MDS\PulseNET\ directory on the primary database server.
   (During steps 3-4 **stingmongo-log** may not stop, it is safe to manually end/kill this process to make the service stop if needed.)

5. Once system updates have completed, run the start.bat/sh from the above directory on the Primary database, Secondary Database, Primary Application, and lastly the Secondary Application Servers.

Notes:

- All PulseNET services start with sting* prefix.
- In the main PulseNET folder is a checkprocesses.bat/sh - this script will check the status of the services.

(Note: the following message may be shown if the services do not exist on the server or if the service is stopped. "INFO: No tasks are running which match the specified criteria.")

- There is a disable.bat/sh script that will disable the services to prevent them from starting up when the OS restarts, so **if multiple restarts** are required this could be used.
- After using the disable.bat/sh script if used, ensure to run the enable.bat when the patching process is completed.

Maintenance Mode for API

Activate/Deactivate Maintenance Mode:

```
curl -H "X-Sting-API-Key: YWRtaW46YWRtaW4=" -X GET http://localhost:8080/api/maintenance/2344661  **Note: Gets the status of Maint. Mode**
```

```
curl -H "X-Sting-API-Key: YWRtaW46YWRtaW4=" -X POST http://localhost:8080/api/maintenance/2344661 **Note: Sets Maint. Mode**
```

```
curl -H "X-Sting-API-Key: YWRtaW46YWRtaW4=" -X DELETE http://localhost:8080/api/maintenance/2344661 **Note: Removes Maint. Mode**
```

Decommission By IP example:

```
curl -H "X-Sting-API-Key: YWRtaW46YWRtaW4=" -X POST http://localhost:8080/api/decommission/10.11.0.176
```

```
curl -H "X-Sting-API-Key: YWRtaW46YWRtaW4=" -X POST --header "Content-Type: application/json" --data '{ "ipaddress" : "10.11.0.176" }' http://localhost:8080/api/decommission
```

Decommission Example Decommission By Serial

```
curl -H "X-Sting-API-Key: YWRtaW46YWRtaW4=" -X POST http://localhost:8080/api/decommission/2344661
curl -H "X-Sting-API-Key: YWRtaW46YWRtaW4=" -X POST --header "Content-Type: application/json" --data
'{ "serialnumber" : "2344661" }' http://localhost:8080/api/decommission
```

Authorize by IP and Serial Example:

```
curl -H "X-Sting-API-Key: YWRtaW46YWRtaW4=" -X POST --header "Content-Type: application/json" --data
'{ "ipaddress" : "10.11.0.176", "serialnumber" : "2344661" }' http://localhost:8080/api/authorize
```

Authorize By IP Example:

```
curl -H "X-Sting-API-Key: YWRtaW46YWRtaW4=" -X POST http://localhost:8080/api/authorize/10.11.0.176
```

```
curl -H "X-Sting-API-Key: YWRtaW46YWRtaW4=" -X POST --header "Content-Type: application/json" --
data '{ "ipaddress" : "10.11.0.176" }' http://localhost:8080/api/authorize
```

Complementary Database SQL Schema

For reference by Database Administrator (s) :

```
USE [master]
GO
/****** Object:  Database [stingray]    Script Date: 3/11/2022 11:52:33 AM ******/
CREATE DATABASE [stingray]
 CONTAINMENT = NONE
 ON  PRIMARY
( NAME = N'stingray', FILENAME = N'C:\Program Files\Microsoft SQL
Server\MSSQL14.MSSQLSERVER\MSSQL\DATA\stingray.mdf' , SIZE = 139264KB , MAXSIZE = UNLIMITED,
FILEGROWTH = 65536KB )
 LOG ON
( NAME = N'stingray_log', FILENAME = N'C:\Program Files\Microsoft SQL
Server\MSSQL14.MSSQLSERVER\MSSQL\DATA\stingray_log.ldf' , SIZE = 401408KB , MAXSIZE = 2048GB ,
FILEGROWTH = 65536KB )
GO
ALTER DATABASE [stingray] SET COMPATIBILITY_LEVEL = 140
GO
IF (1 = FULLTEXTSERVICEPROPERTY('IsFullTextInstalled'))
begin
EXEC [stingray].[dbo].[sp_fulltext_database] @action = 'enable'
end
GO
ALTER DATABASE [stingray] SET ANSI_NULL_DEFAULT OFF
GO
ALTER DATABASE [stingray] SET ANSI_NULLS OFF
GO
ALTER DATABASE [stingray] SET ANSI_PADDING OFF
GO
```

```
ALTER DATABASE [stingray] SET ANSI_WARNINGS OFF
GO
ALTER DATABASE [stingray] SET ARITHABORT OFF
GO
ALTER DATABASE [stingray] SET AUTO_CLOSE OFF
GO
ALTER DATABASE [stingray] SET AUTO_SHRINK OFF
GO
ALTER DATABASE [stingray] SET AUTO_UPDATE_STATISTICS ON
GO
ALTER DATABASE [stingray] SET CURSOR_CLOSE_ON_COMMIT OFF
GO
ALTER DATABASE [stingray] SET CURSOR_DEFAULT  GLOBAL
GO
ALTER DATABASE [stingray] SET CONCAT_NULL_YIELDS_NULL OFF
GO
ALTER DATABASE [stingray] SET NUMERIC_ROUNDABORT OFF
GO
ALTER DATABASE [stingray] SET QUOTED_IDENTIFIER OFF
GO
ALTER DATABASE [stingray] SET RECURSIVE_TRIGGERS OFF
GO
ALTER DATABASE [stingray] SET  DISABLE_BROKER
GO
ALTER DATABASE [stingray] SET AUTO_UPDATE_STATISTICS_ASYNC OFF
GO
ALTER DATABASE [stingray] SET DATE_CORRELATION_OPTIMIZATION OFF
GO
ALTER DATABASE [stingray] SET TRUSTWORTHY OFF
GO
ALTER DATABASE [stingray] SET ALLOW_SNAPSHOT_ISOLATION OFF
GO
ALTER DATABASE [stingray] SET PARAMETERIZATION SIMPLE
GO
ALTER DATABASE [stingray] SET READ_COMMITTED_SNAPSHOT OFF
GO
ALTER DATABASE [stingray] SET HONOR_BROKER_PRIORITY OFF
GO
ALTER DATABASE [stingray] SET RECOVERY FULL
GO
ALTER DATABASE [stingray] SET  MULTI_USER
GO
ALTER DATABASE [stingray] SET PAGE_VERIFY CHECKSUM
GO
ALTER DATABASE [stingray] SET DB_CHAINING OFF
GO
ALTER DATABASE [stingray] SET FILESTREAM( NON_TRANSACTED_ACCESS = OFF )
GO
ALTER DATABASE [stingray] SET TARGET_RECOVERY_TIME = 60 SECONDS
GO
ALTER DATABASE [stingray] SET DELAYED_DURABILITY = DISABLED
GO
EXEC sys.sp_db_vardecimal_storage_format N'stingray', N'ON'
GO
ALTER DATABASE [stingray] SET QUERY_STORE = OFF
GO
```

```
USE [stingray]
GO
ALTER DATABASE SCOPED CONFIGURATION SET IDENTITY_CACHE = ON;
GO
ALTER DATABASE SCOPED CONFIGURATION SET LEGACY_CARDINALITY_ESTIMATION = OFF;
GO
ALTER DATABASE SCOPED CONFIGURATION FOR SECONDARY SET LEGACY_CARDINALITY_ESTIMATION =
PRIMARY;
GO
ALTER DATABASE SCOPED CONFIGURATION SET MAXDOP = 0;
GO
ALTER DATABASE SCOPED CONFIGURATION FOR SECONDARY SET MAXDOP = PRIMARY;
GO
ALTER DATABASE SCOPED CONFIGURATION SET PARAMETER_SNIFFING = ON;
GO
ALTER DATABASE SCOPED CONFIGURATION FOR SECONDARY SET PARAMETER_SNIFFING = PRIMARY;
GO
ALTER DATABASE SCOPED CONFIGURATION SET QUERY_OPTIMIZER_HOTFIXES = OFF;
GO
ALTER DATABASE SCOPED CONFIGURATION FOR SECONDARY SET QUERY_OPTIMIZER_HOTFIXES =
PRIMARY;
GO
USE [stingray]
GO
/****** Object:  User [stingray]    Script Date: 3/11/2022 11:52:33 AM ******/
CREATE USER [stingray] FOR LOGIN [stingray] WITH DEFAULT_SCHEMA=[dbo]
GO
ALTER ROLE [db_owner] ADD MEMBER [stingray]
GO
ALTER ROLE [db_accessadmin] ADD MEMBER [stingray]
GO
ALTER ROLE [db_securityadmin] ADD MEMBER [stingray]
GO
ALTER ROLE [db_ddladmin] ADD MEMBER [stingray]
GO
ALTER ROLE [db_backupoperator] ADD MEMBER [stingray]
GO
ALTER ROLE [db_datareader] ADD MEMBER [stingray]
GO
ALTER ROLE [db_datawriter] ADD MEMBER [stingray]
GO
/****** Object:  Table [dbo].[alert]    Script Date: 3/11/2022 11:52:33 AM ******/
SET ANSI_NULLS ON
GO
SET QUOTED_IDENTIFIER ON
GO
CREATE TABLE [dbo].[alert](
	[id] [varchar](25) NOT NULL,
	[deviceId] [varchar](25) NOT NULL,
	[alert] [varchar](1000) NULL,
PRIMARY KEY CLUSTERED
(
	[id] ASC
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF, ALLOW_ROW_LOCKS
= ON, ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]
) ON [PRIMARY]
```

```
GO
/****** Object:  Table [dbo].[device]    Script Date: 3/11/2022 11:52:34 AM ******/
SET ANSI_NULLS ON
GO
SET QUOTED_IDENTIFIER ON
GO
CREATE TABLE [dbo].[device](
	[id] [varchar](25) NOT NULL,
	[device] [varchar](max) NULL,
PRIMARY KEY CLUSTERED
(
	[id] ASC
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF, ALLOW_ROW_LOCKS
= ON, ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]
) ON [PRIMARY] TEXTIMAGE_ON [PRIMARY]
GO
/****** Object:  Table [dbo].[observation]    Script Date: 3/11/2022 11:52:34 AM ******/
SET ANSI_NULLS ON
GO
SET QUOTED_IDENTIFIER ON
GO
CREATE TABLE [dbo].[observation](
	[id] [varchar](25) NOT NULL,
	[deviceId] [varchar](25) NOT NULL,
	[observation] [varchar](max) NULL,
PRIMARY KEY CLUSTERED
(
	[id] ASC
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF, ALLOW_ROW_LOCKS
= ON, ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]
) ON [PRIMARY] TEXTIMAGE_ON [PRIMARY]
GO
USE [master]
GO
ALTER DATABASE [stingray] SET  READ_WRITE
GO
```

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.

E2E TECHNOLOGIES

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: e2etechinc.com/pages/legal.