

# MDS *Puise*NET

Network Management System

**Version 2.2**

*Enterprise*

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

MDS 05-6566A01, Rev. A  
FEBRUARY 2011



Digital Energy  
MDS

## Quest Copyright Notice

© 2011 Quest Software, Inc.  
ALL RIGHTS RESERVED.

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

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

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

Quest Software World Headquarters  
LEGAL Dept  
5 Polaris Way  
Aliso Viejo, CA 92656  
[www.quest.com](http://www.quest.com)  
email: [legal@quest.com](mailto:legal@quest.com)

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

## Patents

This product includes patent pending technology.

## Trademarks

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

## Third Party Contributions

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

## **About Quest Software, Inc.**

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

## **About GE MDS**

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

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

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

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

## **GE MDS ISO 9001 Registration**

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

## **To GE Customers**

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

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

## **Manual Revision and Accuracy**

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

**Administrator's Guide**  
**February 2011**  
**Version 2.2**



# Table of Contents

<b>Introduction .....</b>	<b>9</b>
Understanding PulseNET Roles.....	9
Starting and Stopping PulseNET.....	10
Starting PulseNET .....	10
Running PulseNET as a Windows Service.....	11
Stopping PulseNET .....	12
Logging in to PulseNET.....	13
Using the Administrator Home Dashboard.....	14
<b>Configuring System Settings.....</b>	<b>17</b>
Email Configuration .....	18
SNMP Trap Action Configuration .....	20
Schedule Management .....	22
Copying a Schedule to Create a New Schedule .....	22
Adding a New Schedule .....	24
Deleting a Schedule .....	27
System Configuration Summary.....	28
<b>Working with Licenses .....</b>	<b>29</b>
Requesting a License.....	29
Installing a License.....	31
Managing Licenses .....	32
Sort the Manage Licenses List .....	32
Search for an Installed License .....	32
Filter the Manage Licenses List.....	33
Install a New License.....	33
Delete an Installed License .....	33

Migrate Authorized Devices from an Expiring License to a New License .....	34
License Order when Authorizing Devices .....	34
<b>Collection Configuration .....</b>	<b>37</b>
SNMP Configuration .....	38
Add an SNMP v1 or v2c Community String .....	39
Delete an SNMP v1 or v2c Community String .....	39
Add SNMP v3 Credentials .....	40
Edit SNMP v3 Credentials .....	41
Delete SNMP v3 Credentials .....	41
Configure Advanced SNMP Settings .....	42
Migrate Devices from One Community String or Set of Credentials to Another .....	44
Sort an SNMP Table .....	45
Search for an SNMP Community String or Set of Credentials .....	46
Filter an SNMP Table .....	46
Dlink Configuration .....	46
Add a Dlink Master Seed .....	47
Edit Dlink Master Seed Settings .....	48
Delete a Dlink Master Seed .....	48
Configure Advanced Dlink Settings .....	49
Sort a Master Seed Table .....	52
Search for a Master Seed .....	53
Filter a Master Seed Table .....	53
Collection Management .....	53
Trigger Delay Values and Data Collection Frequency .....	56
<b>Working with Devices .....</b>	<b>57</b>
Discovering SNMP Devices .....	58
Discovery Progress .....	62
Ineligible Devices .....	62
Discovering Dlink Devices .....	63
Discovery Progress .....	68
Authorizing Devices .....	68
Configuring Access Point Failover .....	69
Creating and Managing Maintenance Windows .....	70

Decommissioning a Monitored Device .....	73
Managing Devices.....	75
Sort a List .....	75
Search for a Device in a List .....	76
Filter a List.....	76
Discover Devices.....	76
<b>Working with Rules and Alerts .....</b>	<b>77</b>
Enabling and Disabling Rules .....	80
Configuring Rule Thresholds.....	80
Turning Notification Email On or Off.....	82
Turning an SNMP Trap Action On or Off.....	82
Creating Custom PulseNET Rules .....	83
Editing a Custom Rule.....	97
Removing a Custom Rule .....	97
<b>Working with Reports .....</b>	<b>99</b>
Generating a Report.....	100
Scheduling a Report.....	100
Managing Reports.....	100
Managing Report Schedules .....	101
Building Custom Reports .....	103
<b>Working with Users .....</b>	<b>111</b>
Creating a User .....	112
Searching for a User .....	114
Managing Users .....	115
Sort the Manage Users List.....	115
Search for a User .....	116
Filter the Manage Users List .....	116
Create a New User.....	116
View the Configuration Details for an Existing User.....	116
Edit the Configuration of an Existing User.....	116
Copy the Configuration of an Existing User for Creating a New User .....	119
Change the Password of an Existing User .....	121
Expire the Password of an Existing User .....	121

Remove a User .....	121
Configuring Password Settings.....	122
Configuring User Session Timeout.....	123
<b>Support.....</b>	<b>125</b>
Generating a Support Bundle .....	126
Requesting Support.....	126
Managing Support Bundles .....	128
Sort the Support Bundles List .....	129
Search for a Generated Support Bundle.....	129
Filter the Support Bundles List.....	129
Generate a New Support Bundle .....	129
Download a Generated Support Bundle .....	129
Delete a Generated Support Bundle.....	130
<b>Appendix: Custom Report Metric View Parameters .....</b>	<b>131</b>
<b>Index .....</b>	<b>135</b>

# Introduction

This guide is intended to assist Administrators with configuring and managing MDS PulseNET Enterprise. It provides instructions on how to perform administrative tasks such as creating users, requesting and installing licenses, discovering and authorizing devices, requesting GE support, and configuring email settings, report schedules, rule thresholds, and the sample frequency of data collection.

For general PulseNET navigation instructions, see the *PulseNET Quick Start Guide*. For Operator role workflow instructions, see the *PulseNET User's Guide*.

This chapter describes the Operator and Administrator roles, provides instructions for starting, stopping and logging into PulseNET, and describes the Administrator Home dashboard you see when you log in with the Administrator role.

Perform these steps before following the instructions in this chapter:

- Obtain your PulseNET user name and password.
- Ensure that your Web browser has JavaScript functionality enabled.

## Understanding PulseNET Roles

There are two PulseNET roles:

- An operator is responsible for tracking the status of the devices that the PulseNET system is monitoring. Operators have access to a restricted set of dashboards.
- An administrator controls the overall functionality of the system and provides support for PulseNET operators. An administrator has a number of responsibilities including creating users, requesting and installing licenses, discovering and authorizing devices, requesting GE support, and configuring email settings, report schedules, rule thresholds, and the sample frequency of data collection.

# Starting and Stopping PulseNET

The following sections describe how to start and stop PulseNET.

---

**Note** For information on how to start and stop PulseNET in high availability (HA) mode, see “Starting and Stopping the Server in High Availability Mode” in the *PulseNET Installation and Setup Guide*.

---

## Starting PulseNET

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

*To start PulseNET from the command line:*

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

```
fms
```

*To start PulseNET from a Windows shortcut:*

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

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

```
PulseNET startup completed.
```

**Additional Commands:**

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

---

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

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

These WARN messages can safely be ignored.

---

## Running PulseNET as a Windows Service

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

---

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

---

## Using the Start Menu Options

To install or remove PulseNET service from the Start menu:

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

To start or stop PulseNET service from the Start menu:

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

## Using the Command Line

From the command line, type the following to install PulseNET as a Windows service:

```
fms.exe -i
```

### Additional Commands:

In addition to the additional commands listed in “[Starting and Stopping PulseNET](#)” on page 10, the following commands are available for the PulseNET Windows service.

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

## Stopping PulseNET

The following section describes how to stop PulseNET.

To stop PulseNET:

Do one of the following:

- Type **Ctrl-C** on the command window in which PulseNET started.
- Navigate to the directory `<pulsenet_home>\bin` and execute the following command:

```
fms -q
```

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

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

## Logging in to PulseNET

This section describes how to log in to the PulseNET browser interface.

---

**Note** PulseNET must be running before you can log in.

---

*To log in to PulseNET using a Web browser:*

- 1 Open a Web browser instance.

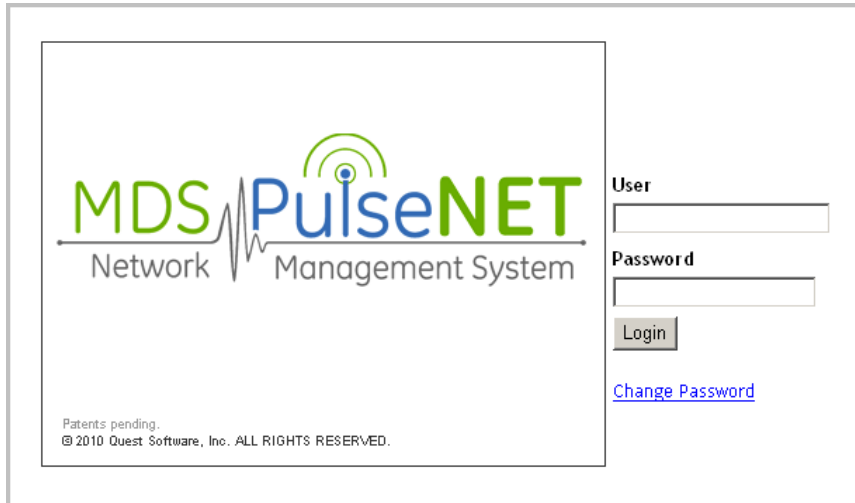
**Note** For a list of browsers supported by PulseNET, see the *PulseNET Release Notes*.

- 2 Navigate to a URL that uses the following syntax:

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

where *<hostname>* is the name of the machine that has a running instance of PulseNET and *<port>* is the http port specified during installation (the default is 8080).

The PulseNET login screen appears.



The screenshot shows the PulseNET login interface. On the left, there is a logo for 'MDS PulseNET Network Management System' with a green pulse line and a signal tower icon. Below the logo, it says 'Patents pending. © 2010 Quest Software, Inc. ALL RIGHTS RESERVED.' To the right of the logo is a login form with fields for 'User' and 'Password', a 'Login' button, and a 'Change Password' link.

- 3 Enter your user name and password on the login screen.
- 4 Click **Login**.

As an administrator, the Administrator Home dashboard is the first dashboard you see.

---

**Note** If you have Administrator-level permissions, you can access advanced dashboards and configuration workflows. Users with the Operator role have permission to access a restricted set of dashboards.

---

*To log in to PulseNET from the GUI:*

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

## Using the Administrator Home Dashboard

The Administrator Home dashboard is the default home page for an administrator. It provides links to other dashboards from which you can perform administrative tasks.

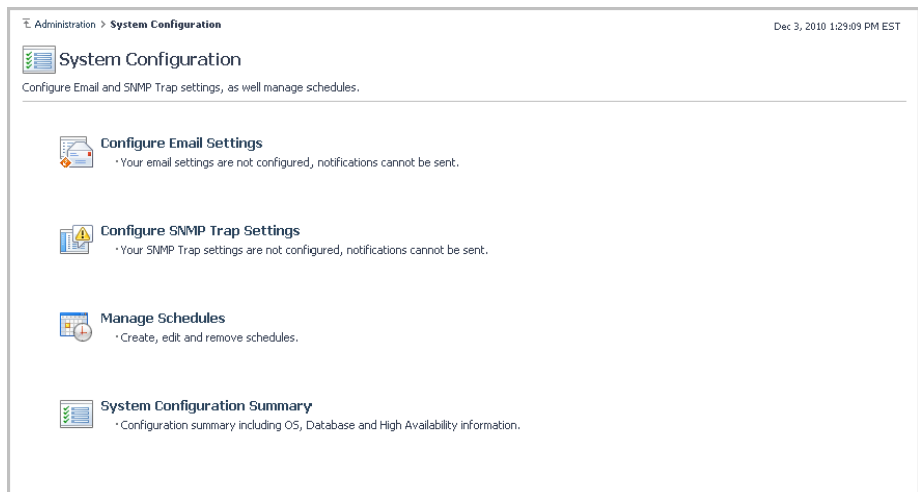
The Administrator Home dashboard provides the following links:

- [Configure System Settings](#)—for configuring system settings. For information, see Chapter 2, “[Configuring System Settings](#)”.
- [Licensing](#)—for requesting, installing, and managing licenses. For information, see Chapter 3, “[Working with Licenses](#)”.
- [Collection Configuration](#)—for configuring SNMP, Dlink, and the sample frequency of data collection. For information, see Chapter 4, “[Collection Configuration](#)”.
- [Device Selection](#)—for discovering, authorizing, and managing devices. For information, see Chapter 5, “[Working with Devices](#)”.
- [Rules and Alerts](#)—for managing rules and rule thresholds. For information, see Chapter 6, “[Working with Rules and Alerts](#)”.
- [Reporting](#)—for generating, scheduling, and managing reports. For information, see Chapter 7, “[Working with Reports](#)”.
- [Users](#)—for creating, configuring, and maintaining PulseNET users. For information, see Chapter 8, “[Working with Users](#)”.
- [Support](#)—for requesting support. For information, see Chapter 9, “[Support](#)”.



# Configuring System Settings

This chapter describes how to use the System Configuration (**Administration > System Configuration**) view.



You can use the System Configuration view for:

- [Email Configuration](#)
- [SNMP Trap Action Configuration](#)
- [Schedule Management](#)
- [System Configuration Summary](#)

## Email Configuration

This section describes how to configure email settings in PulseNET. You configure email settings using the Configure Email Settings dialog box (**Administration > System Configuration > Configure Email Settings**).

Email Configuration Property	Value	Edit	Clear
Mail Server (Name or IP) *	relay.test.com		
Email Sender Address *	katherinew@test.com		
User name to Log in to Server	katherinew@test.com		
User Password	*****		
Mail Server Port	Not Configured		
Mail Protocol	smtp		
Enable Debug Mode?	false		
Enable STARTTLS?	Not Configured		
Enable SSL?	Not Configured		
Global Email Distribution List *	katherinew@test.com		

\* indicates required field

Test Configuration Cancel

The Configure Email Settings dialog box provides the following configurable properties:

Property	Description	Input
Mail Server (Name or IP) <b>Note</b> This is required.	This is the host name for sending emails.	Provide the host name or IP.
Email Sender Address <b>Note</b> This is required.	This is the email address from which PulseNET sends email.	Provide an email address.
User Name to Log in to Server	This is the user name for logging in to the mail server.	Provide a user name.
User Password	This is the user password for logging into the mail server.	Type the user password in both of the two fields provided.
Mail Server Port	This is the mail server port for sending emails.	Provide a port number.
Mail Protocol	This is the transport protocol for emails.	Select smtp or smtps.
Enable Debug Mode?	This is for turning debug mode on or off.	Click the check box to turn on debug mode.
Enable STARTTLS?	This is for enabling or disabling TLS.	Click the check box to enable TLS.
Enable SSL?	This is for enabling or disabling SSL.	Click the check box to enable SSL.
Global Email Distribution List <b>Note</b> This is required.	This is for providing a global email distribution list. Alerts generated by PulseNET are sent to these addresses.	Provide email addresses. Separate email addresses with a comma.

*To configure the properties on the dialog box:*

- 1 Click the **Edit** icon for a property.  
A popup appears.
- 2 Follow the instructions on the popup and click **Save**.
- 3 Repeat steps 1 and 2 for each property you want to configure.
- 4 When you finish configuring the email properties for the server, click **Test Configuration** to make sure the changes you have made are valid.
- 5 To close the Configure Email Settings dialog box, click **Cancel** or the **X** at the top right.

**Note** Cancelling out of this dialog box does not undo the saved changes.

*To clear a property value:*

- Click the **Clear** icon for the property.

---

**Note** If a property is not configured, the Clear icon for the property is disabled.

---

## SNMP Trap Action Configuration

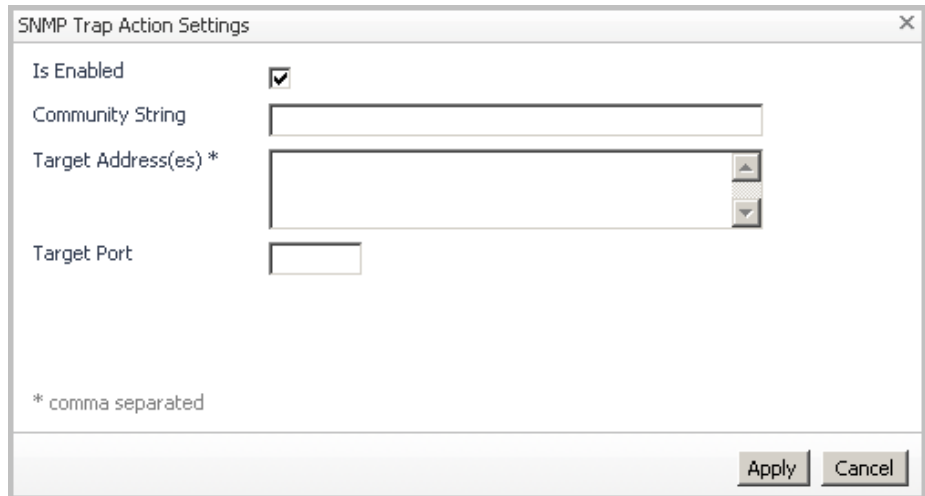
This section describes how to enable SNMP trap actions in PulseNET and how to configure an SNMP trap action to forward an alert for a pre-defined PulseNET rule condition.

---

**Note** MIB files are located in `<INSTALLDIR>/mibs`.

---

You enable SNMP trap actions using the SNMP Trap Action Settings dialog box (**Administration > System Configuration > Configure SNMP Trap Settings**).



The image shows a dialog box titled "SNMP Trap Action Settings". It contains the following fields and controls:

- Is Enabled:** A checked checkbox.
- Community String:** A text input field.
- Target Address(es) \*:** A text input field with a list box icon on the right.
- Target Port:** A text input field.
- \* comma separated:** A note at the bottom left.
- Buttons:** "Apply" and "Cancel" buttons at the bottom right.

*To enable SNMP trap actions:*

- 1 On the SNMP Trap Action Settings dialog box (**Administration > System Configuration > Configure SNMP Trap Settings**), leave the **Is Enabled** check box selected to enable SNMP trap actions.
- 2 Provide a valid community string.
- 3 Provide the IP address(es) for the SNMP trap receiver(s) you want to receive SNMP traps.
- 4 Provide a target port.
- 5 Click **Apply**.

The SNMP trap settings are applied and SNMP trap actions are enabled.

Now that you have enabled SNMP trap actions, you can configure an SNMP trap to be sent to a remote SNMP trap receiver when a rule condition is met. For instructions on how to configure an SNMP trap action for a pre-defined PulseNET rule, see [“Turning an SNMP Trap Action On or Off”](#) on page 82. For instructions on how to configure an SNMP trap action for a custom PulseNET rule, see [“SNMP Trap Actions”](#) on page 96.

## Schedule Management

This section describes how to manage schedules in PulseNET. You manage schedules using the Manage Schedules view (**Administration > System Configuration > Manage Schedules**).

Schedule Name	Next Scheduled Time
Always	Fri Dec 03, 2010 14:32 EST
Business hours	Fri Dec 03, 2010 14:32 EST
Business week	Fri Dec 03, 2010 14:32 EST
Frequent (Test)	Fri Dec 03, 2010 14:35 EST
Hourly	Fri Dec 03, 2010 15:00 EST
End of Day	Fri Dec 03, 2010 17:00 EST
Beginning of the day	Sat Dec 04, 2010 00:00 EST
Weekends	Sat Dec 04, 2010 00:00 EST
Daily Off Hours	Sat Dec 04, 2010 00:00 EST
Daily Database Maintenance	Sat Dec 04, 2010 02:00 EST
Start of Day	Sat Dec 04, 2010 08:00 EST
First day of week	Mon Dec 06, 2010 00:00 EST
Weekly Off Hours	Mon Dec 06, 2010 00:00 EST
Beginning of the week	Mon Dec 06, 2010 00:00 EST
Off-Hours Database Maintenance	Tue Dec 28, 2010 03:00 EST
First day of month	Sat Jan 01, 2011 00:00 EST
Beginning of the month	Sat Jan 01, 2011 00:00 EST
Quarterly Off Hours	Sat Jan 01, 2011 00:00 EST
Monthly Off Hours	Sat Jan 01, 2011 00:00 EST
Create SupportBundle.Schedule	Sat Jan 01, 2011 00:04 EST

You can use the Manage Schedules view (**Administration > System Configuration > Manage Schedules**) for:

- [Copying a Schedule to Create a New Schedule](#)
- [Adding a New Schedule](#)
- [Deleting a Schedule](#)

### Copying a Schedule to Create a New Schedule

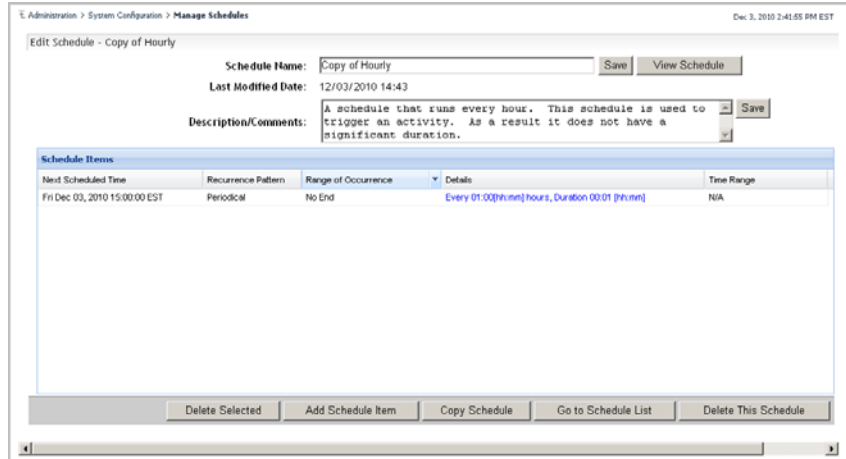
*To copy a schedule with which to create a new schedule:*

- 1 On the Manage Schedules view (**Administration > System Configuration > Manage Schedules**), click the row of the schedule you want to copy.

The schedule is highlighted.

- 2 Click the **Copy Schedule** icon.

The Edit Schedule view appears with a copy of the schedule you selected in the view.



- 3 Change the schedule name and description in the fields provided.
- 4 Click **Save**.
- 5 To edit the details of the schedule, click **Add Schedule Item**.

A view that you can use to edit the details of the schedule appears.

The screenshot shows a web-based form titled "Edit Schedule->Add Schedule Item - Copy of Frequent [Test]". The form is part of the "Administration > System Configuration > Manage Schedules" interface. It contains the following fields and options:

- Schedule Name:** Copy of Frequent [Test]
- Description/Comments:** A schedule that runs very frequently. Primarily used for testing. This schedule is used to trigger an activity. As a result it does not have a significant duration.
- Start Date:** 3 December 2010
- Start Time[h:mm]:** 00 : 00
- Recurrence Pattern:**
  - Once
  - Periodical
  - Daily
  - Weekly
  - Monthly
  - Yearly
- Range of Occurrence:**
  - No End
  - End By Date

End Date: 4 December 2010  
End Time[h:mm]: 00 : 00

At the bottom of the form are three buttons: "Save", "Back", and "Go to Schedule List".

- 6 Use the fields provided to specify new details for the schedule you are creating.
  - Note** At any time you can click **Back** to move to the previous screen.
- 7 When you are finished specifying the new details, click **Save**.  
The new details are added to the schedule.
- 8 Click **Go to Schedule List** to return to the Manage Schedules view.

## Adding a New Schedule

*To add a new schedule:*

- 1 On the Manage Schedules view (**Administration > System Configuration > Manage Schedules**), click **Add Schedule**.

The Create Schedule wizard appears.

The screenshot shows a 'Create Schedule' wizard window. At the top, the title is 'Create Schedule' and the date/time is 'Dec 3, 2010 2:46:23 PM EST'. Below the title bar are three tabs: 'Schedule Name and Description' (which is selected and highlighted), 'Details of Schedule', and 'Schedule Added'. The main content area is titled 'Step 1: Create Schedule - Schedule Name and Description'. It contains two input fields: a text box for 'Schedule Name:' and a larger text area for 'Description/Comments:'. At the bottom right of the main area are two buttons: 'Next' and 'Cancel'. The entire window has a scroll bar at the bottom.

- 2 Type a schedule name and description in the fields provided.
- 3 Click **Next**.

The Details of Schedule view appears.

The screenshot shows a web-based application window titled "Create Schedule". At the top right, it displays the date and time: "Dec 3, 2010 2:53:37 PM EST". Below the title bar, there are three tabs: "Schedule Name and Description", "Details of Schedule" (which is the active tab), and "Schedule Added". The main content area is titled "Step 2: Create Schedule - Details of Schedule".

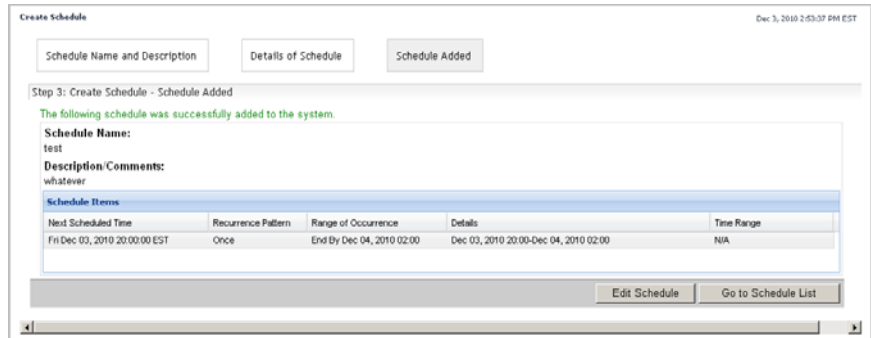
Under the "Details of Schedule" tab, the following fields are visible:

- Schedule Name:** test
- Description/Comments:** whatever
- Start Date:** 3 December 2010
- Start Time(hh:mm):** 00 : 00
- Recurrence Pattern:** A list of radio buttons with "Once" selected. Other options include Periodical, Daily, Weekly, Monthly, and Yearly.
- Range of Occurrence:** Two radio buttons are present. "End By Date" is selected, with "End Time(hh:mm)" set to 00 : 00. The "No End" option is also visible, with an "End Date" of 4 December 2010.

At the bottom of the form, there are three buttons: "Back", "Add", and "Cancel". A scrollbar is visible at the very bottom of the window.

- 4 Use the fields provided to specify the details of the new schedule.  
**Note** At any time you can click **Back** to move to the previous screen.
- 5 When you are finished specifying the details of the schedule, click **Add**.

The Schedule Added view appears. The Schedule Added view displays a summary of the new schedule.



- 6 Click **Go to Schedule List** to return to the Manage Schedules view.

## Deleting a Schedule

*To delete a schedule:*

- 1 On the Manage Schedules view (**Administration > System Configuration > Manage Schedules**), click the row of the schedule you want to delete.

The row is highlighted.

- 2 Click **Delete Selected**.

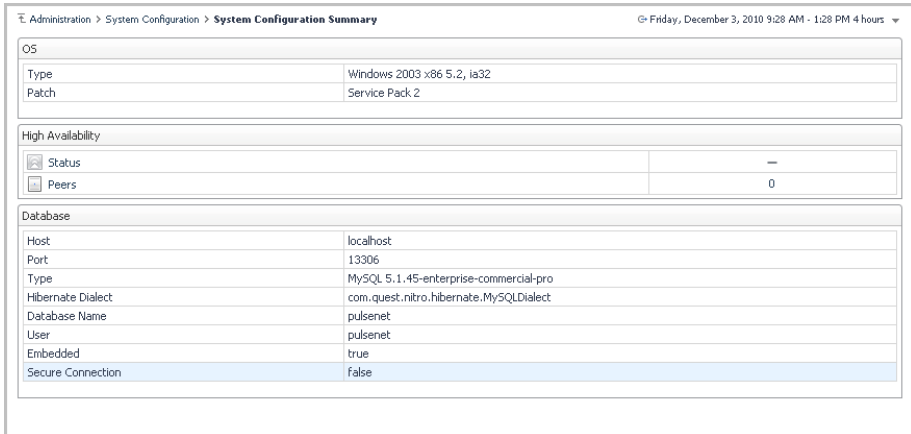
A verification dialog box appears.

- 3 Click **OK**.

The schedule is deleted.

## System Configuration Summary

The System Configuration Summary view (**Administration > System Configuration > System Configuration Summary**) displays various PulseNET configuration details.



Administration > System Configuration > **System Configuration Summary** Friday, December 3, 2010 9:28 AM - 1:28 PM 4 hours

**OS**

Type	Windows 2003 x86 5.2, ia32
Patch	Service Pack 2

**High Availability**

Status	-
Peers	0

**Database**

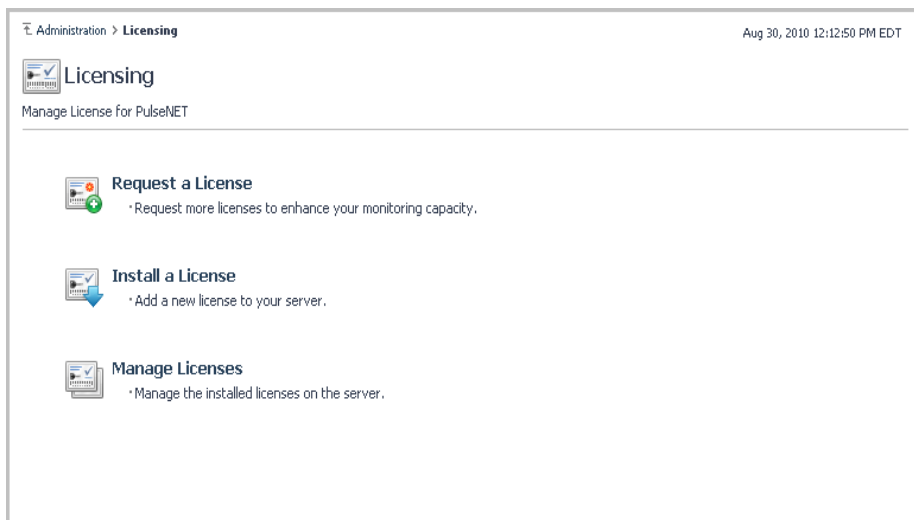
Host	localhost
Port	13306
Type	MySQL 5.1.45-enterprise-commercial-pro
Hibernate Dialect	com.quest.nitro.hibernate.MySQLDialect
Database Name	pulsenet
User	pulsenet
Embedded	true
Secure Connection	false

Click either link on the High Availability panel to view High Availability status or peer information.

# Working with Licenses

This chapter describes how use the Licensing view (**Administration > Licensing**) for:

- [Requesting a License](#)
- [Installing a License](#)
- [Managing Licenses](#)



## Requesting a License

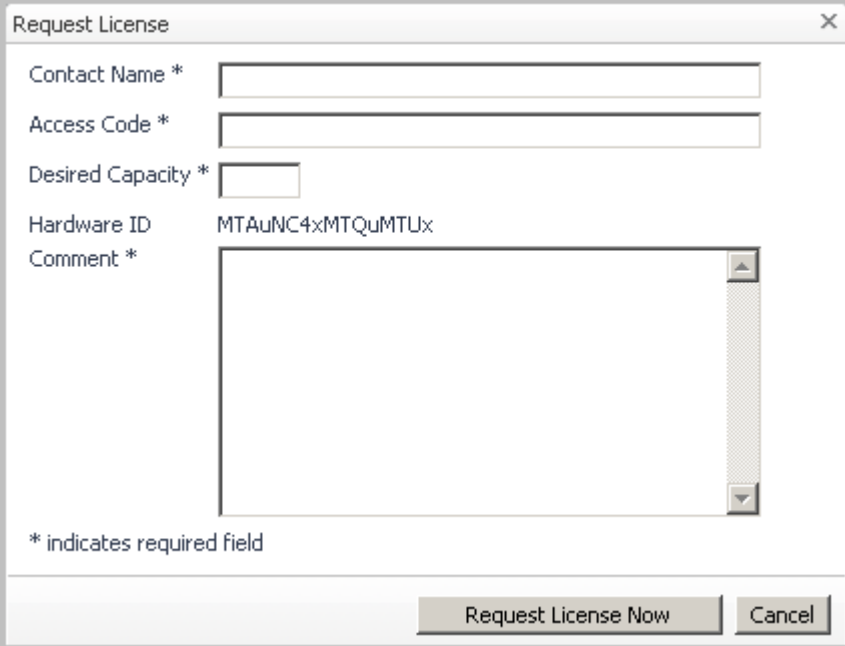
As a PulseNET administrator, you can request PulseNET licenses.

A license provides PulseNET with capacity so that it can authorize and monitor devices.

*To request a PulseNET license:*

- 1 From the Licensing view, click **Request a License**.

A dialog box appears requesting input.



The image shows a dialog box titled "Request License" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Contact Name \***: A text input field.
- Access Code \***: A text input field.
- Desired Capacity \***: A text input field.
- Hardware ID**: A text field containing the value "MTAuNC4xMTQuMTUx".
- Comment \***: A large text area with a vertical scrollbar.

At the bottom left of the dialog, there is a note: "\* indicates required field". At the bottom right, there are two buttons: "Request License Now" and "Cancel".

- 2 Enter your name in the Contact Name field.
- 3 Enter your access code in the next field. This code is saved; you do not have to re-type it for subsequent license requests.
- 4 Enter the desired capacity (remotes and access points) of the license. For example, if you want to be able to monitor 100 access points and 300 remotes, enter 400.
- 5 Enter any comments you have in the Comment field.
- 6 Click **Next**.

An e-mail requesting the license is sent automatically through PulseNET to GE. If you have not configured PulseNET e-mail settings, PulseNET opens the license request for you to send through an external email client.

**Note** For information about configuring PulseNET e-mail settings, see Chapter 2, “Configuring System Settings”.

If the request is granted, the new license is sent to you within one business day.

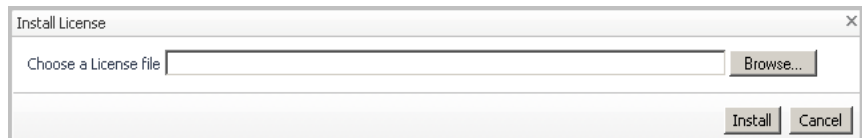
## Installing a License

The following procedure describes how to install a license.

*To install a license:*

- 1 From the Licensing view, click **Install a License**.

A dialog box appears prompting you to provide a License file.



- 2 If you know the name and location of the license file, enter it in the field provided. If you do not know the name of the license file, click **Browse...** to locate it.

**Note** The file must be on the machine where the browser is running.

- 3 Click **Install**.

If the license is valid, it is installed on the PulseNET system. Otherwise, you receive a message stating that the license file is invalid.

**Note** If you have a license installed that is about to expire, you are asked if you want to migrate the existing authorized devices to the new license. If you want to migrate authorized devices to the new license, click **Migrate**. For instructions on how to migrate authorized devices to a new license, see “[Migrate Authorized Devices from an Expiring License to a New License](#)” on page 34.

Installed licenses appear in the Manage Licenses list (**Administration > Licensing > Manage Licenses**).

## Managing Licenses

Installed licenses are listed in the Manage Licenses view (**Administration > Licensing > Manage Licenses**).

Status	Serial Number	Monitoring Capacity			Expires on
		Total	Used	Free	
	555-12345	500	25	475	Aug 17, 292278994 2:12:55 AM

In the Manage Licenses view, you can:

- [Sort the Manage Licenses List](#)
- [Search for an Installed License](#)
- [Filter the Manage Licenses List](#)
- [Install a New License](#)
- [Delete an Installed License](#)
- [Migrate Authorized Devices from an Expiring License to a New License](#)

### Sort the Manage Licenses List

To sort the Manage Licenses list by a particular column heading, click that column heading. An arrow beside that column heading indicates the order (ascending or descending) in which the users are sorted.

### Search for an Installed License

Use the Search tool at the top right of the Manage Licenses list to search for a specific installed license. For instructions on how to use the Search tool, see “Working with Tables” in the *PulseNET Quick Start Guide*.

## Filter the Manage Licenses List

Use the Search tool at the top right of the Manage Licenses list to filter the list. For instructions on how to use the Search tool, see “Working with Tables” in the *PulseNET Quick Start Guide*.

## Install a New License

To install a new license, click Install a License at the top left of the Manage Licenses view and then follow the instructions in “[Installing a License](#)” on page 31.

## Delete an Installed License

*To delete an installed license:*

- 1 Click the check box next to the license’s icon to select the license.  
**Note** The check box is only enabled if the license is expiring (that is, if the license is two weeks or less from its expiration date).  
The Delete icon becomes enabled.
- 2 Click the **Delete** icon.  
A dialog box appears and asks you if you are sure.
- 3 Click **Delete**.

## Migrate Authorized Devices from an Expiring License to a New License

---

**Important** To migrate authorized devices from an expiring licence to a new license, you must have a new license installed. For instructions on how to install a new license, see [“Installing a License”](#) on page 31.

---

*To migrate authorized devices to a new license:*

- 1 Click the number in the Used column (under the Monitoring Capacity heading) for the expiring licence from which you want to migrate devices.

**Note** This functionality is only available if the license is expiring (that is, if the license is two weeks or less from its expiration date).

The Migration dialog box appears.

- 2 In the column at the left, click the check boxes for the devices you want to migrate.

To select all of the devices, click the check box at the top of the column.

- 3 Click **Migrate Now**.

A confirmation dialog box appears.

- 4 Click **Proceed**.

The authorized devices you selected are migrated to the new license.

## License Order when Authorizing Devices

If your environment has a mix of active (the expiry date is more than fourteen days away) and expiring (the expiry date is in fourteen days or less) licenses, the following order is used by PulseNET when authorizing devices:

- 1 the active license pool with remaining capacity that is expiring earliest, followed by the active license pool with remaining capacity that is expiring next, until all active licenses are exhausted
- 2 the expiring license pool with remaining capacity that is expiring earliest, followed by the expiring license pool with remaining capacity that is expiring next, until all expiring licenses are exhausted

## Example 1

There are two active licenses: one with an expiry date of July 1st and remaining capacity for ten devices and another with an expiry date of August 1st and remaining capacity for twenty devices.

Today is May 20th and you want to authorize fifteen devices.

PulseNET will consume license capacity in the following order:

- 1 the ten available on the July 1st license
- 2 five of the twenty available on the August 1st license

The July 1st license will then have no remaining capacity, and the August 1st license will have remaining capacity for fifteen devices.

## Example 2

Like in Example 1, there are two active licenses: one with an expiry date of July 1st and remaining capacity for ten devices and another with an expiry date of August 1st and remaining capacity for twenty devices.

There are also two expiring licenses: one with an expiry date of May 21st and remaining capacity for ten devices and another with an expiry date of May 22nd and remaining capacity for ten devices.

Today is May 20th and you want to authorize forty devices.

PulseNET will consume license capacity in the following order:

- 1 the ten available on the July 1st license
- 2 the twenty available on the August 1st licence
- 3 the ten available on the May 21st license

The July 1st, August 1st, and May 21st licenses will then have no remaining capacity. The May 22nd license will still have remaining capacity for ten devices.



# Collection Configuration

This chapter describes how to use the Collection Configuration view (**Administration > Collection Configuration**) for:

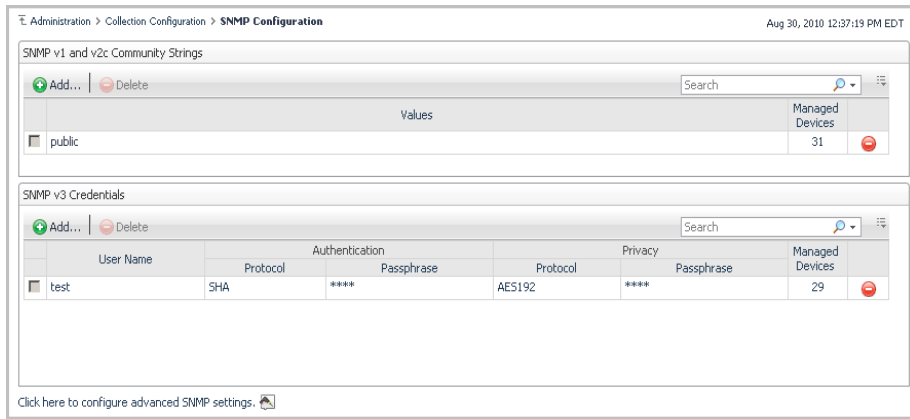
- [SNMP Configuration](#)
- [Dlink Configuration](#)
- [Collection Management](#)

The screenshot shows a web application interface for 'Collection Configuration'. At the top left, there is a breadcrumb trail: 'Administration > Collection Configuration'. At the top right, the date and time are displayed: 'Dec 2, 2010 4:41:50 PM EST'. Below the breadcrumb, there is a header section with a blue icon and the text 'Collection Configuration'. Underneath the header, there is a sub-header: 'Configure credentials used in discovery as well as collection parameters.' The main content area contains three configuration options, each with a small icon and a description:

- SNMP Configuration**: \*Configure your SNMP credentials for discovery and data collection.
- Dlink Configuration**: \*Configure your Dlink settings for discovery and data collection.
- Collection Management**: \*Configure the frequency that your data is collected.

## SNMP Configuration

This section describes how to use the SNMP Configuration view (**Administration > Collection Configuration > SNMP Configuration**).



Administration > Collection Configuration > SNMP Configuration Aug 30, 2010 12:37:19 PM EDT

SNMP v1 and v2c Community Strings

Add... Delete Search

Values	Managed Devices
public	31

SNMP v3 Credentials

Add... Delete Search

	User Name	Authentication		Privacy		Managed Devices	
		Protocol	Passphrase	Protocol	Passphrase		
<input type="checkbox"/>	test	SHA	****	AES192	****	29	<input type="checkbox"/>

[Click here to configure advanced SNMP settings.](#)

From the SNMP Configuration view, you can:

- [Add an SNMP v1 or v2c Community String](#)
- [Delete an SNMP v1 or v2c Community String](#)
- [Add SNMP v3 Credentials](#)
- [Edit SNMP v3 Credentials](#)
- [Delete SNMP v3 Credentials](#)
- [Configure Advanced SNMP Settings](#)
- [Migrate Devices from One Community String or Set of Credentials to Another](#)
- [Sort an SNMP Table](#)
- [Search for an SNMP Community String or Set of Credentials](#)
- [Filter an SNMP Table](#)

## Add an SNMP v1 or v2c Community String

*To add an SNMP v1 or v2c community string:*

- 1 In the SNMP v1 and v2c Community Strings table, click **Add...**  
**Note** The **Add...** button is disabled if neither SNMP v1 or SNMP v2c are selected for use in the advanced SNMP settings. For information about configuring advanced SNMP settings, see [“Configure Advanced SNMP Settings”](#) on page 42.  
A dialog box appears prompting you to provide a community string.
- 2 Enter a community string and click **Save**.

## Delete an SNMP v1 or v2c Community String

*To delete an SNMP v1 or v2c community string:*

- 1 In the SNMP v1 and v2c Community Strings table, click the check box next to the community string you want to delete.  
The Delete button becomes enabled.
- 2 Click **Delete**.

Alternatively, you can click the Delete icon in the row for the community string you want to delete.

---

**Note** It is not possible to delete a community string that is being used to manage devices.

---

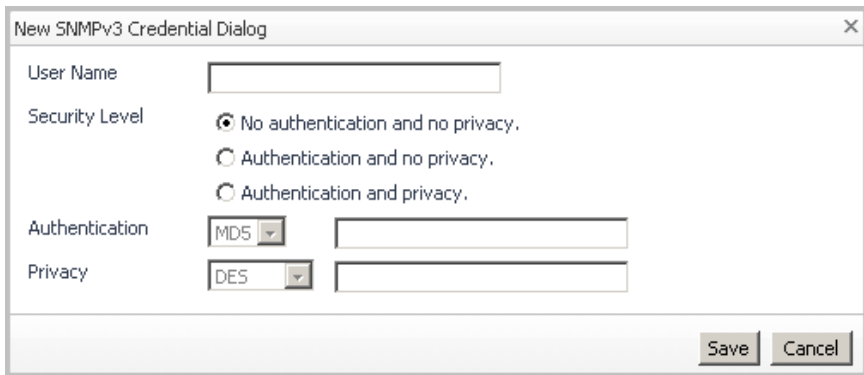
## Add SNMP v3 Credentials

To add SNMP v3 credentials:

- 1 In the SNMP v3 Credentials table, click, click **Add...**

**Note** The **Add...** button is disabled if SNMP v3 is not selected for use in the advanced SNMP settings. For information about configuring advanced SNMP settings, see [“Configure Advanced SNMP Settings”](#) on page 42.

A dialog box appears prompting you to provide SNMP v3 credentials.



The image shows a dialog box titled "New SNMPv3 Credential Dialog". It contains the following fields and options:

- User Name:** A text input field.
- Security Level:** Three radio button options:
  - No authentication and no privacy.
  - Authentication and no privacy.
  - Authentication and privacy.
- Authentication:** A dropdown menu set to "MD5" and an adjacent text input field for a passphrase.
- Privacy:** A dropdown menu set to "DES" and an adjacent text input field for a passphrase.

At the bottom right of the dialog are "Save" and "Cancel" buttons.

- 2 Enter a name in the User Name field.

**Note** At present, PulseNET does not support multiple SNMP v3 credentials with the same user name but different passwords.

- 3 Select a security level:

- a No authentication and no privacy** indicates that the identity of the sender is not verified.
- b Authentication and no privacy** indicates that the identity of the sender is verified.
- c Authentication and privacy** indicates that the identity of the sender is verified and the information is encrypted.

- 4 If the security level requires authentication, specify an authentication protocol and passphrase.
- 5 If the security level requires privacy, specify a privacy protocol and passphrase.
- 6 Click **Save**.

## Edit SNMP v3 Credentials

*To edit SNMP v3 credentials:*

- 1 In the SNMP v3 Credentials table, click the user name corresponding to the SNMP v3 credentials you want to edit.

A dialog box appears prompting you to edit the SNMP v3 credentials.

- 2 Edit the credentials.

For information about the credentials, see “[Add SNMP v3 Credentials](#)” on page 40.

- 3 Click **Save**.

## Delete SNMP v3 Credentials

*To delete SNMP v3 credentials:*

- 1 In the SNMP v3 Credentials table, click the check box next to the set of credentials you want to delete.

The Delete button becomes enabled.

- 2 Click **Delete**.

Alternatively, you can click the Delete icon in the row for the set of credentials you want to delete.

---

**Note** It is not possible to delete a set of credentials that is being used to manage devices.

---

## Configure Advanced SNMP Settings

To configure advanced SNMP settings:

- 1 Click the **advanced SNMP settings** link at the bottom left of the SNMP Configuration view.

The Advanced SNMP Settings dialog box appears.

On the Advanced SNMP Settings dialog box, you can configure the following parameters:

Parameter	Definition	Default
SNMP Usage	This is the version of SNMP that PulseNET uses for communication. Select the check boxes associated with the versions you want your PulseNET system to use.	All
SNMP Target Port	This is the port used for SNMP communication.	161
SNMP Timeout (ms)	This the length of time PulseNET will wait for a device to respond to an SNMP request.	7000

Parameter	Definition	Default
ICMP Timeout (ms)	This is the length of time PulseNET will wait for a device to respond to an ICMP request.	5000
SNMP Worker Threads	This is the number of threads the system uses for SNMP. This value will need to be increased as the number of devices PulseNET is monitoring increases. Additional threads consume CPU and memory, so caution is required when increasing this value.	10
ICMP Worker Threads	This is the number of threads the system uses for ICMP. This value will need to be increased as the number of devices PulseNET is monitoring increases. Additional threads consume CPU and memory, so caution is required when increasing this value.	10

- 2 Make changes to one or more of the settings.
- 3 Click **Save**.

## Migrate Devices from One Community String or Set of Credentials to Another

*To migrate devices:*

- 1 Click in the Managed Devices column of the row for the community string or credential from which you want to migrate devices.

A dialog box appears prompting you to select the devices to be migrated.

Migrate Credential Wizard

Select radios

Search

<input type="checkbox"/>	Device Name	Device Location	Device Contact
<input type="checkbox"/>	WALSEN-1822INet-R	Apt 3609 75 Thorndcliffe Park Dr	Todd Brown (500-063-0815)
<input type="checkbox"/>	MONONA-6538MR-R	Apt 3609 75 Thorndcliffe Park Dr	Anna Nelson (146-241-2722)
<input type="checkbox"/>	SOUTH-2546MR-R	Apt 3609 75 Thorndcliffe Park Dr	Anthony Cain (358-077-2419)
<input type="checkbox"/>	WALSEN-7741INet-R	Apt 3609 75 Thorndcliffe Park Dr	Mary Smith (581-759-1707)
<input type="checkbox"/>	BETHEL-6439MR-R	Apt 3609 75 Thorndcliffe Park Dr	Betty Harper (863-452-6040)
<input type="checkbox"/>	WALSEN-1327INet-R	Apt 3609 75 Thorndcliffe Park Dr	Benjamin Maddox (998-375-8791)
<input type="checkbox"/>	OAKESD-4492MR-R	Apt 3609 75 Thorndcliffe Park Dr	Dorothy Reeves (949-357-0422)
<input type="checkbox"/>	CLARIO-5745INet-R	Apt 3609 75 Thorndcliffe Park Dr	Bernard Riley (135-825-1042)
<input type="checkbox"/>	WALSEN-AP2-B	Apt 3609 75 Thorndcliffe Park Dr	Anita Mathews (201-442-6754)
<input type="checkbox"/>	HINESB-4385INet-R	Apt 3609 75 Thorndcliffe Park Dr	Jacqueline Sosa (752-213-9911)
<input type="checkbox"/>	HAWKIN-9443INet-R	Apt 3609 75 Thorndcliffe Park Dr	Brian Hunt (119-361-6217)
<input type="checkbox"/>	WALSEN-3195INet-R	Apt 3609 75 Thorndcliffe Park Dr	Albert Rodriguez (228-959-8752)

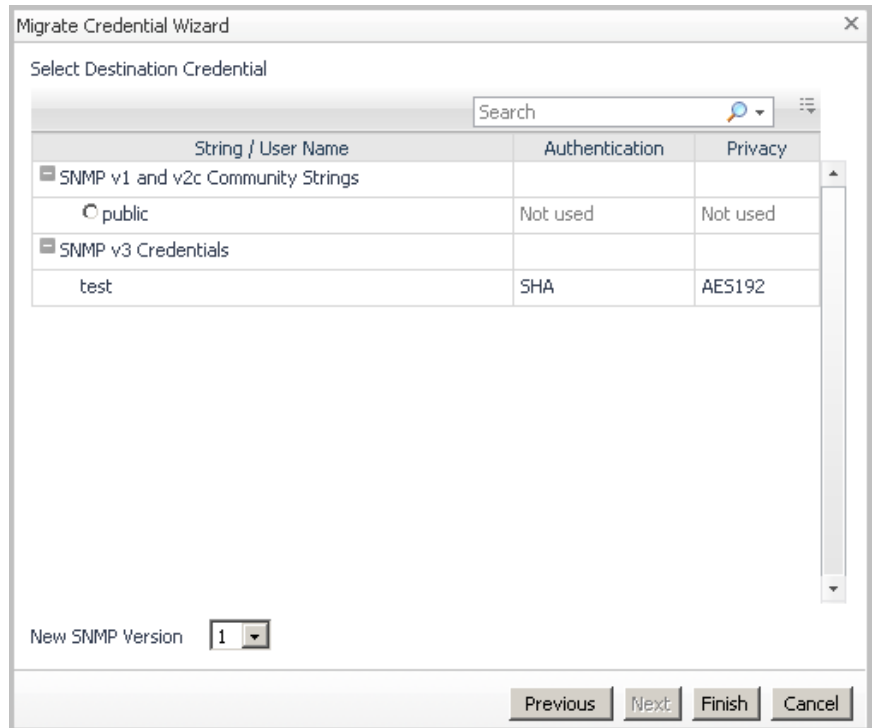
Previous Next Finish Cancel

- 2 In the column at the left, click the check boxes for the devices you want to migrate.

To select all of the devices, click the check box at the top of the column.

**3 Click Next.**

You are prompted to either select a destination community string or set of credentials or to select a new SNMP version.

**4 Select a destination community string or set of credentials or select a new SNMP version.****5 Click Finish.**

## Sort an SNMP Table

To sort an SNMP table by a particular column heading, click that column heading. An arrow beside that column heading indicates the order (ascending or descending) in which the table is sorted.

## Search for an SNMP Community String or Set of Credentials

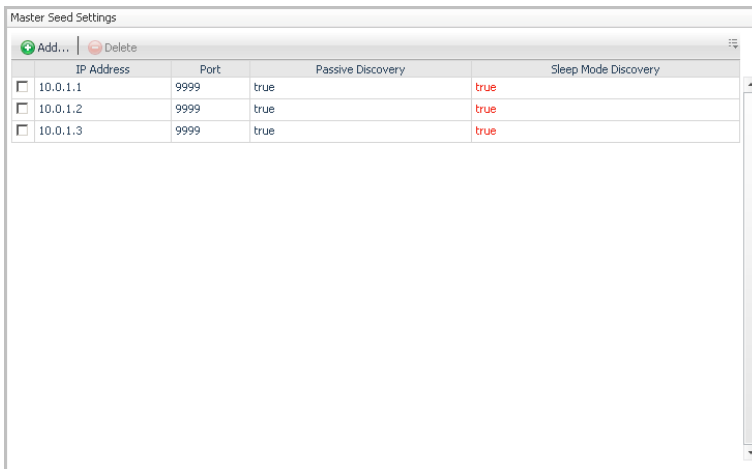
Use the Search tool at the top right of the appropriate table to search for a specific SNMP Community String or set of credentials. For instructions on how to use the Search tool, see “Working with Tables” in the *PulseNET Quick Start Guide*.

## Filter an SNMP Table

Use the Search tool at the top right of an SNMP table to filter the list. For instructions on how to use the Search tool, see “Working with Tables” in the *PulseNET Quick Start Guide*.

# Dlink Configuration

This section describes how to use the Dlink Configuration view (**Administration > Collection Configuration > Dlink Configuration**).



	IP Address	Port	Passive Discovery	Sleep Mode Discovery
<input type="checkbox"/>	10.0.1.1	9999	true	true
<input type="checkbox"/>	10.0.1.2	9999	true	true
<input type="checkbox"/>	10.0.1.3	9999	true	true

From the Dlink Configuration view, you can:

- [Add a Dlink Master Seed](#)
- [Edit Dlink Master Seed Settings](#)
- [Delete a Dlink Master Seed](#)

- [Configure Advanced Dlink Settings](#)
- [Sort a Master Seed Table](#)
- [Search for a Master Seed](#)
- [Filter a Master Seed Table](#)

## Add a Dlink Master Seed

*To add a Dlink Master Seed:*

- 1 In the Master Seed Settings table, click **Add...**  
A dialog box appears prompting you to provide an IP address and a port for the terminal server associated with the master seed.
- 2 Enter the IP address and port in the appropriate fields.
- 3 Leave the Passive Discovery check box selected if you want passive discovery to be the default for this seed. Clear the check box if you want active discovery to be the default.

**Warning:** The choice between active and passive discovery can significantly affect the length of time the discovery process takes and the impact the discovery process has on your network.

Passive polling requests information from the master and waits for the master to provide the details.

Active polling demands an immediate response from the master and requires deliberate requests from the master to the remotes it is managing.

If the application polling in your system is of a relatively high frequency, passive polling may be more efficient.

- 4 Leave the Sleep Mode Discovery check box selected if the radio network is in sleep mode. Clear the check box if the radio network is not in sleep mode.
- 5 Click **Save**.  
If the Sleep Mode Discovery check box is selected, a warning dialog box appears. Click **Continue**.

The master seed is added.

## Edit Dlink Master Seed Settings

*To edit Dlink master seed settings:*

- 1 In the Master Seed Settings table, click the IP address of the terminal server associated with the master seed for which you want to edit settings.  
A dialog box appears prompting you to edit the master seed settings.
- 2 Edit the settings.  
For information about the settings, see “[Add a Dlink Master Seed](#)” on page 47.
- 3 Click **Save**.

## Delete a Dlink Master Seed

*To delete a Dlink master seed:*

- 1 In the Master Seed Settings table, select the check box that corresponds to the master seed you want to delete.  
The Delete button becomes enabled.
- 2 Click **Delete**.

---

**Note** It is not possible to delete a master seed that is the parent of other PulseNET-monitored devices.

---

## Configure Advanced Dlink Settings

To configure advanced Dlink settings:

- 1 Click the **advanced Dlink settings** link at the bottom left of the Dlink Configuration view.

The Dlink Advanced Configuration dialog box appears.

Dlink All Device Advanced Setting Panel	
DLink Active Monitoring Request Timeout (ms)	2000
DLink Active Discovery Request Timeout (ms)	2000
DLink Passive Discovery Request Timeout (ms)	3000
DLink Active Monitoring Request Max Retries (count)	1
DLink Active Discovery Request Max Retries (count)	0
DLink Worker Threads (count)	10
DLink Use Passive Discovery	<input checked="" type="checkbox"/>
DLink Active Discovery Min Unit Address (count)	0
DLink Active Discovery Max Unit Address (count)	9999
DLink Passive Discovery Repeats (count)	2
DLink Active Request Gap (ms)	2000
DLink Sleep Mode Discovery Wakeup Gap (ms)	100
DLink Sleep Mode Discovery Wakeup Iterations (count)	30
DLink Sleep Mode Discovery Timeout (ms)	100
DLink Sleep Mode Discovery Sleep Inhibit Timeout (ms)	655350
DLink Sleep Mode Monitoring Wakeup Gap (ms)	100

Save Cancel

Use the Dlink Advanced Configuration dialog box to configure the following parameters:

Parameter	Definition	Default
Dlink Active Monitoring Request Timeout (ms)	This is the length of time PulseNET will wait for a device to respond to a Dlink monitoring request.	2000
Dlink Active Discovery Request Timeout (ms)	This is the length of time PulseNET will wait for a device to respond to a Dlink active discovery request.	2000
Dlink Passive Discovery Request Timeout (ms)	This is the length of time PulseNET will wait for a device to respond to a Dlink passive discovery request.	60000
Dlink Active Monitoring Request Max Retries (count)	This is the number of times PulseNET will retry a monitoring request.	1
Dlink Active Discovery Request Max Retries (count)	This is the number of times PulseNET will retry a discovery request.	0
Dlink Worker Threads (count)	This is the number of threads the system uses for Dlink. This value will need to be increased as the number of devices PulseNET is monitoring increases. Additional threads consume CPU and memory, so caution is required when increasing this value.	10
Dlink Use Passive Discovery	This is the type of discovery PulseNET uses when communicating with a Dlink device directly, rather than through a master seed. PulseNET uses either passive or active discovery.  <b>Note</b> For passive discovery of devices to run properly, the firmware revision on the devices must support passive discovery.	Check box

Parameter	Definition	Default
Dlink Active Discovery Min Unit Address (count)	This is the lowest unit address in the range of unit addresses you want PulseNET to search through when performing discovery.	0
Dlink Active Discovery Max Unit Address (count)	This is the highest unit address in the range of unit addresses you want PulseNET to search through when performing discovery.	9999
Dlink Passive Discovery Repeats (count)	This is the number of additional times, in succession, you want PulseNET to repeat the discovery.	2
Dlink Active Request Gap (ms)	This is the length of time PulseNET will wait between making active requests for data to a Dlink device.	2000
DLink Sleep Mode Discovery Wakeup Gap (ms)	This is the length of time PulseNET will wait between sending wakeup messages to a Dlink device in sleep mode when doing discovery.	100
DLink Sleep Mode Discovery Wakeup Iterations (count)	This is the number of wakeup messages PulseNET will send to a Dlink device in sleep mode when doing discovery.	30
DLink Sleep Mode Discovery Timeout (ms)	This is the length of time PulseNET will wait for a Dlink device to respond after sending a discovery request.	100
DLink Sleep Mode Discovery Sleep Inhibit Timeout (ms)	This is the maximum length of time PulseNET will keep a sleep-mode Dlink network awake for discovery. PulseNET will wake the network again if discovery has not finished in this amount of time.	655350
DLink Sleep Mode Monitoring Wakeup Gap (ms)	This is the length of time PulseNET will wait between sending wakeup messages to a Dlink device in sleep mode when doing discovery.	100

Parameter	Definition	Default
DLink Sleep Mode Monitoring Wakeup Iterations (count)	This is the number of wakeup messages PulseNET will send to a Dlink device in sleep mode when doing discovery.	30
DLink Sleep Mode Monitoring Timeout (ms)	This is the length of time PulseNET will wait for a Dlink device to respond after sending a collection request.	100
DLink Sleep Mode Monitoring Sleep Inhibit Timeout (ms)	This is the maximum length of time PulseNET will keep a sleep-mode Dlink device awake to collect data. PulseNET will wake the device again if collection has not finished in this amount of time.	655350
Dlink TCP Port	This is the port PulseNET uses when communicating with a Dlink IP device directly, rather than through a master seed.	9999
ICMP Timeout (ms)	This is the length of time PulseNET will wait for an IP device to respond to an ICMP request.	5000
HTTP Timeout (ms)	This is the length of time PulseNET will wait for an IP device to respond to an HTTP request.	5000

- 2 Make changes to one or more of the settings.
- 3 Click **Save**.

## Sort a Master Seed Table

To sort a master seed table by a particular column heading, click that column heading. An arrow beside that column heading indicates the order (ascending or descending) in which the table is sorted.

## Search for a Master Seed

Use the Search tool at the top right of the appropriate table to search for a specific master seed. For instructions on how to use the Search tool, see “Working with Tables” in the *PulseNET Quick Start Guide*.

## Filter a Master Seed Table

Use the Search tool at the top right of a master seed table to filter the list. For instructions on how to use the Search tool, see “Working with Tables” in the *PulseNET Quick Start Guide*.

# Collection Management

As a PulseNET administrator, you can use the Collection Scheduler (**Administration > Collection Configuration > Collection Management**) to configure the sample frequency of data collection.

The screenshot displays the 'Collection Management' page in PulseNET. It features three tables, each with a search bar and a refresh icon. The top table is for MDS Devices, the middle for LAN Devices, and the bottom for DLink Devices.

Type	Role	Schedule Configuration	Performance	Interval	Availability
Mercury 3650 Access Points	AccessPoint		Every 5 minutes	Every 1 minutes	Every 1 minutes
Mercury 900 Access Points	AccessPoint		Every 5 minutes	Every 1 minutes	Every 1 minutes
Mercury 1800 Access Points	AccessPoint		Every 5 minutes	Every 1 minutes	Every 1 minutes
INET 900 Access Points	AccessPoint		Every 5 minutes	Every 1 minutes	Every 1 minutes
INET-II 900 Access Points	AccessPoint		Every 5 minutes	Every 1 minutes	Every 1 minutes
Mercury 3650 Remotes	Remote		Every 5 minutes	Every 1 minutes	Every 1 minutes
Mercury 900 Remotes	Remote		Every 5 minutes	Every 1 minutes	Every 1 minutes
Mercury 1800 Remotes	Remote		Every 5 minutes	Every 1 minutes	Every 1 minutes
INET 900 Remotes	Remote		Every 5 minutes	Every 1 minutes	Every 1 minutes
INET-II 900 Remotes	Remote		Every 5 minutes	Every 1 minutes	Every 1 minutes
Intrepids	Backhaul		Every 5 minutes	Every 1 minutes	Every 1 minutes

Type	Schedule Configuration	Performance	Interval	CPU & Memory
LAN Devices		Every 815 minutes	Every 2 minutes	Every 2 minutes
Cisco Devices		Every 15 minutes	Every 2 minutes	Every 2 minutes

Type	Schedule Configuration	Performance	Interval	Schedule Configuration Enable
DLink Devices		Every 15 minutes	Every 15 minutes	

The Collection Scheduler lists the devices that PulseNET can monitor.

You can configure the sample frequency of data collection for each.

---

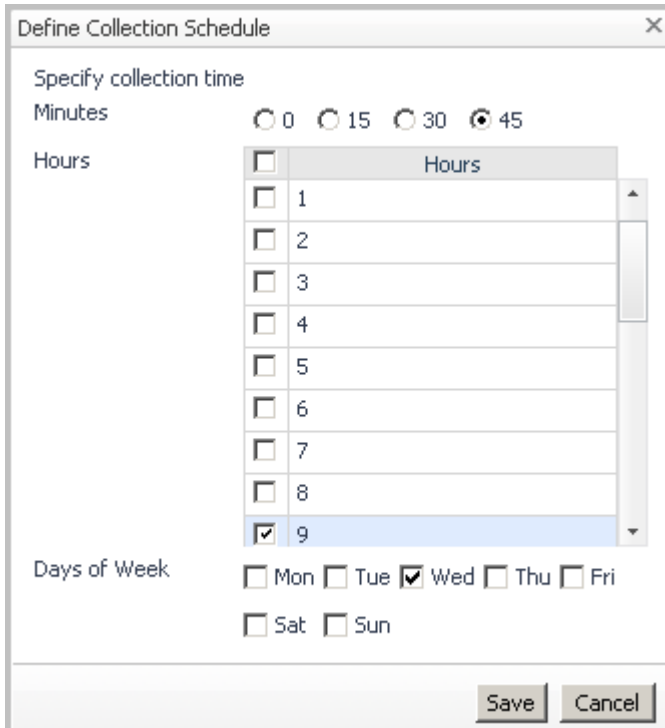
**Important** When configuring data collection frequency for a device, it is important to understand how data collection frequency for performance or availability information and trigger delay values together affect the raising of alerts. For detailed information about this interdependency, see [“Trigger Delay Values and Data Collection Frequency”](#) on page 56.

---

*To configure the collection schedule of configuration data for a device:*

- 1 Click the Schedule Configuration icon for the type of device for which you want to configure the collection schedule.

The Define Collection Schedule dialog box appears.



The dialog box titled "Define Collection Schedule" has a close button (X) in the top right corner. It contains the following sections:

- Specify collection time**
  - Minutes:** Four radio buttons are present: 0, 15, 30, and 45. The 45-minute option is selected.
  - Hours:** A list box with a scroll bar and a "Hours" header. It contains checkboxes for hours 1 through 9. The checkbox for hour 9 is checked.
- Days of Week:** Seven checkboxes are present: Mon, Tue, Wed, Thu, Fri, Sat, and Sun. The checkbox for Wed is checked.

At the bottom right of the dialog box are two buttons: "Save" and "Cancel".

- a Specify the minute of the hour for collection by clicking the appropriate radio button. For example, 15 means 15 minutes after the hour.

**b** Specify the hour(s) for collection by checking the hour(s). For example, 7 means 7 a.m.

**c** Specify the day(s) of the week for collection by checking the day(s).

For example (see image above), if you click 45 for Minutes, 9 for Hours, and Wed, PulseNET will collect data at 9:45 a.m. every Wednesday.

**2** Click **Save**.

*To specify the interval for performance collection for a device:*

**1** Click in the Performance column of the row for the device type for which you want to specify the interval.

A dialog box appears.

**2** Specify the interval.

**3** Click **Save**.

*To specify the interval for availability collection for a device:*

---

**Note** This is not available for Dlink or LAN devices.

---

**1** Click in the Availability column of the row for the device type for which you want to specify the interval.

A dialog box appears.

**2** Specify the interval.

**3** Click **Save**.

*To disable schedule configuration for Dlink devices:*

---

**Note** If you disable schedule configuration for Dlink devices, up time is not collected. Therefore, soon after the device is authorized, the initial up time value reported for the device no longer applies.

---

**1** Click in the Schedule Configuration Enable column of the Dlink Devices row.  
A confirmation dialog appears.

**2** Click **Yes**.

Schedule configuration for Dlink devices is disabled.

Once disabled, to enable schedule configuration for Dlink devices, follow the same steps above.

---

**Important** If you disable schedule configuration for Dlink devices and then later enable it, the collection schedule returns to the default collection schedule. That is, any previous collection schedule you configured is not retained.

---

## Trigger Delay Values and Data Collection Frequency

A trigger delay value is the number of consecutive times a certain threshold must be met to cause a rule to raise the corresponding alert (warning, critical, or failure). For information about rules and alerts, see “[Working with Rules and Alerts](#)” on page 77.

The collection frequency is the frequency with which PulseNET polls a device for a certain type of information (configuration, performance, or availability).

It is important to understand how trigger delay values and data collection frequency for performance or availability information together affect the raising of alerts.

The following example illustrates this interdependency.

### Example

For a particular device, the signal-to-noise ratio (SNR) change for the warning alert is set to 2 dB with a trigger delay value of 4. This means that if the 2 dB threshold is met 4 collections in a row for that device, a warning alert is raised.

The collection frequency for the performance information of the device is set to every 5 minutes.

With this configuration, an SNR change warning alert, if required, will be raised 15 minutes after the first time the 2 dB threshold is noticed by PulseNET.

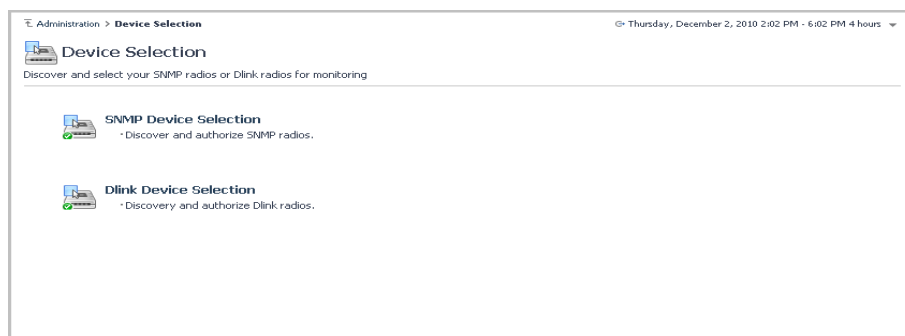
If you change the collection frequency to 1 hour, an SNR change warning alert, if required, will be raised 3 hours after the first time the 2 dB threshold is noticed.

If the collection frequency remains set to every 5 minutes, and you change the trigger delay value to 6, an SNR change warning alert, if required, will be raised 25 minutes after the first time the 2 dB threshold is noticed.

# Working with Devices

This chapter describes how to use the Device Selection view (**Administration > Device Selection**) for:

- [Discovering SNMP Devices](#)
- [Discovering Dlink Devices](#)
- [Authorizing Devices](#)
- [Configuring Access Point Failover](#)
- [Creating and Managing Maintenance Windows](#)
- [Decommissioning a Monitored Device](#)
- [Managing Devices](#)



## Discovering SNMP Devices

Perform discovery to find the devices you want PulseNET to monitor.

*To discover devices:*

- 1 In the Device Selection view (**Administration > Device Selection**), click **SNMP Device Selection**.  
The SNMP Device Selection view appears.
- 2 Click **Discover Devices...** at the top left of the view.  
The Discovery Wizard appears.

Discovery Wizard

Specify the credentials used to discover radios.

SNMP V1 and V2c Community Strings

Search

	Strings
<input type="checkbox"/>	
<input type="checkbox"/>	public

SNMP V3 Credentials

Search

	User Names	Authentication		Privacy	
		Protocol	Passphrase	Protocol	Passphrase
<input type="checkbox"/>	test	SHA	*****	AES192	*****

Couldn't find the SNMP credentials? Click here to configure.

Previous Next Finish Cancel

- 3 On the Discovery Wizard, specify the SNMP community string(s) and/or credential(s) to be used to discover devices.

The more you specify, the longer discovery is likely to take.

**Note** If you do not see the SNMP community string(s) or credential(s), click the link at the bottom left of the Discovery Wizard to configure them. For information about configuring SNMP, see “[SNMP Configuration](#)” on page 38.

**Note** Community strings are disabled if neither SNMP v1 or SNMP v2c are selected for use in the advanced SNMP settings. Credentials are disabled if SNMP v3 is not selected for use in the advanced SNMP settings. For information about configuring advanced SNMP settings, see “[Configure Advanced SNMP Settings](#)” on page 42.

- 4 Click **Next**.

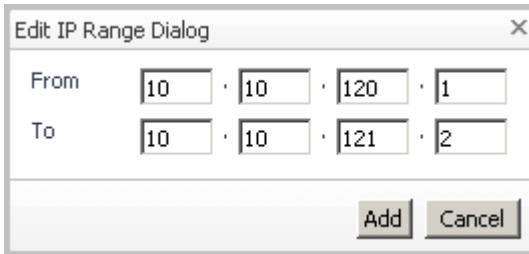
**Note** At any time you can click **Previous** to go back to the previous step.

The Discovery Wizard prompts you to specify an IP address search space.

The screenshot shows the 'Discovery Wizard' dialog box with the 'IP Search Space' section. It features two sections: 'IP Search Space' and 'Exclude Criteria'. Each section has a table with a header 'IP' and a text input field below it. The 'IP Search Space' section has a text input field with the placeholder 'Add an IP criteria for searching'. The 'Exclude Criteria' section has a text input field with the placeholder 'Specify IP to remove from search'. At the bottom of the dialog, there are four buttons: 'Previous', 'Next', 'Finish', and 'Cancel'. A status message at the bottom left reads 'No IP ranges have been specified.'

To specify an IP address, click **Add IP...** The Edit IP dialog box appears. Enter the IP address and click **Add**. The IP address is added to the search space.

To specify an IP address range, click **Add IP Range...** The Edit IP Range dialog box appears.



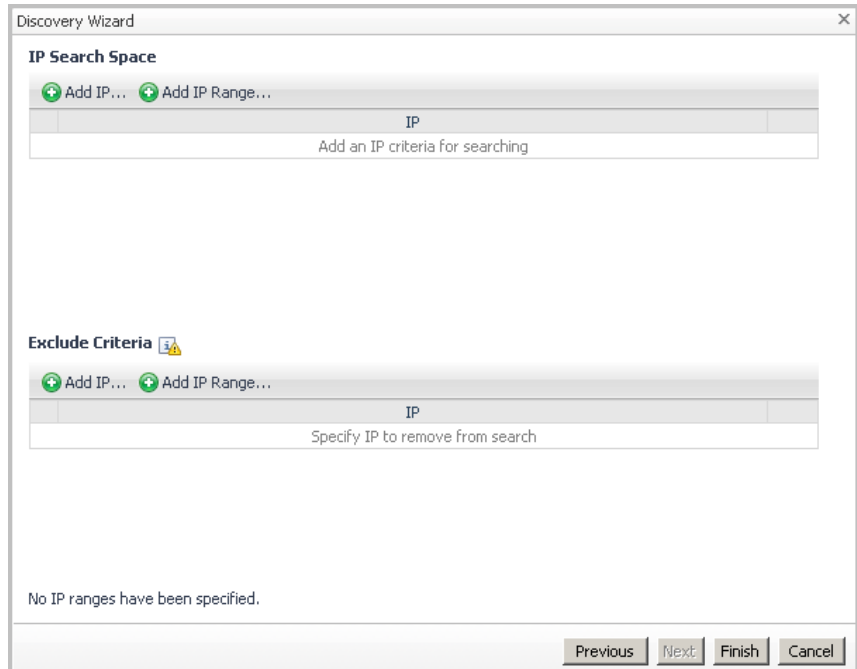
The screenshot shows a dialog box titled "Edit IP Range Dialog" with a close button (X) in the top right corner. The dialog contains two rows of input fields. The first row is labeled "From" and contains four input boxes with the values "10", "10", "120", and "1". The second row is labeled "To" and contains four input boxes with the values "10", "10", "121", and "2". Below the input fields are two buttons: "Add" and "Cancel".

Enter an IP address range and click **Add**. The IP address range is added to the search space.

For example, an IP address range of 10.10.120.1 - 10.10.121.2 will add 10.10.120.1, 10.10.120.2, 10.10.121.1, and 10.10.121.2 to the search space.

Add several IP addresses and IP address ranges, if necessary.

On the same screen of the Discovery Wizard, you are prompted to specify IP address exclude criteria.



To specify an IP address, click **Add IP...** The Edit IP dialog box appears. Enter the IP address and click **Add**. The IP address is added to the exclude criteria.

**Note** There is no need to exclude the IP addresses of devices that are already authorized; PulseNET excludes them by default. Click the Exclude Criteria Information icon to see a list of other IP addresses PulseNET excludes by default.

To specify an IP address range, click **Add IP Range...** The Edit IP Range dialog box appears. Enter an IP address range and click **Add**. The IP address range is added to the exclude criteria.

Add several IP addresses and IP address ranges, if necessary.

**Note** The Discovery Wizard provides an estimate of the time it will take to perform discovery. This is a worst-case estimate based on the configuration of the advanced SNMP and ICMP settings. For information about configuring advanced SNMP and ICMP settings, see [“Configure Advanced SNMP Settings”](#) on page 42.

## 5 Click **Finish**.

PulseNET processes your discovery request.

## Discovery Progress

Discovered devices that can be authorized appear in the list in the left pane and discovered devices that are ineligible appear in the Ineligible Devices pane at the right. For instructions on how to authorize devices, see “[Authorizing Devices](#)” on page 68. For information about discovered ineligible devices, see the “[Ineligible Devices](#)” section.

During discovery, in the Discovery Notice Message pane, you are notified about any decommissioned devices (that you may want to re-authorize) and about any monitored devices that have significant configuration changes.

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

## Ineligible Devices

---

**Note** PulseNET cannot discover ineligible Dlink devices.

---

SNMP devices can be deemed ineligible for one of the following reasons:

- The device is one that PulseNET does not monitor.
- PulseNET successfully made contact with the device, but could not connect to it.

**Note** This could be a configuration problem and should be investigated. To assist you in this investigation, you may want to export the ineligible devices list. For information about how to do this, see “[Exporting the Ineligible Devices List](#)”.

## Exporting the Ineligible Devices List

If PulseNET discovered ineligible devices and you want to investigate, you can export the ineligible devices list to assist you in the investigation.

*To export the ineligible devices list:*

- 1 Click the Customizer icon at the top right of the list.  
A popup appears.
- 2 On the popup, click **Export...**  
Another popup appears.
- 3 On this new popup, select an export format.  
The list is exported in the format you selected.

## Discovering Dlink Devices

---

**Caution** When the Dlink discovery process starts, scheduled collections for already-authorized Dlink devices are suspended. The collections resume automatically when Dlink discovery is completed.

---

Perform discovery to find the devices you want PulseNET to monitor.

---

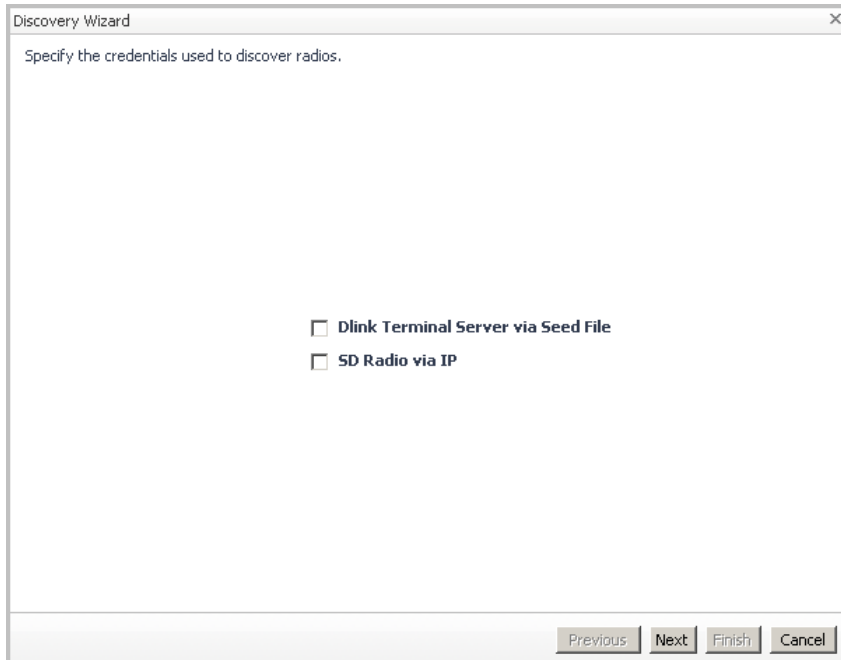
**Note** For the discovery of devices to run properly, the DType of the master device must be configured as Root.

---

*To discover devices:*

- 1 In the Device Selection view (**Administration > Device Selection**), click **Dlink Device Selection**.  
The Dlink Device Selection view appears.
- 2 Click **Discover Devices...** at the top left of the view.

The Discovery Wizard appears.



- 3 On the Discovery Wizard, specify the search type to be used to discover devices.

PulseNET can search for Dlink devices using references (seeds) to specific master devices and/or it can attempt to find master devices automatically (SD only), within a specified IP range.

- 4 Click **Next**.

**Note** At any time you can click **Previous** to go back to the previous step.

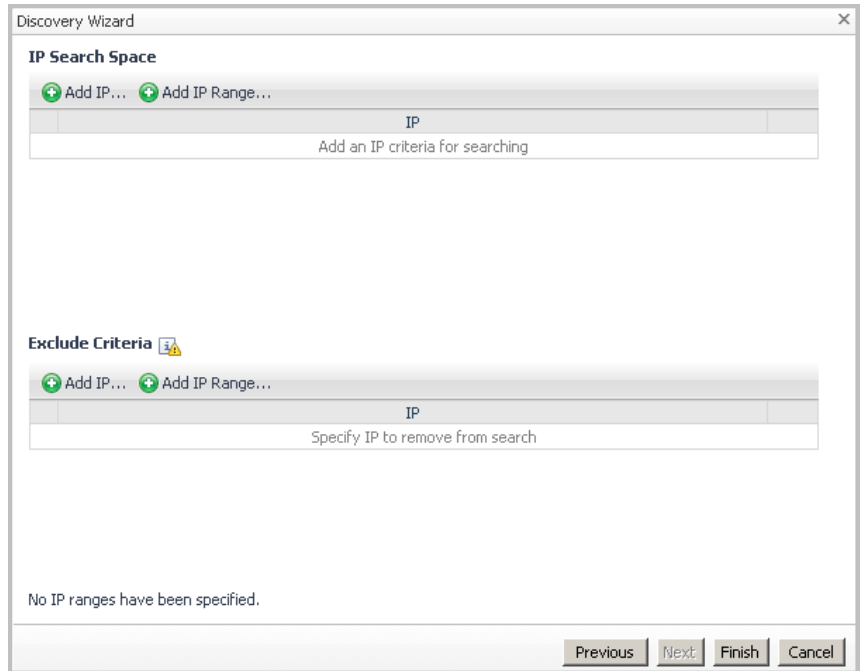
- 5 If you selected Dlink Terminal Server via Seed File on the previous screen, specify the Dlink master seed(s) to be used to discover devices. Otherwise, proceed to the next step.

The more master seeds you specify, the longer discovery is likely to take.

**Note** If you do not see any Dlink master seeds, click the link at the bottom left of the Discovery Wizard to configure one or more. For information about configuring Dlink, see "[Dlink Configuration](#)" on page 46.

- 6 Click **Next**.

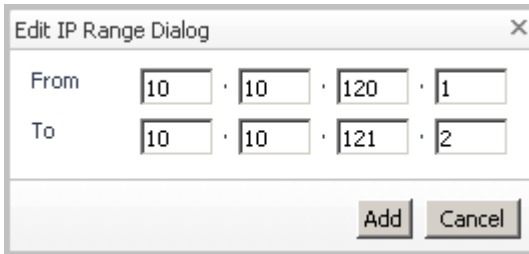
If you selected the SD Radio via IP check box in [step 2](#), the Discovery Wizard prompts you to specify an IP address search space. Otherwise, proceed to the next step.



The screenshot shows the 'Discovery Wizard' dialog box. It has a title bar with a close button (X). The main content is divided into two sections: 'IP Search Space' and 'Exclude Criteria'. Each section has a header with a plus icon and the text 'Add IP...' and 'Add IP Range...'. Below each header is a table with a single column labeled 'IP'. Under the 'IP Search Space' table, there is a text input field with the placeholder text 'Add an IP criteria for searching'. Under the 'Exclude Criteria' table, there is a text input field with the placeholder text 'Specify IP to remove from search'. At the bottom of the dialog, there is a message that says 'No IP ranges have been specified.' and a row of four buttons: 'Previous', 'Next', 'Finish', and 'Cancel'.

To specify an IP address, click **Add IP...** The Edit IP dialog box appears. Enter the IP address and click **Add**. The IP address is added to the search space.

To specify an IP address range, click **Add IP Range...** The Edit IP Range dialog box appears.



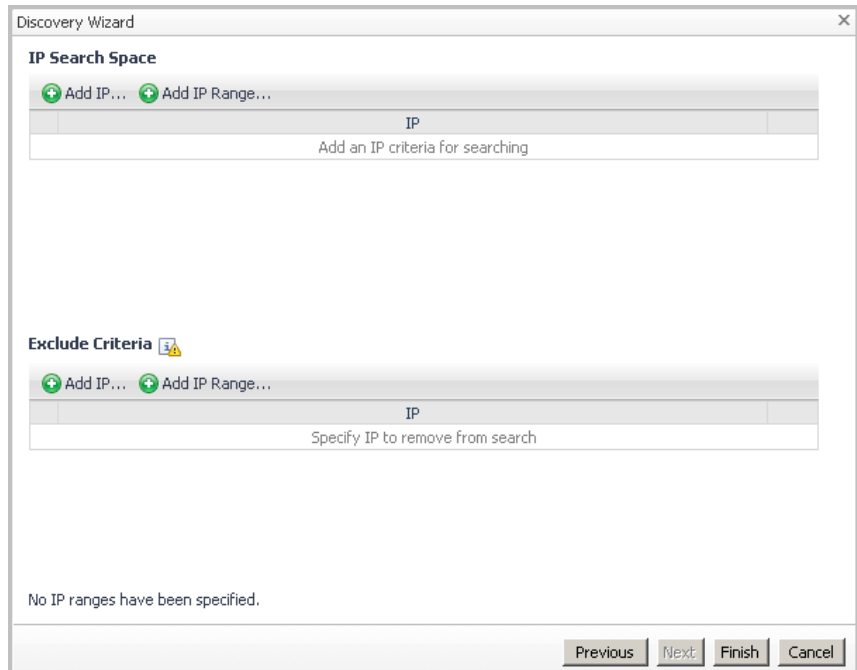
The screenshot shows a dialog box titled "Edit IP Range Dialog" with a close button (X) in the top right corner. The dialog contains two rows of input fields. The first row is labeled "From" and contains four input boxes with the values "10", "10", "120", and "1". The second row is labeled "To" and contains four input boxes with the values "10", "10", "121", and "2". At the bottom right of the dialog are two buttons: "Add" and "Cancel".

Enter an IP address range and click **Add**. The IP address range is added to the search space.

For example, an IP address range of 10.10.120.1 - 10.10.121.2 will add 10.10.120.1, 10.10.120.2, 10.10.121.1, and 10.10.121.2 to the search space.

Add several IP addresses and IP address ranges, if necessary.

On the same screen of the Discovery Wizard, you are prompted to specify IP address exclude criteria.



To specify an IP address, click **Add IP...** The Edit IP dialog box appears. Enter the IP address and click **Add**. The IP address is added to the exclude criteria.

**Note** There is no need to exclude the IP addresses of devices that are already authorized; PulseNET excludes them by default. Click the Exclude Criteria Information icon to see a list of other IP addresses PulseNET excludes by default.

To specify an IP address range, click **Add IP Range...** The Edit IP Range dialog box appears. Enter an IP address range and click **Add**. The IP address range is added to the exclude criteria.

Add several IP addresses and IP address ranges, if necessary.

**Note** The Discovery Wizard provides an estimate of the time it will take to perform discovery. This is a worst-case estimate based on the configuration of the advanced Dlink settings. For information about configuring advanced Dlink settings, see [“Configure Advanced Dlink Settings”](#) on page 49.

## 7 Click **Finish**.

PulseNET processes your discovery request.

## Discovery Progress

Discovered devices that can be authorized appear in the list in the left pane. For instructions on how to authorize devices, see “[Authorizing Devices](#)” on page 68.

During discovery, in the Discovery Notice Message pane at the top right you are notified about any decommissioned devices (that you may want to re-authorize) and about any monitored devices that have significant configuration changes.

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

## Authorizing Devices

After discovering devices, you can authorize them to be monitored by PulseNET.

*To authorize devices:*

- 1 In the Device Selection view (**Administration > Device Selection**), for the device(s) you want to authorize, click the corresponding check box(es) in the list in the left pane.

The **Authorize...** button becomes enabled.

- 2 Click **Authorize...**

A dialog box appears and asks you if you are sure.

- 3 Click **Authorize**.

PulseNET processes your request.

---

**Note** If your environment has a mix of active (the expiry date is more than 14 days away) and expiring (the expiry date is in 14 days or less) licenses, PulseNET assigns authorized devices to licenses in a specific license order. For more information, see “[License Order when Authorizing Devices](#)” on page 34.

---

## Configuring Access Point Failover

If a Mercury access point has a failover device, you can configure that in PulseNET. When the failover device for an access point is configured in PulseNET and failover occurs, PulseNET polls the failover device for availability and performance data instead of the primary device.

---

**Note** Before configuring a failover device, you must first discover and authorize the primary device. For information on how to perform discovery, see [“Discovering SNMP Devices”](#) on page 58. For information on how to authorize devices, see [“Authorizing Devices”](#) on page 68.

---

*To configure a failover device for a Mercury access point:*

- 1 Navigate to the Detail view of the access point for which you want to configure a failover device.
- 2 At the top right of the Detail view, click the **Administrative Menu** icon and select **Configure Fail-Over Device** from the list.  
The Update/Remove Fail-Over Device dialog box appears.
- 3 Enter the IP address of the failover device.
- 4 Click **Update**.

When the failover device for an access point is configured in PulseNET and failover occurs, the device identity information (device name, serial number, location, and so on) displayed in the Role Summary view and in the Detail view of the device does not change; that is, the device identity information for the primary access point is still displayed. However, PulseNET now polls the failover device for availability and performance data.

The presence of the Failover icon, next to the device name, on the Role Summary view and on the Detail view of the device indicates that the failover device is now the operational device. Also, on the Detail view of the device, the IP address of the failover device is displayed in the Configuration pane at the top of the view.

## Promote the Failover Device to be the Primary Access Point

*To promote the failover device to be the primary access point:*

- 1 While the original failover device is the operational access point, decommission the primary access point.

For information on how to decommission a device, see “[Decommissioning a Monitored Device](#)” on page 72.

- 2 Perform discovery so that you can authorize the original failover device to be a PulseNET-licensed device.

For information on how to perform discovery, see “[Discovering SNMP Devices](#)” on page 58.

- 3 Authorize the original failover device.

For information on how to authorize a device, see “[Authorizing Devices](#)” on page 68.

- 4 Configure a third device to be the new failover device.

For information on how to configure a device to be a failover device in PulseNET, see “[Configuring Access Point Failover](#)” on page 69.

## Creating and Managing Maintenance Windows

If you know that maintenance tasks are scheduled to be performed on a device and you do not want alerts raised for that device during the maintenance period, you can configure a maintenance window for the device.

There are two types of maintenance window: temporary and scheduled. A temporary maintenance window is configured to happen only once. A scheduled maintenance window is configured to happen repeatedly according to a schedule.

*To create a temporary maintenance window:*

- 1 Navigate to the Detail view of the device for which you want to create a maintenance window.

For more information on Detail views, see “Detail Views” in the *PulseNET User's Guide*.

- 2 At the top right of the Detail view, click the **Administrative Menu** icon and select Temporary Maintenance Window from the list.

The Create Temporary Maintenance Window dialog box appears.

- 3 Click within the **Start Time** field to configure a start time.  
A calendar appears.
- 4 From the calendar, select a month and day and enter a time.
- 5 When you are finished, click within the **Start Time** field again to close the calendar.
- 6 Select an end time configuration method from the list provided.
- 7 Click **Next**.

If you selected Custom Duration, enter the number of hours, days, months or years the maintenance window is to last. If you selected Choose the End Time, configure an end date and time for the maintenance window. When you are finished, click **Next** again.

- 8 **Optional.** If this is an access point with authorized remotes, you can choose to apply the maintenance window to downstream devices.

**Note** Once a maintenance window is created that includes downstream devices, it is not possible to remove the window for just a subset of those devices.

Click the check box beside a downstream device to include that device in the maintenance window. To include all downstream devices in the maintenance window, click **Select All**.

- 9 Click **Finish**.

*To create a scheduled maintenance window:*

- 1 Navigate to the Detail view of the device for which you want to create a maintenance window.

For more information on Detail views, see “Detail Views” in the *PulseNET User’s Guide*.

- 2 At the top right of the Detail view, click the **Administrative Menu** icon and select Scheduled Maintenance Window from the list.

The Create Scheduled Maintenance Window dialog box appears.

- 3 Select a PulseNET pre-defined schedule from the list provided, or click **Create New Schedule** to create your own schedule.

For descriptions of the PulseNET pre-defined schedules, see “Working with PulseNET Reports” in the *PulseNET User’s Guide*.

If you chose to create your own schedule, create the schedule using the New Schedule wizard and click **Finish**.

4 Click **Next**.

5 **Optional.** If this is an access point with authorized remotes, you can choose to apply the maintenance window to downstream devices.

**Note** Once a maintenance window is created that includes downstream devices, it is not possible to remove the window for just a subset of those devices.

Click the check box beside a downstream device to include that device in the maintenance window. To include all downstream devices in the maintenance window, click **Select All**.

6 Click **Finish**.

## Managing Maintenance Windows

You can view a list of the configured maintenance windows for a device, and you can delete maintenance windows.

*To view a list of the configured maintenance windows for a device:*

- At the top right of the Detail view for the device, click the **Administrative Menu** icon and select Review Maintenance Windows from the list.

A popup with a list of the configured maintenance windows for the device appears. For each maintenance window, the schedule is defined. The popup also indicates if the device is presently within a particular maintenance window and if a maintenance window is scheduled for the future.

*To delete a maintenance window for a device:*

---

**Note** For a maintenance window that includes downstream devices, it is not possible to remove the window for just a subset of those devices.

---

- 1 At the top right of the Detail view for the device, click the **Administrative Menu** icon and select Review Maintenance Windows from the list.

A popup with a list of the configured maintenance windows for the device appears.

- 2 Click the check box next to the maintenance window you want to delete.

To select all maintenance windows, click **Select All**.

- 3 Click **Remove Selected**.

A confirmation dialog box appears.

- 4 Click **Delete**.

## Decommissioning a Monitored Device

If you know that a monitored device is not available and you do not want data collected from that device (because, for example, that would incorrectly impact PulseNET summary statistics), you can decommission the device.

*To decommission a monitored device:*

- 1 Navigate to the Detail view of the device you want to decommission.

For more information on Detail views, see “Detail Views” in the *PulseNET User’s Guide*.

- 2 At the top right of the Detail view, click the **Administrative Menu** icon and select Decommission from the list.

The Decommission dialog box appears.

- 3 Click the check mark beside any associated downstream device (if applicable) that you also want to decommission. To select all downstream devices, click **Select All**.

**Note** When you decommission a Dlink device, any downstream devices are automatically decommissioned.

- 4 Click **Yes**.

A dialog box asking if you are sure you want to decommission the device(s) appears.

- 5 Click **Yes**.

The device is decommissioned and removed from the Monitored Devices list.

*To re-authorize a decommissioned device:*

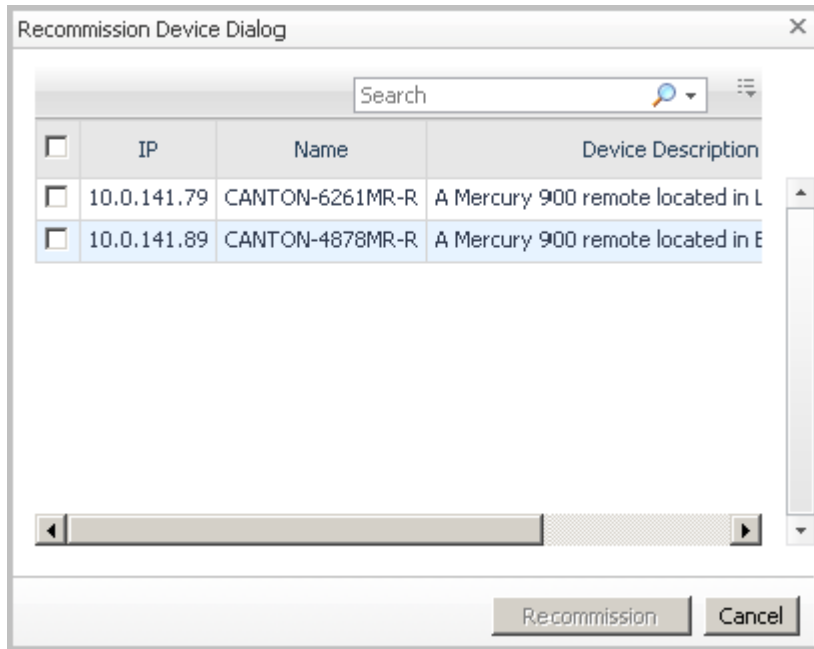
- 1 Perform discovery. For instructions on how to perform discovery, see “[Discovering SNMP Devices](#)” on page 58.

**Note** In [step 4](#) of the “Discovering Devices” procedure, if you know an IP range within which the device resides, simply configure that range to be the IP address search space. Similarly, if you know the IP address of the device, configure just that IP address to be the search space.

During discovery, in the Discovery Progress pane at the top right, you are notified about any decommissioned devices that you may want to re-authorize.

- 2 When PulseNET completes discovery, click the link provided to re-authorize the device.

The Recommission Device dialog box appears.



- 3 Select the device(s) you want to re-authorize and click **Recommission**.

The device(s) are re-authorized.

---

**Note** Authorized devices consume license capacity. For more information about licenses, see Chapter 3, "Working with Licenses".

---

# Managing Devices

On a Device Selection view (**Administration > Device Selection > SNMP or Dlink Device Selection**), devices are listed in either the Discovered Devices list (at the top left), the Ineligible Devices list (at the top right, and for SNMP devices only), or in the Monitored Devices list below.

The Monitored Devices list can be toggled open or closed using the arrow to the right of its heading.

The screenshot shows the 'Device Selection' interface. At the top, it displays the breadcrumb 'Administration > Device Selection > Device Selection' and the date 'Monday, August 30, 2010 7:03 AM - 7:03 AM 24 hours'. The interface is divided into three main sections:

- Discovered Devices:** Shows 'Selected 0 (remaining capacity 575)'. It includes a search bar and a table with columns: IP, Model, Role, Serial Number, and Vendor. A message states: 'No devices have been discovered. Run "Discover Devices" to find devices.'
- Ineligible Devices:** Includes a search bar and a table with columns: IP, Name, Device Description, and Serial Number. A message states: 'There Is No Data To Display.'
- Monitored Devices:** A large table with columns: Device Name, Device Description, Device Contact, IP, Mac, Model Number, Device Location, Serial Number, and Decommission Device. The table contains 14 rows of device information.

Device Name	Device Description	Device Contact	IP	Mac	Model Number	Device Location	Serial Number	Decommission Device
BRIDGE-AP1-A	A Mercury 900 access point located in Bridgeville, PA	Dwight Harris (441-736-6261)	10.0.142.36	B5:EA:F7:CE:8B:8F	Mercury 900	Apt 3609 75 Thorncliffe Park Dr	245503793	⊖
PERCY-AP1-A	An MDS INET-II 900 access point located in Percy, IL	Mathew Williamson (430-464-3579)	10.0.140.248	78:4A:BC:34:E1:68	MDS INET-II 900	Apt 3609 75 Thorncliffe Park Dr	289961531	⊖
GILBER-AP5-B	An MDS INET-II 900 access point located in Gilbert, SC	David Bradley (962-789-1680)	10.0.141.195	1E:83:FD:4C:FE:56	MDS INET-II 900	Apt 3609 75 Thorncliffe Park Dr	789961531	⊖
RICHLA-AP3-A	An MDS INET-II 900 access point located in Richlands, NC	Ernest Mccarthy (789-017-5367)	10.0.140.15	50:21:2A:02:40:05	MDS INET-II 900	Apt 3609 75 Thorncliffe Park Dr	701185375	⊖
COMSTO-AP6-A	A Mercury 900 access point located in Constock, NE	Sharon Perkins (931-882-1730)	10.0.144.202	75:6A:03:59:92:0F	Mercury 900	Apt 3609 75 Thorncliffe Park Dr	945503793	⊖
COMSTO-8952MR-R	A Mercury 900 remote located in Metamora, IN	Karen Brooks (971-756-2473)	10.0.141.92	C5:18:82:2B:84:FD	Mercury 900	Apt 3609 75 Thorncliffe Park Dr	123347917	⊖
PLYMOU-2528Net-R	An INET 900 remote located in Genburn, ND	Margaret Taylor (615-893-1771)	10.0.141.116	F7:7B:CE:07:28:A9	INET 900	Apt 3609 75 Thorncliffe Park Dr	356618048	⊖
BOLING-2351Net-R	An INET-II 900 remote located in Auburn, IL	William Miller (228-329-4216)	10.0.141.49	A1:01:83:02:84:09	INET-II 900	Apt 3609 75 Thorncliffe Park Dr	267729159	⊖
PLYMOU-6976Net-R	An INET 900 remote located in Round Top, NY	Harold Miller (582-135-3339)	10.0.141.59	DD:33:E5:57:DE:83	INET 900	Apt 3609 75 Thorncliffe Park Dr	145503793	⊖
DEERFL-9231MR-R	A Mercury 3650 remote located in Argyle, IA	Jeffrey Johnson (742-322-0585)	10.0.142.28	18:36:CA:98:07:AC	Mercury 3650	Apt 3609 75 Thorncliffe Park Dr	538850420	⊖
BOLING-2213Net-R	An INET-II 900 remote located in Salsbury Center, NY	Glenn Wilson (501-857-8551)	10.0.142.48	0A:6B:5A:3F:EA:64	INET-II 900	Apt 3609 75 Thorncliffe Park Dr	370034264	⊖

From the Device Selection view, you can:

- [Sort a List](#)
- [Search for a Device in a List](#)
- [Filter a List](#)
- [Discover Devices](#)

## Sort a List

To sort a list by a particular column heading, click that column heading. An arrow beside that column heading indicates the order (ascending or descending) in which the devices are sorted.

## Search for a Device in a List

Use the Search tool at the top right of the list to search for a specific device. For instructions on how to use the Search tool, see “Working with Tables” in the *PulseNET Quick Start Guide*.

## Filter a List

Use the Search tool at the top right of the list to filter the list. For instructions on how to use the Search tool, see “Working with Tables” in the *PulseNET Quick Start Guide*.

## Discover Devices

Perform discovery to find the devices you want PulseNET to monitor. For instructions on how to perform discovery, see “[Discovering SNMP Devices](#)” on page 58 and “[Discovering Dlink Devices](#)” on page 63.

# Working with Rules and Alerts

This chapter describes how to use the Rules view (**Administration > Rules and Alerts**) for:

- [Enabling and Disabling Rules](#)
- [Configuring Rule Thresholds](#)
- [Turning Notification Email On or Off](#)
- [Turning an SNMP Trap Action On or Off](#)
- [Creating Custom PulseNET Rules](#)
- [Editing a Custom Rule](#)
- [Removing a Custom Rule](#)

Administration > Rules and Alerts Dec 9, 2010 9:24:51 AM EST

PulseNET System Rules Custom Rules Search

Name	Type	Description	Enabled	Email				SNMP Trap				Threshold	
				Normal	Warning	Critical	Fatal	Normal	Warning	Critical	Fatal		
AP Fail-over	Mercury Access Points	Raise a warning when an AP fails over to its backup.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Bad Access Point health	INET 900 Access Points	Bad Access Point health detected.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Bad Access Point health	INET-II 900 Access Points	Bad Access Point health detected.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Bad Access Point health	Mercury 1000 Access Points	Bad Access Point health detected.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Bad Access Point health	Mercury 3650 Access Points	Bad Access Point health detected.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Bad Access Point health	Mercury 900 Access Points	Bad Access Point health detected.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Bad Access Point health	Dlink Access Points	Bad Access Point health detected.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Device Unavailable	INET 900 Access Points	The INET-I Access Point is not available.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Device Unavailable	INET 900 Remotes	The INET-I Remote is not available.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Device Unavailable	INET-II 900 Access Points	The INET-II Access Point is not available.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Device Unavailable	INET-II 900 Remotes	The INET-II Remote is not available.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Device Unavailable	Intrepsids	The Intrepid Device is not available.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Device Unavailable	LAN Devices	The LAN Device is not available.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Device Unavailable	Mercury 1800 Access Points	The Mercury 1800 Access Point is not available.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Device Unavailable	Mercury 1800 Remotes	The Mercury 1800 Remote is not available.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Device Unavailable	Mercury 3650 Access Points	The Mercury 3650 Access Point is not available.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Device Unavailable	Mercury 3650 Remotes	The Mercury 3650 Remote is not available.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Device Unavailable	Mercury 900 Access Points	The Mercury 900 Access Point is not available.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Device Unavailable	Mercury 900 Remotes	The Mercury 900 Remote is not available.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Device Unavailable	Dlink Access Points	The Dlink Device Access Point is not available.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Device Unavailable	Dlink Remotes	The Dlink Device Remote is not available.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
High CPU Utilization	Cisco Devices	High CPU utilization detected.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
High Memory Utilization	Cisco Devices	High Memory utilization detected.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Poor Response Time	Backhaul Devices	Poor SNMP round trip time detected.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Poor Response Time	INET 900 Access Points	Poor ICMP round trip time detected.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Poor Response Time	INET 900 Remotes	Poor ICMP round trip time detected.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Poor Response Time	INET-II 900 Access Points	Poor ICMP round trip time detected.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Poor Response Time	INET-II 900 Remotes	Poor ICMP round trip time detected.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Poor Response Time	LAN Devices	Poor SNMP round trip time detected.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

The following table provides a description for each of the pre-defined PulseNET rules.

Rule	Description	Severity
AP Fail-over	This rule monitors for access point failover. <b>Note</b> Failover is supported for Mercury devices only.	warning
Bad Access Point Health	This rule monitors the percentage of remotes 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
Device Unavailable	This rule monitors the availability of the device.	fatal
High CPU Utilization	This rule monitors for high CPU utilization on Cisco devices.	warning, critical, fatal
High Memory Utilization	This rule monitors for high memory utilization on Cisco devices.	warning, critical, fatal
Poor Response Time	This rule monitors the ICMP round trip time for a device.	warning, critical, fatal
RSSI Change	This rule monitors for values of RSSI (for devices) that are outside a two-day moving average.	warning, critical, fatal
RSSI Level	This rule monitors the levels of RSSI for devices.	warning, critical, fatal
SNR Change	This rule monitors for values of SNR (for devices) that are outside a two-day moving average.	warning, critical, fatal
SNR Level	This rule monitors the levels of SNR for devices.	warning, critical, fatal

**Note** With the exception of the Device Unavailable rule, all PulseNET rules are disabled by default.

## Enabling and Disabling Rules

---

**Note** The following procedure applies to PulseNET system and custom rules.

---

*To enable or disable a rule:*

- 1 Click the Enable/Disable icon for the rule.  
A rule status confirmation dialog box appears.
- 2 Click **Yes**.

## Configuring Rule Thresholds

Most PulseNET rules have three thresholds (warning, critical, and fatal).

---

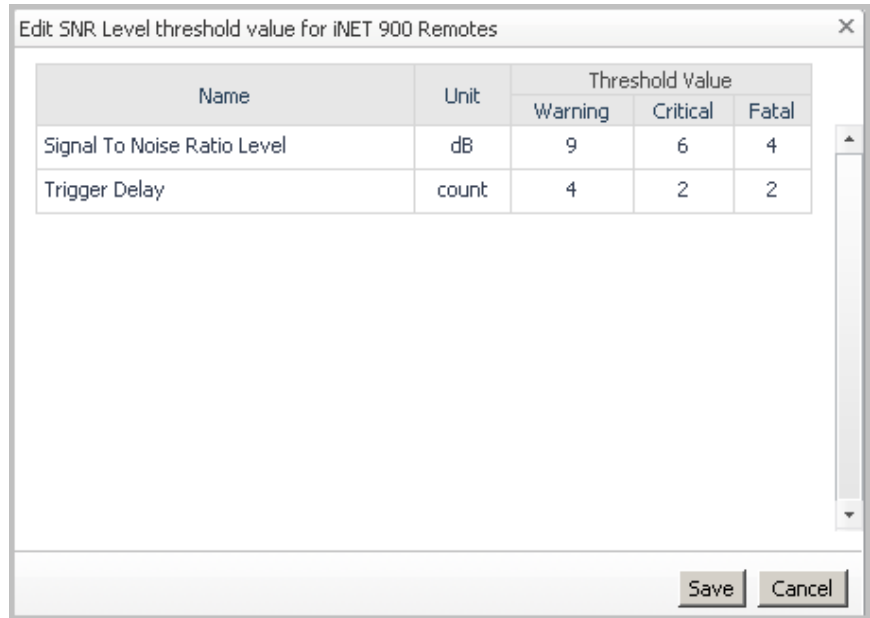
**Note** The following procedure applies to PulseNET system and custom rules.

---

*To configure the threshold(s) for a rule:*

- 1 Click the Threshold icon for the rule.

An Edit dialog box appears.



Name	Unit	Threshold Value		
		Warning	Critical	Fatal
Signal To Noise Ratio Level	dB	9	6	4
Trigger Delay	count	4	2	2

- 2 In the table provided, click the value you want to edit.

The value becomes highlighted.

**Important** When altering trigger delay values, it is important to understand how trigger delay values and data collection frequency for performance or availability information together affect the raising of alerts. For detailed information about this interdependency, see [“Trigger Delay Values and Data Collection Frequency”](#) on page 56.

- 3 Enter the new value.

**Note** Each of the configurable thresholds has an upper and lower limit. Hover over the name of the threshold to view those limits.

- 4 When you are finished configuring threshold values, click **Save**.

## Turning Notification Email On or Off

Pre-defined PulseNET rules are configured by default not to send a notification email when a certain threshold is met.

---

**Note** The following procedure applies to PulseNET system and custom rules.

---

*To turn notification email on or off:*

- 1 Click the Email On/Off icon for the rule/severity pair for which you want to change email notification.

A confirmation dialog box appears.

**Note** If you have not configured PulseNET email settings, the confirmation dialog box will ask you if you want to do that now. For information about how to configure email settings, see Chapter 2, “Configuring System Settings”.

- 2 If you have configured PulseNET email settings, click **Yes**.

## Turning an SNMP Trap Action On or Off

Pre-defined PulseNET rules are configured by default not to send an SNMP trap when a certain threshold is met.

---

**Important** The method of configuring an SNMP trap action to forward an alert for a custom rule condition is different. For information on how to configure an SNMP trap action to forward an alert for a custom rule condition, see “[SNMP Trap Actions](#)” on page 96.

---

*To configure an SNMP trap action to forward an alert for a pre-defined PulseNET rule condition:*

- 1 Navigate to the Rules and Alerts view (**Administration > Rules and Alerts**).
- 2 In the SNMP Trap column, click the icon that corresponds to the rule and severity for which you want an SNMP trap sent.

The Change SNMP Trap Action dialog box appears, asking you to confirm or cancel your choice.

- 3 Click **Yes**.

The SNMP trap action is set.

## Creating Custom PulseNET Rules

The custom rules functionality is available on the Rules view (**Administration > Rules and Alerts**).

The custom rules functionality is extensive and can be complex. The functionality that is not documented here is currently not supported. We recommend that you use the following three examples to help you create the custom rules you need. For additional information about rule parameters, see “[Working with Custom Rule Parameters](#)” on page 91.

### Example 1: Add a rule that raises an alert when a metric drops below a certain value.

*To add a rule that raises an alert when a metric drops below a certain value:*

- 1 On the Rules view (**Administration > Rules and Alerts**), click the **Custom Rules** tab.  
The **Custom Rules** list appears.
- 2 Click **Add Rule**.  
The **Create Rule** view appears.
- 3 On the **Rule Definition** tab, type a name for the rule in the field provided (for example, INET1 Remote Low Transmit Power Alert).
- 4 Specify the Multiple-Severity Rule type.
- 5 Specify Data Driven for rule triggering.
- 6 Under Rule Scope, select a topology type (for example, INET1Remote) from the list provided. For more information on topology types, see “[Topology Types](#)” on page 92.
- 7 To the right of the Topology Type field, click the **Append** icon.  
The topology type is appended to the rule.
- 8 Click **Validate Rule Scope** icon.  
The rule scope is validated.
- 9 Type a rule description in the field at the top right.
- 10 Click **Next** at the top of the view.
- 11 On the **Conditions, Alerts & Actions** tab, click **Warning**.
- 12 On the **Condition** tab, select the **Activate** check box (if not already selected).

- 13 Click the **Condition Editor** icon.

The **Condition Editor** appears.

- 14 Select the **Metric/Property** tab.

- 15 Click the type of scope (in this case, INET1Remote).

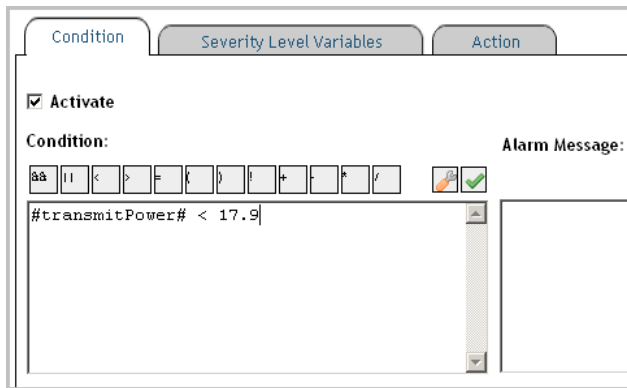
- 16 From the list of metrics at the right, select a metric (for example, transmitPower).

- 17 Click **Insert**.

The metric appears in the Condition field.

- 18 Click **Close**.

- 19 Add a condition to the metric (for example, < 17.9).



- 20 Click the **Validate Condition** icon to the right.

The condition is validated.

- 21 Test the new condition:

- a Click **Run Condition Query**.
- b Select a scoped object, on which to test the new condition, from the list provided.

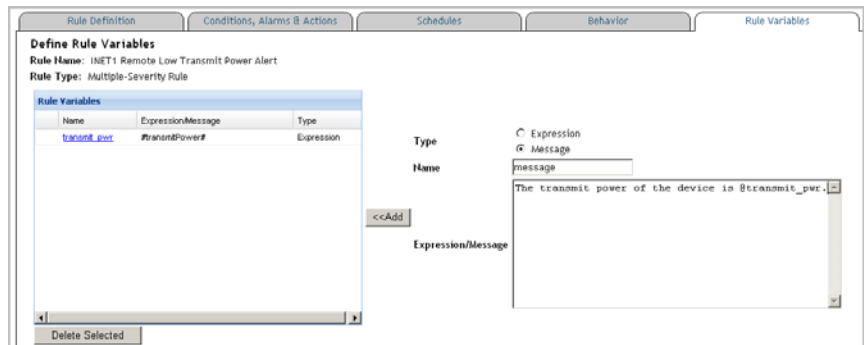
**Note** PulseNET must have obtained data that corresponds to the topology type you defined in [step 6](#) in order for scoped objects to appear in the list.

- c Click the **Paste** icon next to Condition Query, and then select **Warning** from the list that appears.

The rule condition is pasted into the field provided.

d Click **Execute Query**.

- 22 Repeat [step 12](#) through [step 21](#) for Critical (with < 17.1 for the condition) and Fatal (with < 17.0 for the condition).
- 23 Click **Next** at the top of the view.  
You do not require the functionality on the **Schedules** tab for this rule.
- 24 Click **Next** at the top of the view.  
You do not require the functionality on the **Behavior** tab for this rule.
- 25 Click **Next** at the top of the view.
- 26 On the **Rule Variables** tab, set Type to Expression (if not already set).
- 27 Under name, type a name (for example, transmit\_pwr) for a new variable.
- 28 In the Expression field, define the variable to be #transmitPower#.
- 29 Click **Add**.
- 30 For the next variable, set Type to Message.
- 31 Under name, type a name (for example, message) for the new variable.
- 32 In the Expression field, define the variable to be: The transmit power of the device is @transmit\_pwr.



- 33 Click **Add**.
- 34 Click the **Conditions, Alerts & Actions** tab.
- 35 For each of the Warning, Critical, and Fatal actions, in the Alert Message field, define the alert message to be @message. Now the conditions will call the

variable you defined in [step 30](#) through [step 33](#) and provide it for the alert message.

- 36 Click **Finish** at the top of the tab.

An overview of the new rule appears.

- 37 From the breadcrumbs at the top, click **Rules and Alerts**.

Now you have a rule that fires a warning alert when the transmit power of any INET 1remote drops below 17.9, a critical alert when the transmit power of any INET 1remote drops below 17.1, and a fatal alert when the transmit power of any INET 1remote drops below 17.0. The rule appears in the **Custom Rules** list.

## Example 2: Add a rule that raises an alert when a metric exceeds a certain value.

*To add a rule that raises an alert when a metric exceeds a certain value:*

- 1 On the Rules view (**Administration > Rules and Alerts**), click the **Custom Rules** tab.  
The **Custom Rules** list appears.
- 2 Click **Add Rule**.  
The **Create Rule** view appears.
- 3 On the **Rule Definition** tab, type a name for the rule in the field provided (for example, Merc3650 Remote High Temp Alert).
- 4 Specify the Multiple-Severity Rule type.
- 5 Specify Data Driven for rule triggering.
- 6 Under Rule Scope, select a topology type (for example, Mercury3650Remote) from the list provided. For more information on topology types, see [“Topology Types”](#) on page 92.
- 7 To the right of the Topology Type field, click the **Append** icon.  
The topology type is appended to the rule.
- 8 Click the **Validate Rule Scope** icon.  
The rule scope is validated.
- 9 Type a rule description in the field at the top right.
- 10 Click **Next** at the top of the view.
- 11 On the **Conditions, Alerts & Actions** tab, click **Warning**.

- 12 On the **Condition** tab, select the **Activate** check box (if not already selected).
- 13 Click the **Condition Editor** icon.

The **Condition Editor** appears.
- 14 Select the **Metric/Property** tab.
- 15 Click the type of scope (in this case, Mercury3650Remote).
- 16 From the list of metrics at the right, select a metric (for example, paTemp).
- 17 Click **Insert**.

The metric appears in the Condition field.
- 18 Click **Close**.
- 19 Add a condition to the metric (for example, > 60).
- 20 Click the **Validate Condition** icon to the right.

The condition is validated.
- 21 Test the new condition:
  - a Click **Run Condition Query**.
  - b Select a scoped object, on which to test the new condition, from the list provided.

**Note** PulseNET must have obtained data that corresponds to the topology type you defined in [step 6](#) in order for scoped objects to appear in the list.
  - c Click the **Paste** icon next to Condition Query, and then select **Warning** from the list that appears.

The rule condition is pasted into the field provided.
  - d Click **Execute Query**.
- 22 Repeat [step 12](#) through [step 21](#) for Critical (with > 65 for the condition) and Fatal (with > 70 for the condition).
- 23 Click **Next** at the top of the view.

You do not require the functionality on the **Schedules** tab for this rule.
- 24 Click **Next** at the top of the view.

You do not require the functionality on the **Behavior** tab for this rule.
- 25 Click **Next** at the top of the view.
- 26 On the **Rule Variables** tab, set Type to Expression (if not already set).

- 27 Under name, type a name (for example, temp) for a new variable.
- 28 In the Expression field, define the variable to be #paTemp#.
- 29 Click **Add**.
- 30 For the next variable, set Type to Message.
- 31 Under name, type a name (for example, message) for the new variable.
- 32 In the Expression field, define the variable to be: The temperature of the device is @temp.
- 33 Click **Add**.
- 34 Click the **Conditions, Alerts & Actions** tab.
- 35 For each of the Warning, Critical, and Fatal actions, in the Alert Message field, define the alert message to be @message. Now the conditions will call the variable you defined in [step 30](#) through [step 33](#) and provide it for the alert message.
- 36 Click **Finish** at the top of the tab.

An overview of the new rule appears.
- 37 From the breadcrumbs at the top, click **Rules and Alerts**.

Now you have a rule that fires a warning alert when the temperature of any Mercury 3650 remote is above 60 C, a critical alert when the temperature of any Mercury 3650 remote is above 65 C, and a fatal alert when the temperature of any Mercury 3650 remote is above 70 C. The rule appears in the **Custom Rules** list.

### Example 3: Add a rule that raises an alert when two metrics are both at warning levels.

*To add a rule that raises an alert when two metrics are both at warning levels:*

- 1 On the Rules view (**Administration > Rules and Alerts**), click the **Custom Rules** tab.

The **Custom Rules** list appears.
- 2 Click **Add Rule**.

The **Create Rule** view appears.
- 3 On the **Rule Definition** tab, type a name for the rule in the field provided (for example, Merc900 Remote RSSI and SNR both Warning Alert).
- 4 Specify the Multiple Severity Rule type.

- 5 Specify Data Driven for rule triggering.
- 6 Under Rule Scope, select a topology type (for example, Mercury900Remote) from the list provided. For more information on topology types, see “[Topology Types](#)” on page 92.
- 7 To the right of the Topology Type field, click the **Append** icon.  
The topology type is appended to the rule.
- 8 Click the **Validate Rule Scope** icon.  
The rule scope is validated.
- 9 Type a rule description in the field at the top right.
- 10 Click **Next** at the top of the view.
- 11 On the **Conditions, Alerts & Actions** tab, click **Warning**.
- 12 On the **Condition** tab, select the **Activate** check box (if not already selected).
- 13 Click the **Condition Editor** icon.  
The **Condition Editor** appears.
- 14 Select the **Metric/Property** tab.
- 15 Click the type of scope (in this case, Mercury900Remote).
- 16 From the list of metrics at the right, select a metric (for example, rssi).
- 17 Click **Insert**.  
The metric appears in the Condition field.
- 18 Add a condition to the metric (for example, < -85).
- 19 From the list of metrics at the right, select a metric (for example, snr).
- 20 Click **Insert**.  
The metric appears in the Condition field.
- 21 Click **Close**.
- 22 Add a condition to the metric (for example, < 9).
- 23 Place the cursor between the two statements and click the **Ampersand** button to add && (and) to the condition.
- 24 Click the **Validate Condition** icon to the right.  
The condition is validated.
- 25 Test the new condition:

- a Click **Run Condition Query**.
  - b Select a scoped object, on which to test the new condition, from the list provided.  
**Note** PulseNET must have obtained data that corresponds to the topology type you defined in [step 6](#) in order for scoped objects to appear in the list.
  - c Click the **Paste** icon next to Condition Query, and then select **Warning** from the list that appears.  
The rule condition is pasted into the field provided.
  - d Click **Execute Query**.
- 26 Click **Next** at the top of the view.  
You do not require the functionality on the **Schedules** tab for this rule.
  - 27 Click **Next** at the top of the view.  
You do not require the functionality on the **Behavior** tab for this rule.
  - 28 Click **Next** at the top of the view.
  - 29 On the **Rule Variables** tab, set Type to Expression (if not already set).
  - 30 Under name, type a name (for example, rssi) for a new variable.
  - 31 In the Expression field, define the variable to be #rssi#.
  - 32 Click **Add**.
  - 33 Ensure Type is still set to Expression.
  - 34 Under name, type a name (for example, snr) for a new variable.
  - 35 In the Expression field, define the variable to be #snr#.
  - 36 Click **Add**.
  - 37 For the next variable, set Type to Message.
  - 38 Under name, type a name (for example, message) for the new variable.
  - 39 In the Expression field, define the variable to be: The RSSI for the device is @rssi and the SNR for the device is @snr.
  - 40 Click **Add**.
  - 41 Click the **Conditions, Alerts & Actions** tab.
  - 42 For the Warning action, in the Alert Message field, define the alert message to be @message. Now the warning condition will call the variable you defined in [step 37](#) through [step 40](#) and provide it for the alert message.

43 Click **Finish** at the top of the tab.

An overview of the new rule appears.

44 From the breadcrumbs at the top, click **Rules and Alerts**.

Now you have a rule that fires a warning alert when the RSSI and SNR values for any Mercury 900 remote are both at warning levels. The rule appears in the **Custom Rules** list.

## Working with Custom Rule Parameters

This section provides information on the more commonly used custom rule parameters, which are available in the Create Rule view (**Administration > Rules and Alerts > Custom Rules > Add/Edit Rule**).

---

**Note** There are other custom rule parameters available through the Create Rule view. The parameters that are not documented here are currently not supported.

---

### Rule Types

For each custom rule, you must select one rule type.

The following table describes the rule types, which are available on the Rule Definition tab of the Create Rule view.

Rule Type	Description
Multiple-Severity <sup>1</sup>	For a multiple-severity rule, you define warning, critical, and fatal thresholds.
Simple	For a simple rule, you define only one fire condition.

<sup>1</sup> This is the recommended rule type.

### Rule Triggering Types

For each custom rule, you must select one rule triggering type, which defines the evaluation pattern of the rule.

The following table describes the rule triggering types, which are available on the Rule Definition tab of the Create Rule view.

Triggering Type	Description
Time Driven <sup>1</sup>	The rule conditions are evaluated at a specified interval (defined in the form hh:mm:ss).
Data Driven <sup>2</sup>	The rule conditions are evaluated every time the data associated with the rule is collected.
Event Driven <sup>1</sup>	The rule conditions are evaluated in response to one of the following event types: AgentManagementSystemEvent, AlertSystemEvent, IncidentSystemEvent, or ReportGeneratedEvent.
Schedule Driven <sup>1</sup>	The rule conditions are evaluated according to a schedule (either a PulseNET pre-defined schedule you choose or a custom schedule you define). The functionality for defining a custom schedule for a rule is the same as that for defining a custom schedule for a report. For information on how to define a custom schedule, see the procedures in “Working with PulseNET Reports” in the <i>PulseNET User's Guide</i> .

<sup>1</sup> This triggering type is currently not supported.

<sup>2</sup> This is the recommended triggering type.

### Topology Types

For each custom rule, you must select one PulseNET topology type for which the rule is defined. A topology type represents a PulseNET object or group of PulseNET objects. The following table lists and describes examples of the topology types, which are available on the Rule Definition tab of the Create Rule view.

Topology Type	Description
MercuryAccessPoint	This topology type represents all PulseNET-monitored Mercury access points.
MercuryRemote	This topology type represents all PulseNET-monitored Mercury remotes.
Mercury900AccessPoint	This topology type represents all PulseNET-monitored Mercury 900 access points.
Mercury900Remote	This topology type represents all PulseNET-monitored Mercury 900 remotes.
INetAccessPoint	This topology type represents all PulseNET-monitored INet access points.
INetRemote	This topology type represents all PulseNET-monitored INet remotes.
INet2AccessPoint	This topology type represents all PulseNET-monitored INet2 access points.
INet2Remote	This topology type represents all PulseNET-monitored INet2 remotes.
PnSdRadioDetail	This topology type represents all PulseNET-monitored Dlink devices.
PnSdAccessPoint	This topology type represents all PulseNET-monitored Dlink access points.
PnSdRemote	This topology type represents all PulseNET-monitored Dlink remotes.
PnLanDeviceDetail	This topology type represents all PulseNET-monitored LAN devices.
PnCiscoDeviceDetail	This topology type represents all PulseNET-monitored Cisco devices

Topology Type	Description
Intrepid	This topology type represents all PulseNET-monitored Intrepid devices.

---

**Note** All topology types from the PulseNET topology model are listed in the Topology Type list. Most are not recommended for creating custom rules.

---

To exclude Cisco devices from a LAN device custom rule, you need to specify the following under Rule Scope on the Rule Definition tab:

```
PnLanDeviceDetail where topologyTypeName<>'PnCiscoDeviceDetail'
```

### Email Actions

You can configure an email action to forward a custom rule alert to one or more email addresses.

---

**Note** Before you configure email actions, you must first configure email settings. For information on how to configure email settings, see [“Email Configuration”](#) on page 18.

---

*To configure an email action to forward an alert:*

- 1 Navigate to the Rules view (**Administration > Rules and Alerts**) and click the **Custom Rules** tab.  
The **Custom Rules** list appears.
- 2 For the rule to which you want to add an e-mail action, click the **Edit** icon.  
The **Edit Rule** view appears. The **Edit Rule** view has the same functionality as the **Create Rule** view. For information on this functionality, see [“Creating Custom PulseNET Rules”](#) on page 83.
- 3 Navigate to the **Conditions, Alerts & Actions** tab.
- 4 For a multiple-severity rule, click the severity level (Warning, Critical, Fatal) bar for which you want to configure an email action. For a simple rule, click the Fire bar.  
**Note** Multiple-severity is the recommended rule type.
- 5 Click the **Action** tab.

6 Define the action type.

**Note** PulseNET can initiate the email action when the rule condition becomes valid (enters) or when the rule condition is no longer valid (exits).

Select one of the following Action Type options: **Entering** or **Exiting**.

7 Select **EmailAction** from the list provided.

8 **Optional.** In the Description field, add a description of the action.

9 Click **Add**.

The email action is added.

10 From the Actions list, click the new **EmailAction** link.

The action parameters appear.

11 Define the email recipient(s).

a Locate the mail.recipient parameter and click the link to its value.

b From the Registry Variables list, select the mail.recipient registry variable.

The mail.recipient registry variable corresponds to the mail recipient(s) configured in the PulseNET email settings. For information on how to configure PulseNET email settings, see [“Email Configuration”](#) on page 18.

c Click **Close**.

12 Define the email subject.

a Locate the mail.subject parameter and click the link to its value.

b Click the **User Defined** tab.

c Type an appropriate subject (for example, the name of the rule) in the field provided.

d Click **Close**.

13 Define the email message.

a Locate the mail.message parameter and click the link to its value.

b From the Rule/System Variables list, select the message variable.

A message variable for a custom PulseNET rule is user-defined. For information on how to define a message variable, see [step 26](#) to [step 33](#) in [“Example 1: Add a rule that raises an alert when a metric drops below a certain value.”](#) on page 83.

If you choose the message variable for the mail.message parameter, the e-mail message is the same as the alert message.

- c Click **Close**.

14 Click **Save All** at the bottom of the **Conditions, Alerts & Actions** tab.

Now an email is sent to the email address(es) configured when either the associated rule condition becomes valid or the associated rule condition is no longer valid (depending on the action type you defined in [step 6](#)).

### SNMP Trap Actions

You can configure an SNMP trap action to forward a custom rule alert to a remote SNMP trap receiver.

---

**Note** Before you configure SNMP trap actions, you must first enable SNMP trap actions and provide a community string and a target address for the remote SNMP trap receiver. For information on how to configure SNMP trap action settings, see “[SNMP Trap Action Configuration](#)” on page 20.

---

*To configure an SNMP trap action to forward an alert:*

- 1 Navigate to the Rules view (**Administration > Rules and Alerts**) and click the **Custom Rules** tab.  
The **Custom Rules** list appears.
- 2 For the rule to which you want to add an SNMP trap action, click the **Edit** icon.  
The **Edit Rule** view appears. The **Edit Rule** view has the same functionality as the **Create Rule** view. For information on this functionality, see “[Creating Custom PulseNET Rules](#)” on page 83.
- 3 Click the **Rule Variables** tab.
- 4 Make sure the variable type is Message.
- 5 Under name, type a name in the following format: snmpEmbedded<*Severity*> (where <*Severity*> is the rule severity for which you are configuring an SNMP trap action). Example: snmpEnabledWarning.
- 6 In the Expression field, define the variable to be true.
- 7 Click **Add**.

The new variable is added. Make sure the change is saved.

- 8 When you are finished making the change, click **Rules and Alerts** in the breadcrumbs at the top of the screen to return to the **Custom Rules** list.

Now an SNMP trap is sent to the designated SNMP trap receiver when the associated rule condition becomes valid.

## Editing a Custom Rule

You can edit custom rules.

*To edit a custom rule:*

- 1 Navigate to the Rules view (**Administration > Rules and Alerts**) and click the **Custom Rules** tab.  
The **Custom Rules** list appears.
- 2 Click the **Edit** icon in the row of the rule you want to edit.  
The **Edit Rule** view appears. The **Edit Rule** view has the same functionality as the **Create Rule** view. For information on this functionality, see “[Creating Custom PulseNET Rules](#)” on page 83.
- 3 Using the available tabs, make the change(s) you want to the rule. Make sure any changes you make on a tab are saved before you move to another tab.
- 4 When you are finished making the change(s), click **Rules and Alerts** in the breadcrumbs at the top of the screen to go back to the **Custom Rules** list.

## Removing a Custom Rule

You can delete custom rules.

*To delete a custom rule:*

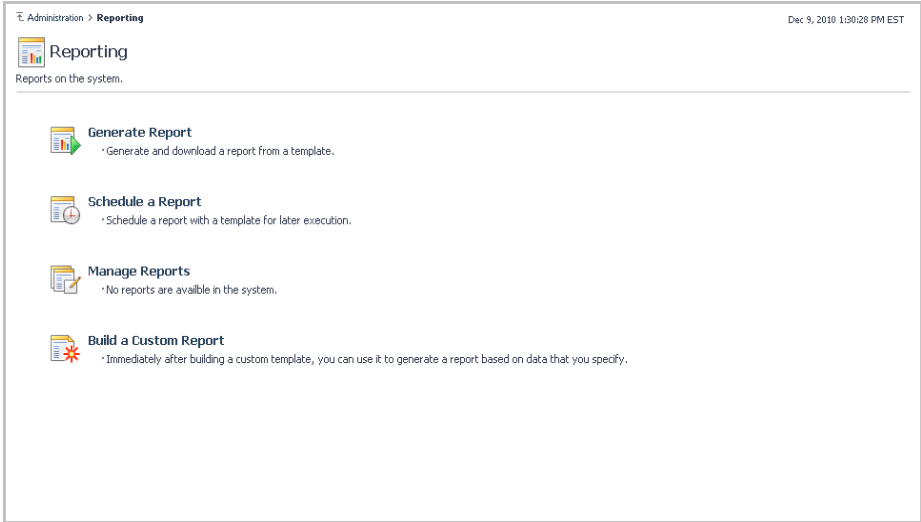
- 1 Navigate to the Rules view (**Administration > Rules and Alerts**) and click the **Custom Rules** tab.  
The **Custom Rules** list appears.
- 2 Click the **Remove** icon in the row of the rule you want to remove.  
A dialog box appears asking if you are sure.
- 3 Click **Delete**.



# Working with Reports

This chapter describes how to use the Reporting view (**Administration > Reporting**) for:

- [Generating a Report](#)
- [Scheduling a Report](#)
- [Managing Reports](#)
- [Building Custom Reports](#)



The screenshot shows the 'Reporting' view within an 'Administration' menu. The page title is 'Reporting' and the subtitle is 'Reports on the system.' The date and time are 'Dec 9, 2010 1:30:28 PM EST'. There are four main sections, each with an icon and a description:

- Generate Report**: Represented by a bar chart icon with a green arrow. Description: 'Generate and download a report from a template.'
- Schedule a Report**: Represented by a calendar icon with a clock. Description: 'Schedule a report with a template for later execution.'
- Manage Reports**: Represented by a document icon with a pencil. Description: 'No reports are available in the system.'
- Build a Custom Report**: Represented by a document icon with a starburst. Description: 'Immediately after building a custom template, you can use it to generate a report based on data that you specify.'

## Generating a Report

As a PulseNET administrator, you can generate the various PulseNET reports.

To generate a report, from the Reporting view (**Administration > Reporting**) click **Generate Report** and then follow the instructions under “Generate a New Report” in “Working with PulseNET Reports” in the *PulseNET User's Guide*.

## Scheduling a Report

As a PulseNET administrator, you can schedule PulseNET reports to run in the future.

To schedule a report, from the Reporting view (**Administration > Reporting**) click **Schedule a Report** and then follow the instructions under “Schedule a Report to Run in the Future” in “Working with PulseNET Reports” in the *PulseNET User's Guide*.

## Managing Reports

Generated and scheduled reports are listed in the Manage Reports view (**Administration > Reporting > Manage Reports**).

Execution	Name	Template	Schedule	Format	Size (bytes)
Oct 1, 2010 12:00:00 AM	AP Overview 1	Access Point/Master Overview (Report)	Beginning of the month	PDF	Run now...
Sep 28, 2010 3:00:00 AM	Test Run 1	Availability For All Devices (Report)	Off-Hours Database Maintenance	PDF	Run now...
Sep 11, 2010 12:00:00 AM	Test Run 2	Availability For Monitored Access Points/Masters (Report)	Daily Off Hours	PDF	Run now...

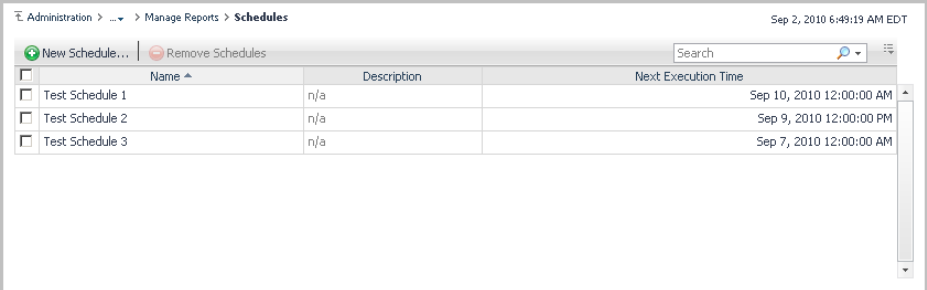
You can use the Manage Reports view to perform a number of report-related tasks.

For information about and procedures for the report-related tasks that are common to both operators and administrators, see “Working with PulseNET Reports” in the *PulseNET User's Guide*.

For information about and procedures for the report-related tasks only administrators can perform, see the “[Managing Report Schedules](#)” subsection.

## Managing Report Schedules

An administrator has access to the Manage Report Schedules view (**Administration > Reporting > Manage Reports > Schedules**).



<input type="checkbox"/>	Name ^	Description	Next Execution Time
<input type="checkbox"/>	Test Schedule 1	n/a	Sep 10, 2010 12:00:00 AM
<input type="checkbox"/>	Test Schedule 2	n/a	Sep 9, 2010 12:00:00 PM
<input type="checkbox"/>	Test Schedule 3	n/a	Sep 7, 2010 12:00:00 AM

You can use the Manage Report Schedules view to:

- [Create a New Schedule](#)
- [Delete an Administrator-Created Schedule](#)

---

**Note** The schedules that are provided with PulseNET cannot be deleted.

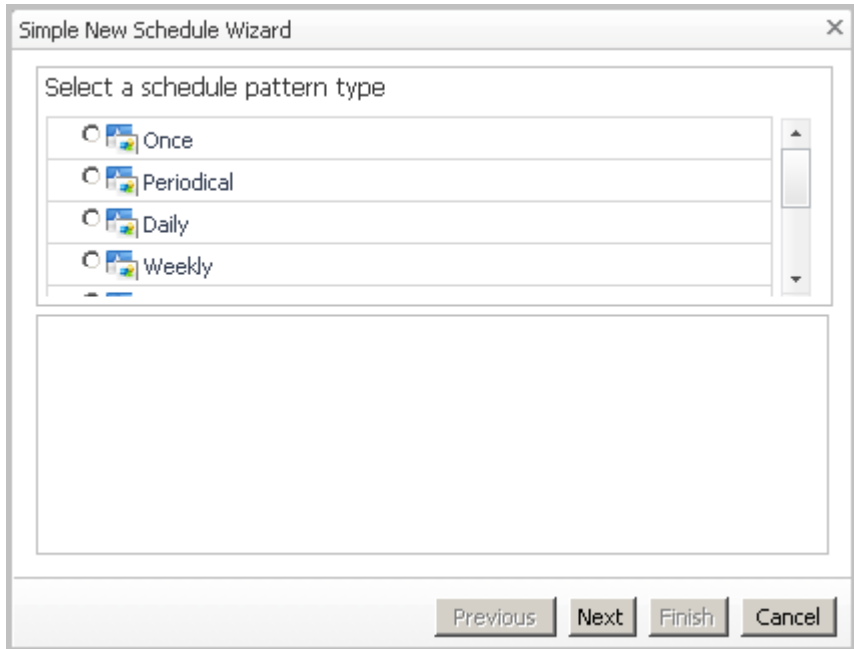
---

## Create a New Schedule

*To create a new schedule:*

- 1 Click **New Schedule...**

The New Schedule Wizard appears.



- 2 Create your new schedule using the New Schedule Wizard and click **Finish**.

Your schedule is added to the list of available schedules.

## Delete an Administrator-Created Schedule

*To delete and administer-created schedule:*

- 1 Click the check box next to the schedule's icon to select the schedule.  
The Delete icon becomes enabled.
- 2 Click the **Delete** icon.  
A dialog box appears and asks you if you are sure.
- 3 Click **Delete**.

# Building Custom Reports

As a PulseNET administrator, you can build a custom report.

## Build a Custom Report

The following instructions guide you through building a custom report.

*To begin building a custom report:*

- From the Reporting view (**Administration > Reporting**), click **Build a Custom Report**.

The **Add view** dialog box appears with a new blank report displayed in the background. The Add view dialog box is a wizard that assists you with adding a view to your report.

On the Add view dialog box, the available input data is displayed at the left and the available view styles are displayed at the right.

## Adding the First View to Your Custom Report

*To add the first view to your new custom report:*

- 1 With the Add view dialog box open, select a type of input data (a group of objects or an individual object) from the list provided (for example, **PN Operation > All Access Points**).

The view styles available for the type of input data you select are enabled at the right.

**Note** The Table view style is only available when you choose a group for the input data type. The Property view style is only available when you choose an individual object for the input data type.

- 2 Select the view style for displaying the data. The following table describes the available view styles.

**Important** The Table view style presents data the most efficiently and is the recommended view style.

View Style	Description
Metric View <sup>1</sup>	Choose metrics, for the input data item you selected, to be represented in a chart, as a gauge, or in a list.
Table View <sup>2</sup>	Choose metrics to be represented as the columns of a table, where each row in the table is an object from the group you selected for the input data item.
Property View <sup>1</sup>	Choose properties of the object you selected for the input data item to be displayed in a name-value list or as labels.
Pre-defined View Template <sup>1</sup>	Choose a pre-defined PulseNET view template to display data associated with the input data item you selected.

<sup>1</sup> This view style is currently not supported.

<sup>2</sup> This is the recommended view style.

- 3 Click **Next**.

If you selected Metric View, go to [step 4](#). If you selected Table View, go to [step 5](#). If you selected Property View, go to [step 6](#). If you selected View Template, go to [step 7](#).

- 4 Metric View steps:

- a From the list at the top left, select a metric, or a number of metrics, to be represented in a chart, on a gauge, or in a list.
- b At the bottom left, select the type of chart, gauge, or list.

A preview of how the data will be displayed in the report is shown at the right.

- c Click the **Common** tab.
- d **Optional.** Add a title for the view and adjust the height of the title.
- e Click the **Metric Labels** tab.

- f **Optional.** For the metric(s) you selected, select a metric label from the list(s) provided.
  - g There may only be one metric label in a list, depending on the metric(s) you selected.
  - h **Optional.** For the metric(s) you selected, select a parent label from the list(s) provided.
  - Note** There may only be one parent label in a list, depending on the input data you selected.
  - i Click the **Options** tab.
  - j **Optional.** Set the available metric view parameters. For descriptions of the available parameters, see [Appendix: Custom Report Metric View Parameters](#).
  - k Proceed to [step 8](#).
- 5 Table View steps:
- a From the list provided, select the properties you want to appear in the view.
  - b Click **Next**.
  - c **Optional.** Alter order of the columns and the label of and alignment within each column, and select a renderer (Current Average, Period Average, or Sparkline) for the data for each metric.
  - d Click **Next** to preview the new view.
  - e Click **Next**.
  - f **Optional.** Specify rules to filter the selected data.
  - g Proceed to [step 8](#).
- 6 Property View steps:
- a From the list at the left, select the properties you want listed in the view.
  - b Select the view style for displaying the properties in the view.
  - c Click **Next**.
  - d **Optional.** Add a title for the view.
  - e **Optional.** If you selected Name-Value List as the view style, alter the list order, select a renderer (Current Average, Period Average, or Sparkline) for the data for each metric you added and then click **Next** to preview the new view.
- If you selected Property Renderer as the view style, alter the list order, add the same preceding text for all properties, configure the preceding text style, select

a renderer (Current Average, Period Average, or Sparkline) for the data for each metric you added, add following text to the properties, and configure the following text style(s).

f Proceed to [step 8](#).

7 View Template steps:

a From the list at the left, select a pre-defined report view template.

A preview of how data will be displayed in the report view is shown at the right.

b Click the **Common** tab.

c **Optional.** Add a title for the view.

d Proceed to [step 8](#).

8 Click **Finish**.

The first view is added to the report.

### Adding Another View to Your Custom Report

*To add another view to your report using the Add view dialog box:*

- Click **Add view** to access the Add view dialog box and follow the steps in “[Adding the First View to Your Custom Report](#)” on page 103.

*To add another view to your report using the drag and drop functionality:*

- 1 Click the arrow at the far right of the PulseNET interface to open the Action panel.
- 2 On the Action panel, click the **Data** tab.
- 3 From the list of data, select a data item for the input data and drag the data item to the custom report workspace.

A popup appears with three of the following four view style choices: **Select metrics**, **Create a table**, **Select properties**, and **Select a view**. These choices correspond to the four view styles described in the table in “[Adding the First View to Your Custom Report](#)” on page 103.

**Note** Create a table is only available when you choose a group for the input data type. Select properties is only available when you choose an individual object for the input data type.

- 4 Select the view style for displaying the properties in the view.

The **Create view** dialog box appears.

- 5 If you chose Select metrics, go to [step 4](#) of “[To add the first view to your new custom report:](#)” on page 103 and follow the rest of that procedure. If you chose Create a table, go to [step 5](#) and follow the rest of the procedure. If you chose Select properties, go to [step 6](#) and follow the rest of the procedure. If you chose Select a view, go to [step 7](#) and follow the rest of the procedure.

### Changing the Name of Your Custom Report

*To change the name of your custom report:*

- 1 Click the name of the report at the top of the custom report workspace.
- 2 Enter a new name and press **Enter** on the keyboard.

### Adding Text to the First Page of Your Custom Report

*To add text to the first page of your custom report:*

- 1 Click **Add text** near the top of the custom report workspace.  
The **Entering User Text** dialog box appears.
- 2 **Optional.** Select a style for the text from the list provided.
- 3 Enter the text in the field provided.
- 4 **Optional.** Click the **Background Image** icon to provide a background image.  
Provide a valid URL to an image, select one from the tree provided, or upload an image, and then click **OK**.
- 5 Click **OK**.

### Adding a Header or Footer to Your Custom Report

*To add a header to the pages of your custom report:*

- 1 Click **Header** near the top of the custom report workspace.  
The **Customize Header** dialog box appears.
- 2 Define a header using the controls provided.
  - a Click the left, center, and/or right field(s) provided and add your own text.
  - b **Optional.** Add variables using the controls provided at the top of the dialog box.
- 3 Click **OK**.

*To add a footer to the pages of your custom report:*

- 1 Click **Footer** near the top of the custom report workspace.  
The **Customize Footer** dialog box appears.
- 2 Define a footer using the controls provided.
  - a Click the left, center, and/or right field(s) provided and add your own text.
  - b **Optional.** Add variables using the controls provided at the top of the dialog box.
- 3 Click **OK**.

### Configuring Report Properties

*To configure report properties:*

- 1 Click **Properties** near the top of the custom report workspace.  
The **Edit Properties** dialog box appears.
- 2 **Optional.** Edit the name of the report.
- 3 **Optional.** Click the Relevant Role(s) icon to define the relevant roles for the report.
- 4 **Optional.** Click the Allowed Role(s) icon to define the roles allowed to see the report.
- 5 **Optional.** Provide a descriptive tool tip message for the report.
- 6 **Optional.** Click the Background Image icon to provide a background image.  
Provide a valid URL to an image, select one from the tree provided, or upload an image, and then click **OK**.
- 7 Select the check box at the bottom of the dialog box if you want this report to be able to be included in other reports.
- 8 Click **OK**.

### Running a New Custom Report

*To run the new custom report:*

- 1 Click **Run report** near the top of the custom report workspace.
- 2 **Optional.** Click the **Time Range** icon and select **Time Range** from the list to edit the time range.  
The Edit - timeRange dialog box appears.

Adjust the time range settings and click **Set**.

**3 Optional.** Edit the name of the report.

**Note** This alters the name of the report for this run only. It does not change the name of the report permanently.

**4 Optional.** Select a report format from the list provided.

**5 Optional.** Provide a comma-separated list of e-mail recipients.

**6** Click **Run**.

### Scheduling a Custom Report

*To schedule the custom report:*

- To schedule the report, click **Schedule report** near the top of the custom report workspace and then follow the instructions under “Schedule a New Report to run in the Future” in “Working with PulseNET Reports” in the *PulseNET User’s Guide*.



# Working with Users

This chapter describes how to use the Users view (**Administration > Users**) for:

[Creating a User](#)

[Searching for a User](#)

[Managing Users](#)

[Configuring Password Settings](#)

[Configuring User Session Timeout](#)

The screenshot shows the 'Administration > Users' dashboard. At the top left, it says 'Administration > Users' and at the top right, the date and time 'Aug 30, 2010 1:41:25 PM EDT'. Below the breadcrumb is a 'Users' header with a user icon and the text 'Use this dashboard to manage users, and configure password policy settings.' The main content area contains five sections:

- User Look Up**: Includes a search icon, the text 'Enter part of the user name.', a text input field, and a 'Lookup' button.
- Create New User**: Includes a user icon with a plus sign and the text 'Invoke a wizard and follow the steps to create users.'
- Manage Users**: Includes a group of user icons and the text 'There are 2 users in the system.'
- Password Policy Settings**: Includes a document icon with a key and the text 'Use the Configure Password Settings dashboard to edit any policies that you want to change.'
- User Session Settings**: Includes a clock icon and the text 'Configure how long users are allowed to be inactive before they are logged out.' and 'Currently users are logged out after 60 minutes.'

## Creating a User

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

*To create a new PulseNET user from the Users view:*

- 1 Navigate to **Administration > Users**.

**Note** You can also create new PulseNET users from the Manage Users view. For information about how to create PulseNET users from the Manage Users view, "[Create a New User](#)" on page 116.

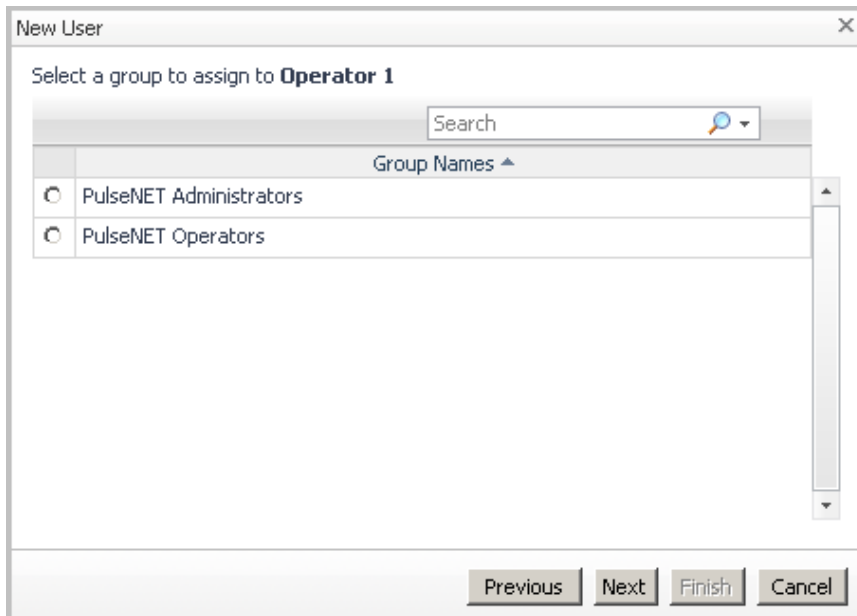
- 2 Click **Create New User**.

A wizard appears and prompts you to provide a name for the new user.

- 3 Enter a name for the new user and click **Next**.

**Note** At any time you can click **Previous** to go back to the previous step.

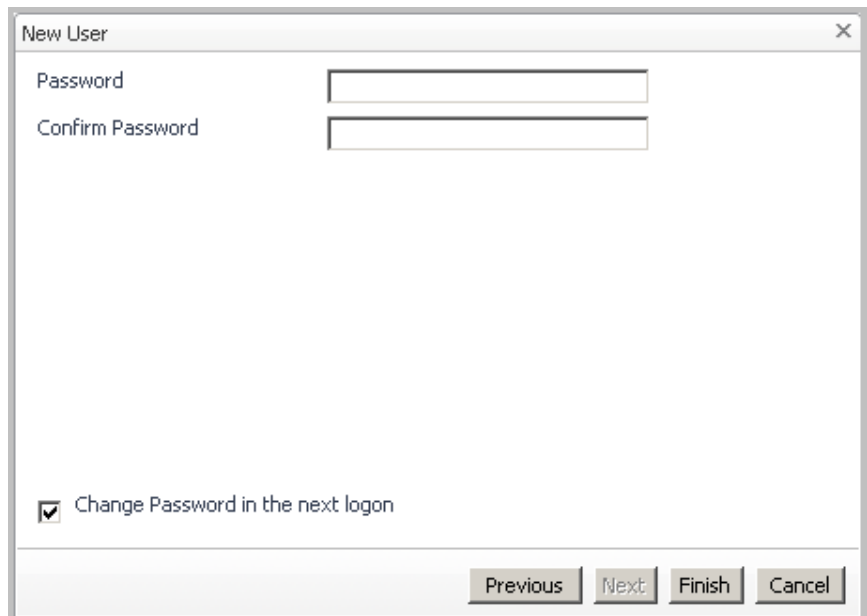
The wizard prompts you to assign the new user to a group.



**Note** A user can be an administrator or an operator, but not both. Administrators have access to all operator functionality.

- 4 Assign the new user to a group and click **Next**.

The wizard prompts you to provide a password for the new user. The password requirements depend on configurable password settings. For more information, see “[Configuring Password Settings](#)” on page 122.



The screenshot shows a dialog box titled "New User" with a close button (X) in the top right corner. It contains two text input fields: "Password" and "Confirm Password". Below these fields is a checkbox labeled "Change Password in the next logon", which is currently checked. At the bottom right of the dialog box, there are four buttons: "Previous", "Next", "Finish", and "Cancel".

- 5 Type the same password in each of the fields (**Password** and **Confirm Password**) provided.

**Note** If you want the new user to change the password at first login, leave the check box at the bottom left selected. If not, clear the check box.

- 6 Click **Finish**.

The new user appears in the Manage Users list (**Administration > Users > Manage Users**).

## Searching for a User

You can search the system for a user by using the User Look Up field in the Users View.



---

**Note** You can also search the system for a user from within the Manage Users view. For information about how to search for a user from within the Manage Users view, "[Search for a User](#)" on page 116.

---

*To search the system for a user using the User Look Up field:*

- 1 Enter all or part of the user's name in the **User Look Up** field.
- 2 Click **Look up**.

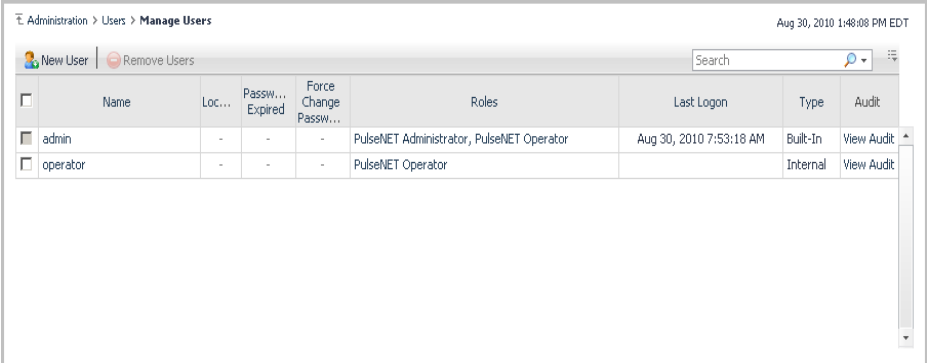
If only one user name matches what you entered, the details for that user appear. If more than one user name matches what you entered, a dialog box, listing the user names that match, appears.

- 3 If you are presented with a dialog box, select (click to highlight) a user and click **View Detail**.

The details for the user you selected appear.

# Managing Users

Users are listed in the Manage Users view (**Administration > Users > Manage Users**).



<input type="checkbox"/>	Name	Loc...	Passw... Expired	Force Change Passw...	Roles	Last Logon	Type	Audit
<input checked="" type="checkbox"/>	admin	-	-	-	PulseNET Administrator, PulseNET Operator	Aug 30, 2010 7:53:18 AM	Built-In	View Audit
<input type="checkbox"/>	operator	-	-	-	PulseNET Operator		Internal	View Audit

In the Manage Users view, you can:

- [Sort the Manage Users List](#)
- [Search for a User](#)
- [Filter the Manage Users List](#)
- [Create a New User](#)
- [View the Configuration Details for an Existing User](#)
- [Edit the Configuration of an Existing User](#)
- [Copy the Configuration of an Existing User for Creating a New User](#)
- [Change the Password of an Existing User](#)
- [Expire the Password of an Existing User](#)
- [Remove a User](#)

## Sort the Manage Users List

To sort the Manage Users list by a particular column heading, click that column heading. An arrow beside that column heading indicates the order (ascending or descending) in which the users are sorted.

## Search for a User

Use the Search tool at the top right of the Manage Users list to search for a specific user. For instructions on how to use the Search tool, see “Working with Tables” in the *PulseNET Quick Start Guide*.

## Filter the Manage Users List

Use the Search tool at the top right of the Manage Users list to filter the list. For instructions on how to use the Search tool, see “Working with Tables” in the *PulseNET Quick Start Guide*.

## Create a New User

To create a new user, click New User at the top left of the Manage Users view and then follow the instructions in “[Creating a User](#)” on page 112.

## View the Configuration Details for an Existing User

*To view the configuration details of an existing user:*

- 1 Click the user's name.  
A popup menu appears.
- 2 Click **View**.  
The configuration details for the user appear.

## Edit the Configuration of an Existing User

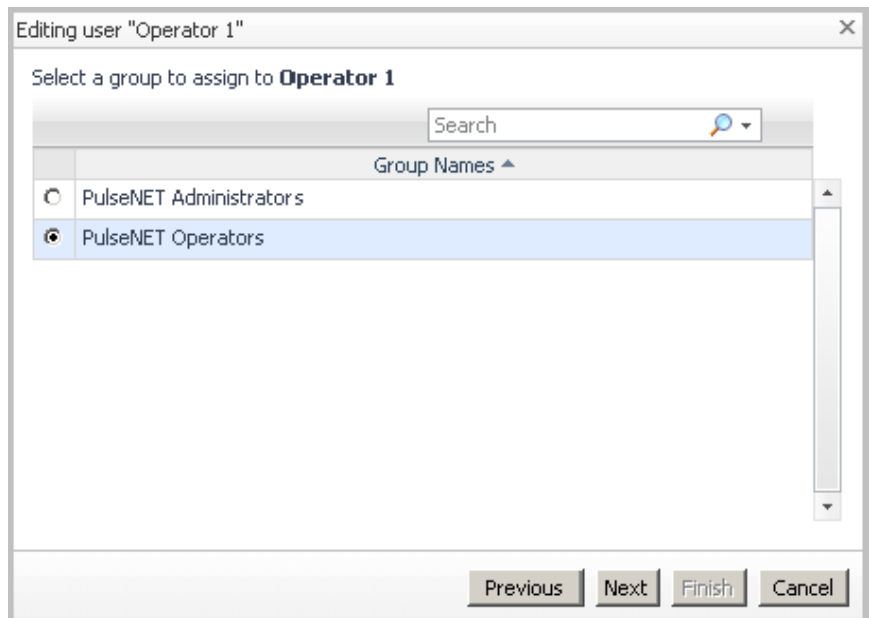
*To edit the configuration of an existing user:*

- 1 Click the user's name.  
A popup menu appears.
- 2 Click **Edit**.  
A wizard appears and prompts you to alter the name of the user if you want.
- 3 If you want to alter the name of the user, do so. If not, skip to the next step.

**4** Click **Next**.

**Note** At any time you can click **Previous** to go back to the previous step.

The wizard prompts you to assign the user to a different group.

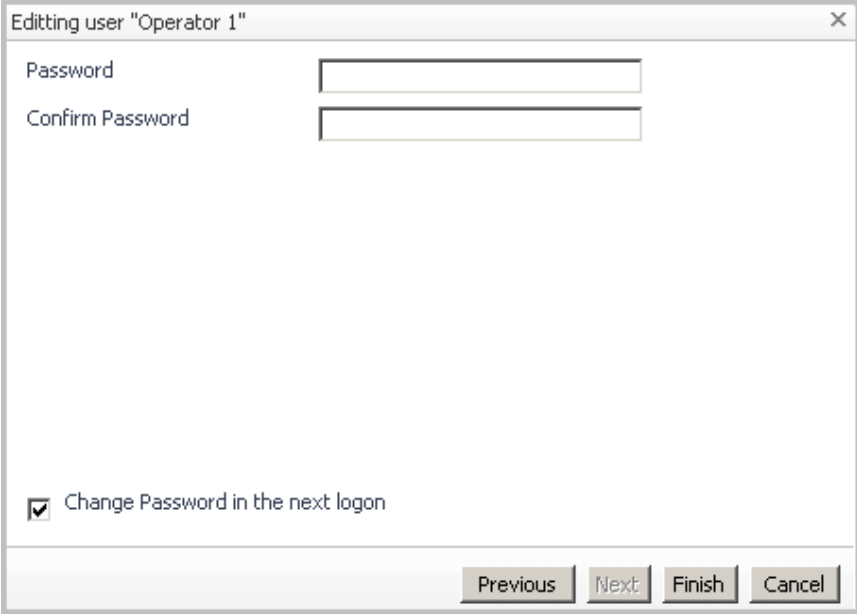


**Note** A user can be an administrator or an operator, but not both. Administrators have access to all operator functionality.

**5** **Optional.** Assign the user to a different group.

**6 Click Next.**

The wizard prompts you to alter the password for the user. The password requirements depend on configurable password settings. For more information, see [“Configuring Password Settings”](#) on page 122.



Editing user "Operator 1" [X]

Password [ ]

Confirm Password [ ]

Change Password in the next logon

Previous Next Finish Cancel

**7** If you want to alter the user's password, type the new password in each of the fields (**Password** and **Confirm Password**) provided.

**8 Click Finish.**

The edited user appears in the Manage Users list (**Administration > Users > Manage Users**).

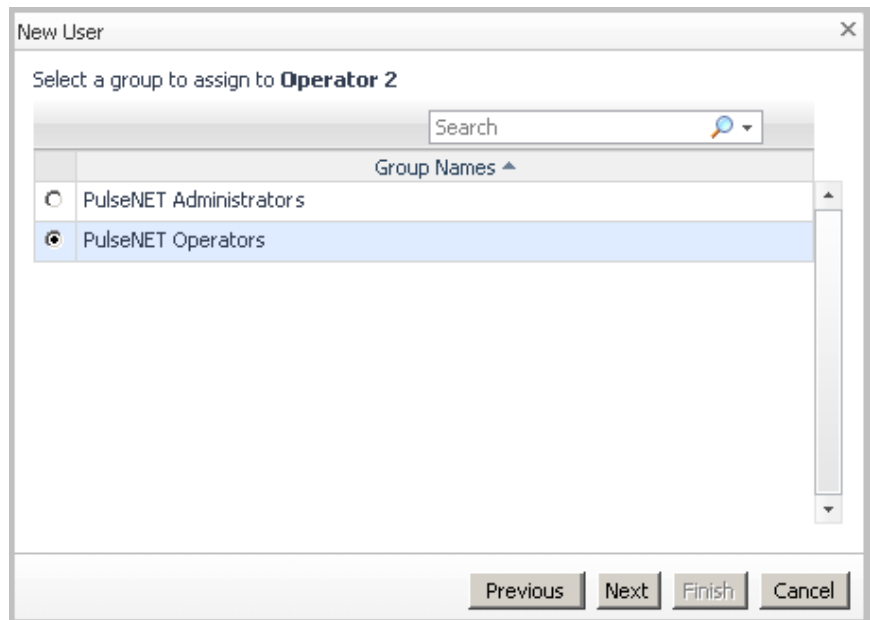
## Copy the Configuration of an Existing User for Creating a New User

*To copy the configuration of an existing user for creating a new user:*

- 1 Click the user's name.  
A popup menu appears.
- 2 Click **Copy**.  
A wizard appears and prompts you to enter a name for the new user.
- 3 Enter a name for the new user and click **Next**.

**Note** At any time you can click **Previous** to go back to the previous step.

The wizard prompts you to assign the user to a group.

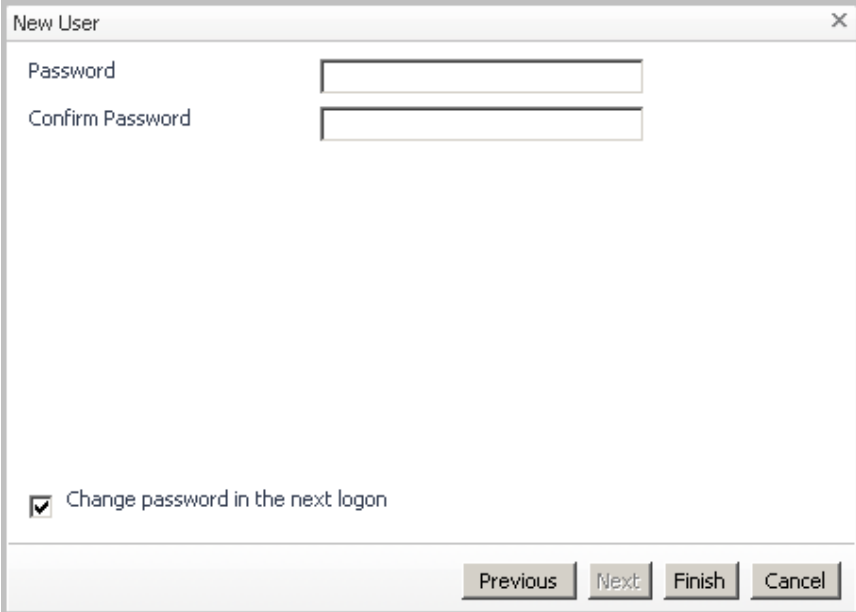


**Note** A user can be an administrator or an operator, but not both. Administrators have access to all operator functionality.

- 4 **Optional.** Assign the user to a different group.

**5 Click Next.**

The wizard prompts you to provide a password for the new user. The password requirements depend on configurable password settings. For more information, see [“Configuring Password Settings”](#) on page 122.



The screenshot shows a dialog box titled "New User" with a close button (X) in the top right corner. The dialog contains two text input fields: "Password" and "Confirm Password". Below these fields is a checked checkbox labeled "Change password in the next logon". At the bottom right, there are four buttons: "Previous", "Next", "Finish", and "Cancel".

**6 Type the new password in each of the fields (**Password** and **Confirm Password**) provided.**

**Note** If you want the new user to change the password at first login, leave the check box at the bottom left selected. If not, clear the check box.

**7 Click **Finish**.**

The new user appears in the Manage Users list (**Administration > Users > Manage Users**).

## Change the Password of an Existing User

*To change the password of an existing user:*

- 1 Click the user's name.  
A popup menu appears.
- 2 Click **Change Password**.  
A dialog box appears.
- 3 Type the new password in each of the fields (**Password** and **Confirm Password**) provided.
- 4 Click **Change**.

## Expire the Password of an Existing User

*To expire the password of an existing user:*

- 1 Click the user's name.  
A popup menu appears.
- 2 Click **Expire Password**.  
A dialog box appears.
- 3 Click **Change Password Next Logon** to force the user to change the password.  
A notification icon appears in the Force Change Password column for the user.

## Remove a User

*To remove one or more users:*

- 1 Click the check box next to the user's icon to select the user. Click multiple check boxes to select multiple users to be removed.  
The Delete icon becomes enabled.
- 2 Click the **Delete** icon.  
A dialog box appears and asks you if you are sure.
- 3 Click **Delete**.

## Configuring Password Settings

As an administrator, you can configure a number of password settings from the Configure Password Settings view (**Administration > Users > Password Policy Settings**). The following password settings are configurable:

Password Setting	Default Setting
Days before user password expires	90
Days before administrator password expires	45
Bad logins before user account is locked out	5
Seconds after which lockout expires (0 for no expiration)	900
Minimum password length	7
Number of old passwords that will be remembered	12
Maximum user name length	15
Number of days before password expiry to warn user	15
All other user's password complexity level <ul style="list-style-type: none"><li>• 1: password must be seven or more characters in length and contain at least one alpha and one numeric character</li><li>• 2: password must be seven or more characters in length and contain at least one alpha, one numeric, and one upper case character</li><li>• 3: password must be seven or more characters in length and contain at least one alpha, one numeric, one upper case, and one special character</li></ul>	1

Password Setting	Default Setting
Admin password complexity level <ul style="list-style-type: none"><li>• 1: password must be seven or more characters in length and contain at least one alpha and one numeric character</li><li>• 2: password must be seven or more characters in length and contain at least one alpha, one numeric, and one upper case character</li><li>• 3: password must be seven or more characters in length and contain at least one alpha, one numeric, one upper case, and one special character</li></ul>	2
User cache expiry in minutes (login is fast until cache expires)	600

*To configure one of the password settings:*

- 1 Navigate to **Administration > Users > Password Policy Settings**.
- 2 Click the value of the password setting you would like to change.  
A dialog box appears.
- 3 Make the change.
- 4 Click **Save**.

*To configure a number of password settings:*

- 1 Navigate to **Administration > Users > Password Policy Settings**.
- 2 Click **Edit** at the top left.  
The Settings Editor dialog box appears.
- 3 Make your changes.
- 4 Click **Save**.

## Configuring User Session Timeout

As an administrator, you can configure the user session timeout (**Administration > Users > User Session Settings**).

*To configure the user session timeout:*

- 1 Navigate to **Administration > Users > User Session Settings**.

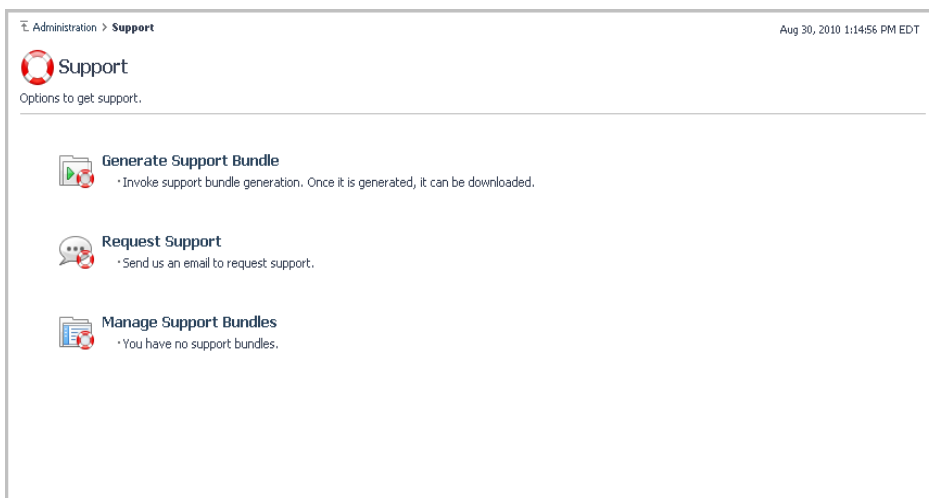
The Change User Session Timeout dialog box appears.

- 2 In the field provided, enter the number of minutes after which a user will be logged out.
- 3 **Optional.** If you do not want users to ever be logged out automatically, select the check box toward the bottom of the dialog box.
- 4 Click **Ok**.

# Support

This chapter describes how to use the Support view (**Administration > Support**) for:

- [Generating a Support Bundle](#)
- [Requesting Support](#)
- [Managing Support Bundles](#)



The screenshot shows the 'Support' view within the 'Administration' section. The breadcrumb navigation is 'Administration > Support'. The page title is 'Support' with a red circular icon containing a white 'S'. Below the title, it says 'Options to get support.' There are three main options listed, each with an icon and a description:

- Generate Support Bundle**: Represented by a document icon with a red circle and a green arrow. Description: 'Invoke support bundle generation. Once it is generated, it can be downloaded.'
- Request Support**: Represented by a speech bubble icon with a red circle and a white 'S'. Description: 'Send us an email to request support.'
- Manage Support Bundles**: Represented by a document icon with a red circle and a white 'S'. Description: 'You have no support bundles.'

## Generating a Support Bundle

You can request diagnostic data from PulseNET. The data gets saved as a collection of files, in the .ZIP format, called a support bundle.

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

*To generate a support bundle:*

- 1 From the Support view (**Administration > Support**), click **Generate Support Bundle**.

PulseNET creates the .ZIP file in the `<pulsenet_home>/support/<user_name>` directory on the computer hosting PulseNET.

- 2 To download the new support bundle now, click **Download Now**.

The support bundles you download are listed in the Manage Support Bundles view (**Administration > Support > Manage Support Bundles**). For information about managing support bundles, see “[Managing Support Bundles](#)” on page 128.

## Requesting Support

You can request support for PulseNET through email.

To request support through email, it is best practice to first configure PulseNET email settings. For instructions on how to configure PulseNET email settings, see Chapter 2, “Configuring System Settings”. If you have not configured PulseNET email settings, PulseNET will open the support request for you to send through an external email client.

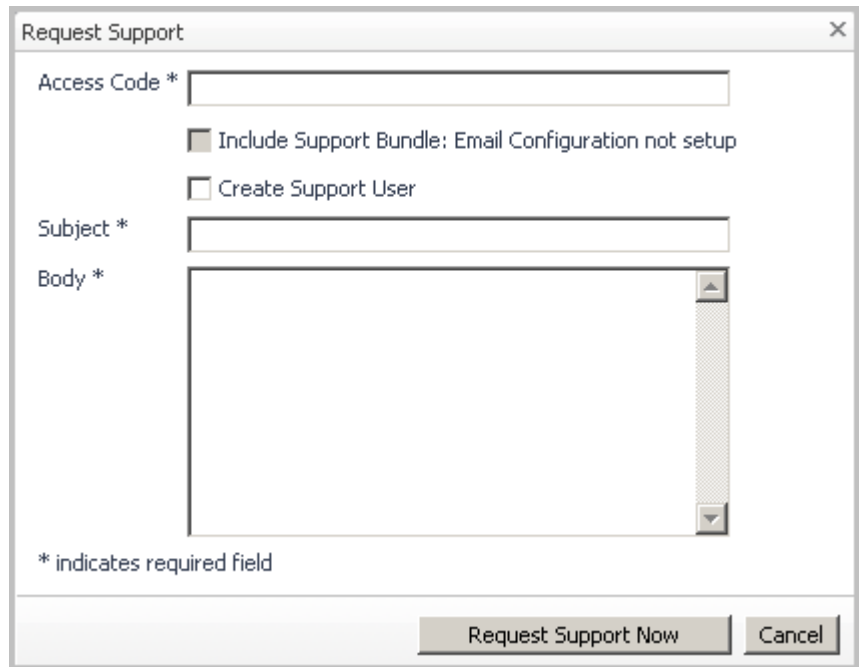
---

**Important** If you are requesting support through an external email client and you want to attach a support bundle to the request, you will have to generate and attach the support bundle manually. For information about how to generate a support bundle, see the “[Generating a Support Bundle](#)” section.

---

*To request support:*

- 1 From the Support view (**Administration > Support**), click **Request Support**.  
The Request Support dialog box appears.



The screenshot shows a dialog box titled "Request Support" with a close button (X) in the top right corner. The dialog contains the following fields and options:

- Access Code \***: A text input field.
- Include Support Bundle: Email Configuration not setup**
- Create Support User**
- Subject \***: A text input field.
- Body \***: A large text area with a vertical scrollbar on the right side.

At the bottom left of the dialog, there is a note: **\* indicates required field**. At the bottom right, there are two buttons: **Request Support Now** and **Cancel**.

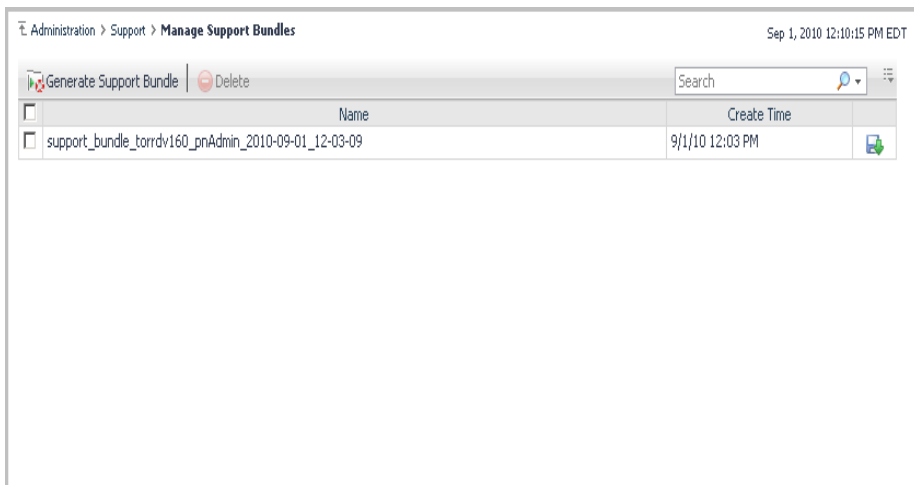
- 2 Type your customer number in the field provided.
- 3 Leave the **Include Support Bundle** check box selected if you want to include a support bundle.  
A support bundle will be generated and included in the support request.
- 4 Leave the **Create Support User** check box cleared, unless the Support team requests that you select it.
- 5 Type an appropriate subject in the **Subject** field.

- 6 Type a description of the problem in the **Body** field.
- 7 Click **Request Support Now**.

Your request for support is sent to the GE MDS Technical Support Department.

## Managing Support Bundles

Generated support bundles are listed in the Manage Support Bundles view (**Administration > Support > Manage Support Bundles**).



In the Manage Support Bundles view, you can:

- [Sort the Support Bundles List](#)
- [Search for a Generated Support Bundle](#)
- [Filter the Support Bundles List](#)
- [Generate a New Support Bundle](#)
- [Download a Generated Support Bundle](#)
- [Delete a Generated Support Bundle](#)

## Sort the Support Bundles List

To sort the support bundles list by name or create time, click the **Name** or **Create Time** column headings as required.

## Search for a Generated Support Bundle

Use the Search tool at the top right of the support bundles list to search for a specific generated support bundle. For instructions on how to use the Search tool, see “Working with Tables” in the *PulseNET Quick Start Guide*.

## Filter the Support Bundles List

Use the Search tool at the top right of the support bundles list to filter the list. For instructions on how to use the Search tool, see “Working with Tables” in the *PulseNET Quick Start Guide*.

## Generate a New Support Bundle

To generate a new support bundle, click Generate Support Bundle at the top left of the Manage Support Bundles view and then follow the instructions in “[Generating a Support Bundle](#)” on page 126.

## Download a Generated Support Bundle

*To download a generated support bundle:*

- 1 Click the size value for the generated support bundle at the far right of the support bundles list.

The Download Now button appears.

- 2 Click **Download Now**.

## Delete a Generated Support Bundle

*To delete a generated support bundle:*

- 1 Click the check box next to the support bundle's icon to select the support bundle.  
The Delete button becomes enabled.
- 2 Click **Delete**.  
A dialog box appears and asks you if you are sure.
- 3 Click **Delete**.

# A

## Appendix: Custom Report Metric View Parameters

The following tables list and describe the Metric View options.

### Metric View Chart Options

The options available depend on the type of chart you select.

Parameter	Description	Options
Use these settings as default	The configured settings are used as the default settings.	Check box
Metric value	Specifies the type of value to be displayed for one metric, or all metrics, in a chart.	None, Average, Minimum, Maximum
Show one chart per metric	A separate chart is displayed for each metric.	Check box
Only show axis of selected metric (different charts will line up)	Only the axes for the selected metric are displayed.	Check box
Show thresholds for selected metric	If a metric has a threshold, it is displayed.	Check box
Show data at both start and end of intervals	Data is shown at both the start and end of intervals. This applies only to plot and area charts.	Check box

Parameter	Description	Options
Honor bounds (calibrated max, unit bounds)	Sets the chart axes so that they do not go out of the chart boundaries.	Check box
On Select	Specifies what you want a select action to invoke.	Drilldown, Highlight
Show overall	Displays the overall value for the set time range as a dashed line.	Average, Min, Max
Show min/max as	Displays the minimum and maximum per interval.	Envelope, Marks, Lines
Show baseline min/max as	Displays the baseline minimum and maximum.	Envelope, Marks, Lines
Show standard deviation as	Highlights a range per interval.	Envelope, Marks, Lines
Standard deviation multiplier	Displays the high and low (that is, deviation from the average) values.	1, 2, 3
Show Average Line	Emphasizes the highest and lowest values.	Check box

### Metric View Gauge Options

The options available depend on the type of gauge you select.

Parameter	Description	Options
Use these settings as default	The configured settings are used as the default settings.	Check box
Indicator Size	Highlights a fluctuating value in your real-time application in a visually meaningful way.	Normal, Wider

Parameter	Description	Options
Bar Thickness	Determines the thickness of the bar.	Thinner, Normal, Thicker
Metric Value Source	Specifies the metric value to be displayed, the current value or the average over the configured period.	Metric Current, Metric Period

### Metric View List Options

The options available depend on the type of list you select.

Parameter	Description	Options
Use these settings as default	The configured settings are used as the default settings.	Check box
Show Sparkline	Displays a sparkline for each metric.	Check box.
Show Column For	Displays the columns you select.	Check boxes for: Min, Average, Max, Sum, Baseline Min, Baseline Max, Standard Deviation



# Index

## A

### access point

- failover
  - configuring* 57, 69
- redundancy
  - configuring* 57

### adding

- schedules 24

### Administration Home dashboard 14

### Administrator

- role 9

### alerts

- working with 77

### authorizing devices 57, 68

### availability

- data collection 56

## C

### Collection Configuration view 37

### Collection Scheduler view 53

### community string

- adding 39
- deleting 39

### configuration

- change
  - discovery* 62, 68
- data collection sample frequency 37, 53, 54
- Dlink 37
- email settings 18, 20

- rule thresholds 80

- SNMP 37, 38, 46

- system 28

### Configure Password Settings view 122

### configuring

- user password settings 111, 122

### copying

- schedules 22
- user configuration 119

### creating

- report schedules 102
- users 111, 112, 116

### credentials

- adding 40
- deleting 41
- editing 41

## D

### dashboards

- Administration Home 14

### data collection

- availability 56
  - specifying an interval* 55
- configuring sample frequency 37, 53, 54
- frequency 56
- performance 56
  - specifying an interval* 55

### decommissioning

- devices 73

### decommissioning devices 57

**deleting**

- licenses 33
- report schedules 103
- schedules 27
- support bundles 130

**Device Selection view** 57, 75**devices**

- authorizing 57, 68
- configuration
  - change* 62, 68
- decommissioning 57, 73
  - summary statistics* 73
- discovery 57, 76
- Dlink discovery 63
- filtering a list 76
- ineligible 62
- Ineligible Devices List 63
- maintenance windows
  - creating* 57
  - managing* 57
- managing 57, 75
- recommission
  - discovery* 62, 68
- recommissioning 73
- searching for 76
- SNMP discovery 58
- sorting a list 75

**discovery**

- configuration
  - change* 62, 68
- devices 57, 76
- Dlink devices 63
- progress 62, 68
- recommission
  - devices* 62, 68
- SNMP devices 58

**Dlink**

- adding a master seed 47
- configuring 37
  - advanced settings* 49
- deleting a master seed 48

- editing master seed settings 48

**Dlink Configuration view** 46**Dlink devices**

- schedule configuration
  - disabling* 55

**downloading**

- support bundles 129

**E****editing**

- schedules 22
- user configuration 116

**email settings**

- configuring 18, 20
- properties 19

**exporting**

- Ineligible Devices List 63

**F****failover**

- access point
  - configuring* 57, 69
- device
  - promoting* 70

**filtering**

- device lists 76
- Manage Users List 116
- master seed tables 53
- SNMP tables 46
- Support Bundles List 129

**G****generating**

- reports 99, 100
- support bundles 125, 126, 129

**I**

- ineligible devices** 62
- Ineligible Devices List**

exporting 63

## installing

licenses 29, 31, 33

## L

### licenses

deleting 33

installing 29, 31, 33

managing 29, 32

migrating devices 34

order, when authorizing devices 34

requesting 29

working with 29

Licensing view 29

logging in to PulseNET 13

## M

### maintenance windows

creating 57, 70

deleting 72

list 72

managing 57, 72

scheduling 71

Manage Licenses view 32

Manage Reports view 100

Manage Support Bundles view 128

### Manage Users List

filtering 116

searching 116

sorting 115

Manage Users view 115

### managing

devices 57, 75

licenses 29

report schedules 101

reports 99, 100

schedules 22

support bundles 125, 128

users 111, 115

managing licenses 32

### master seed

adding 47

deleting 48

editing settings 48

### master seed tables

filtering 53

searching 53

sorting 52

### metric view

parameters 131, 132, 133

### migrating devices

licenses 34

SNMP credentials 44

## O

### Operator

role 9

## P

### password

changing for a user 121

configuring user settings 111, 122

expiring for a user 121

### performance

data collection 56

### properties

email settings 19

## R

### recommission

devices

*discovery* 62, 68

### recommissioning

devices 73

### redundancy

access point

*configuring* 57

### removing

users 121

**report schedules**

- creating 102
- deleting 103
- managing 101

**Reporting view** 99**reports**

## custom

- adding a footer* 107
- adding a header* 107
- adding a view* 103, 106
- adding text* 107
- bulding* 103
- configuring properties* 108
- creating* 99
- editing* 99
- naming* 107
- running a report* 108
- scheduling a report* 109

- generating 99, 100
- managing 99, 100
- scheduling 99, 100

**requesting**

- licenses 29
- support 125, 126

**roles**

- Administrator 9
- Operator 9

**rule email notification**

- turning on or off 82

**rule thresholds**

- configuring 80

**rules**

## custom

- creating* 83
- deleting* 97
- editing* 97
- email actions* 94
- example* 83, 86, 88
- metric view*

**parameters** 131, 132, 133

- parameters* 91

*SNMP trap actions* 96

- topology types* 92
- triggering types* 91
- types* 91

- descriptions 78
- disabling 80
- email notification 82
- enabling 80
- SNMP trap actions 82
- thresholds 80
- working with 77

**Rules view** 77**S****schedule configuration**

- Dlink devices
- disabling* 55

**schedules**

- adding 24
- copying 22
- deleting 27
- editing 22
- managing 22

**scheduling**

- reports 99, 100

**searching**

- device lists 76
- Manage Users List 116
- master seed tables 53
- SNMP tables 46
- Support Bundles List 129
- users 111, 114

**server**

- starting 10
- stopping 12

**session**

- user
- timeout* 111, 123

**SNMP**

- adding a community string 39

- adding credentials 40
- configuring 37, 38, 46
- configuring advanced settings 42
- deleting a community string 39
- deleting credentials 41
- editing credentials 41
- migrating devices 44
- SNMP Configuration view** 38
- SNMP tables**
  - filtering 46
  - searching 46
  - sorting 45
- SNMP trap actions**
  - enabling 20
  - turning on or off 82
- sorting**
  - device lists 75
  - Manage Users List 115
  - master seed tables 52
  - SNMP tables 45
  - Support Bundles List 129
- starting the server** 10
- stopping the server** 12
- support**
  - requesting 125, 126
- support bundles**
  - deleting 130
  - downloading 129
  - generating 125, 126, 129
  - managing 125, 128
  - searching for 129
- Support Bundles List**
  - filtering 129
  - sorting 129
- Support view** 125
- system**
  - configuration 28

## T

- timeout

- user session 111, 123
- trigger delay value** 56

## U

### users

- changing a password 121
- configuing password settings 111, 122
- configuration details 116
- copying a configuration 119
- creating 111, 112, 116
- editing a configuration 116
- expiring a password 121
- Manage Users List 115, 116
- managing 111, 115
- removing 121
- searching for 111, 114
- Users view** 111

## V

### views

- Collection Configuration 37
- Collection Scheduler 53
- Configure Password Settings 122
- Device Selection 57, 75
- Dlink Configuration 46
- Licensing 29
- Manage Licenses 32
- Manage Reports 100
- Manage Support Bundles 128
- Manage Users 115
- Reporting 99
- Rules 77
- SNMP Configuration 38
- Support 125
- Users 111

**W****Windows**

- service, from the command line 12
- service, running PulseNET as a 11

## IN CASE OF DIFFICULTY...

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

Phone: 585 241-5510

E-mail: [gemds.techsupport@ge.com](mailto:gemds.techsupport@ge.com)

FAX: 585 242-8369

Web: [www.gemds.com](http://www.gemds.com)

