

MDS PulseNET

Network Management System

Version 2.2

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

MDS 05-6137A01, Rev. B
FEBRUARY 2011



Digital Energy
MDS

Quest Copyright Notice

© 2011 Quest Software, Inc.
ALL RIGHTS RESERVED.

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

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

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

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

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

Patents

This product includes patent pending technology.

Trademarks

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

Third Party Contributions

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

About Quest Software, Inc.

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

About GE MDS

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

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

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

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

GE MDS ISO 9001 Registration

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

To GE Customers

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

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

Manual Revision and Accuracy

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

Administrator's Guide
February 2011
Version 2.2

Table of Contents

| | |
|--|-----------|
| Introduction | 9 |
| 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 |
| Configuring E-mail Settings..... | 17 |
| Email Configuration | 17 |
| Working with Licenses | 21 |
| Requesting a License..... | 21 |
| Installing a License..... | 23 |
| Managing Licenses | 24 |
| Sort the Manage Licenses List | 24 |
| Search for an Installed License | 24 |
| Filter the Manage Licenses List..... | 25 |
| Install a New License..... | 25 |
| Delete an Installed License | 25 |
| Migrate Authorized Devices from an Expiring License to a New License | 26 |
| License Order when Authorizing Devices | 26 |
| Collection Configuration | 29 |
| SNMP Configuration..... | 30 |
| Add an SNMP v1 or v2c Community String..... | 31 |

| | |
|--|-----------|
| Delete an SNMP v1 or v2c Community String | 31 |
| Add SNMP v3 Credentials | 32 |
| Edit SNMP v3 Credentials | 33 |
| Delete SNMP v3 Credentials | 33 |
| Configure Advanced SNMP Settings | 34 |
| Migrate Devices from One Community String or Set of Credentials to Another | 36 |
| Sort an SNMP Table | 37 |
| Search for an SNMP Community String or Set of Credentials | 38 |
| Filter an SNMP Table | 38 |
| Dlink Configuration | 38 |
| Add a Dlink Master Seed | 39 |
| Edit Dlink Master Seed Settings | 40 |
| Delete a Dlink Master Seed | 40 |
| Configure Advanced Dlink Settings | 41 |
| Sort a Master Seed Table | 44 |
| Search for a Master Seed | 45 |
| Filter a Master Seed Table | 45 |
| Collection Management | 45 |
| Trigger Delay Values and Data Collection Frequency | 48 |
| Working with Devices | 49 |
| Discovering SNMP Devices | 50 |
| Discovery Progress | 54 |
| Ineligible Devices | 54 |
| Discovering Dlink Devices | 55 |
| Discovery Progress | 60 |
| Authorizing Devices | 60 |
| Decommissioning a Monitored Device | 61 |
| Managing Devices | 63 |
| Sort a List | 63 |
| Search for a Device in a List | 64 |
| Filter a List | 64 |
| Discover Devices | 64 |
| Working with Rules and Alerts | 65 |

| | |
|--|-----------|
| Enabling and Disabling Rules | 67 |
| Configuring Rule Thresholds | 67 |
| Turning Notification Email On or Off | 68 |
| Working with Reports | 71 |
| Generating a Report | 72 |
| Scheduling a Report | 72 |
| Managing Reports | 72 |
| Managing Report Schedules | 73 |
| Working with Users | 77 |
| Creating a User | 78 |
| Searching for a User | 80 |
| Managing Users | 81 |
| Sort the Manage Users List | 81 |
| Search for a User | 82 |
| Filter the Manage Users List | 82 |
| Create a New User | 82 |
| View the Configuration Details for an Existing User | 82 |
| Edit the Configuration of an Existing User | 82 |
| Copy the Configuration of an Existing User for Creating a New User | 85 |
| Change the Password of an Existing User | 87 |
| Expire the Password of an Existing User | 87 |
| Remove a User | 87 |
| Configuring Password Settings | 88 |
| Configuring User Session Timeout | 89 |
| Support | 91 |
| Generating a Support Bundle | 92 |
| Requesting Support | 92 |
| Managing Support Bundles | 94 |
| Sort the Support Bundles List | 95 |
| Search for a Generated Support Bundle | 95 |
| Filter the Support Bundles List | 95 |
| Generate a New Support Bundle | 95 |
| Download a Generated Support Bundle | 95 |

8 | PulseNET
Administrator's Guide

Delete a Generated Support Bundle..... 96

Index..... **97**

Introduction

This guide is intended to assist Administrators with configuring and managing MDS PulseNET. 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.

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.

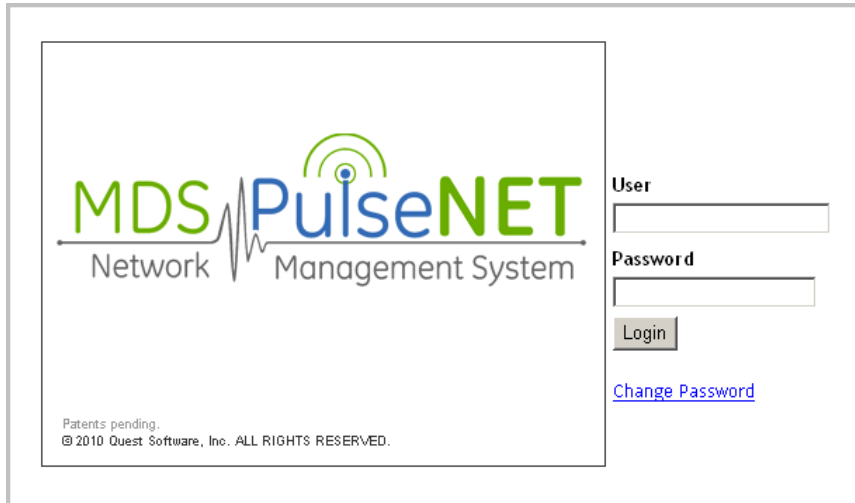
Note For a list of browsers supported by PulseNET, see the *PulseNET Release Notes*.

- 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 Email Settings**—for configuring email settings. For information, see Chapter 2, “[Configuring E-mail Settings](#)”.
- **Licensing**—for requesting, installing, and managing licenses. For information, see Chapter 3, “[Working with Licenses](#)”.
- **Collection Configuration**—for configuring SNMP 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 E-mail Settings

This chapter describes [Email Configuration](#).

Email Configuration

This section describes how to configure email settings in PulseNET. You configure email settings using the Configure Email Settings dialog box (**Administration > 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) Note This is required. | This is the host name for sending emails. | Provide the host name or IP. |
| Email Sender Address Note 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 Note 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:

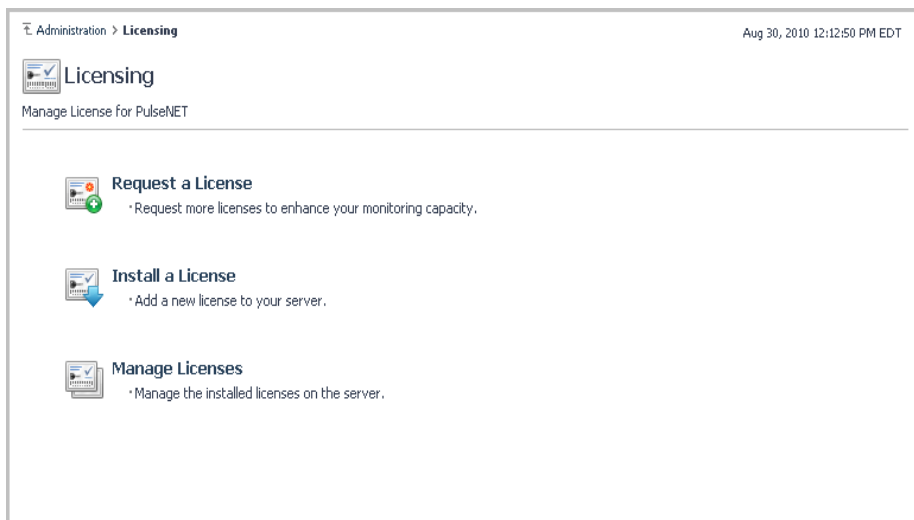
- Click the **Clear** icon for the property.

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

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

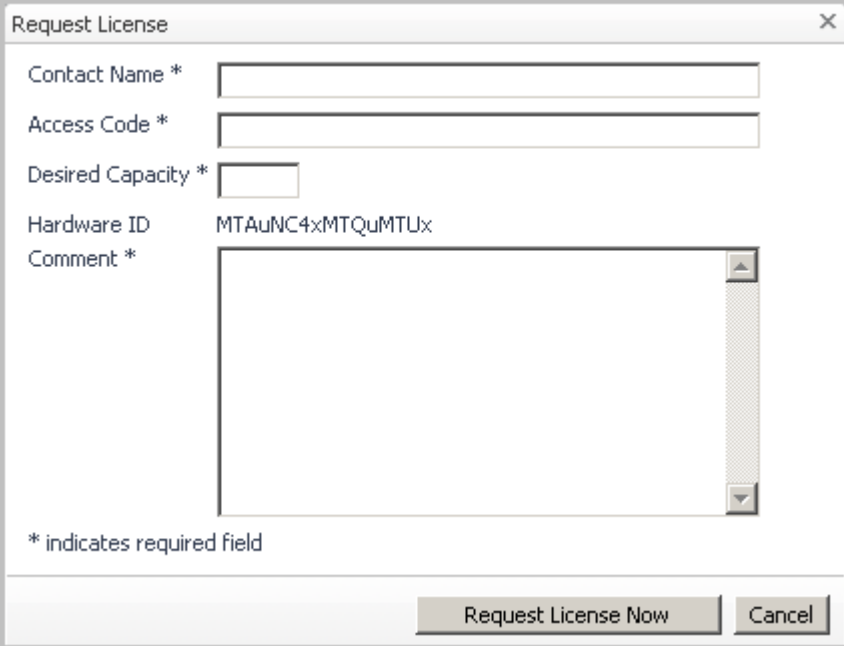
As a PulseNET administrator, you can request PulseNET licenses.

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 E-mail Settings”.

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

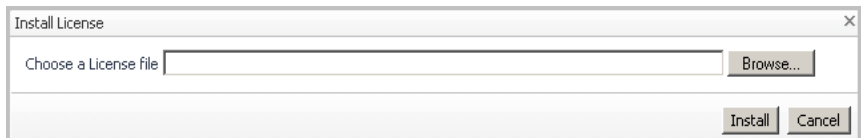
Installing a License

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 26.

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 23.

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 23.

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:

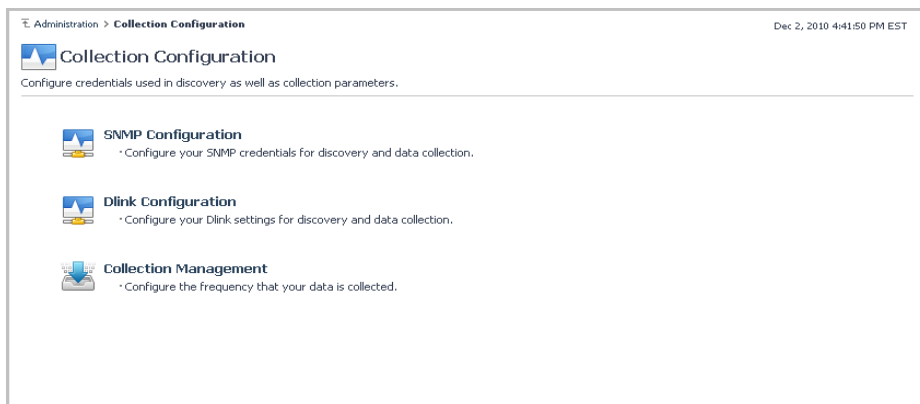
- 1 the ten available on the July 1st license
- 2 the twenty available on the August 1st licence
- 3 the ten available on the May 21st license

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 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." Below this, there are three main configuration sections, each with a blue icon and a title:

- 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**).

The screenshot shows the SNMP Configuration view with the following data:

| SNMP v1 and v2c Community Strings | |
|-----------------------------------|-----------------|
| Values | Managed Devices |
| public | 31 |

| SNMP v3 Credentials | | | | | | |
|--------------------------|-----------|----------------|------------|----------|------------|-----------------|
| | User Name | Authentication | | Privacy | | Managed Devices |
| | | Protocol | Passphrase | Protocol | Passphrase | |
| <input type="checkbox"/> | test | SHA | **** | AES192 | **** | 29 |

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 34.
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.

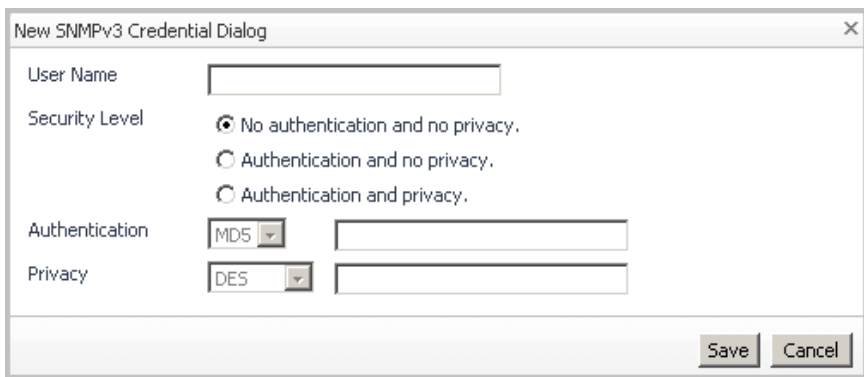
Add SNMP v3 Credentials

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 34.

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 32.

- 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 |

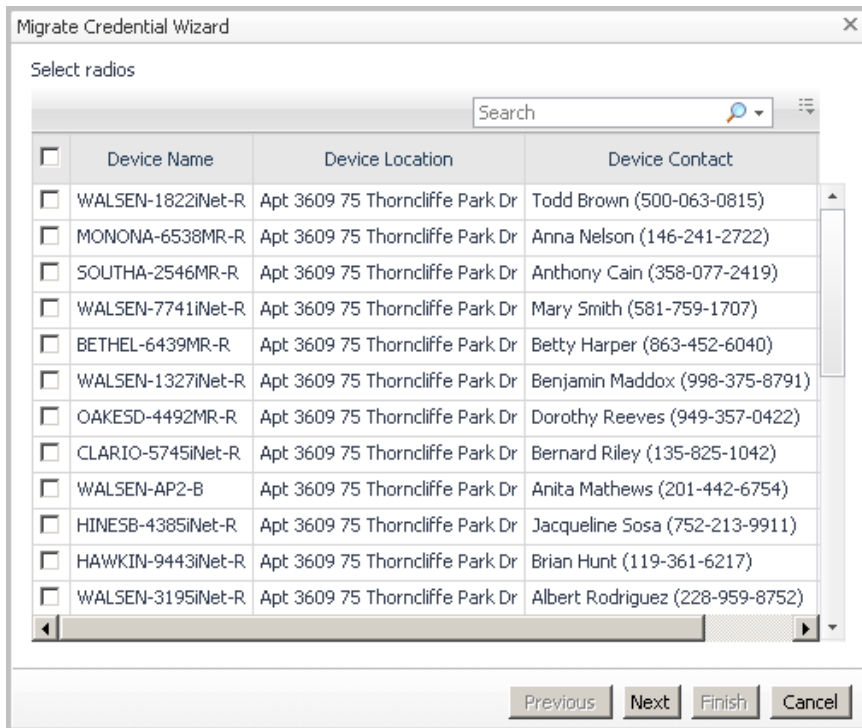
- 2 Make changes to one or more of the settings.
- 3 Click **Save**.

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.

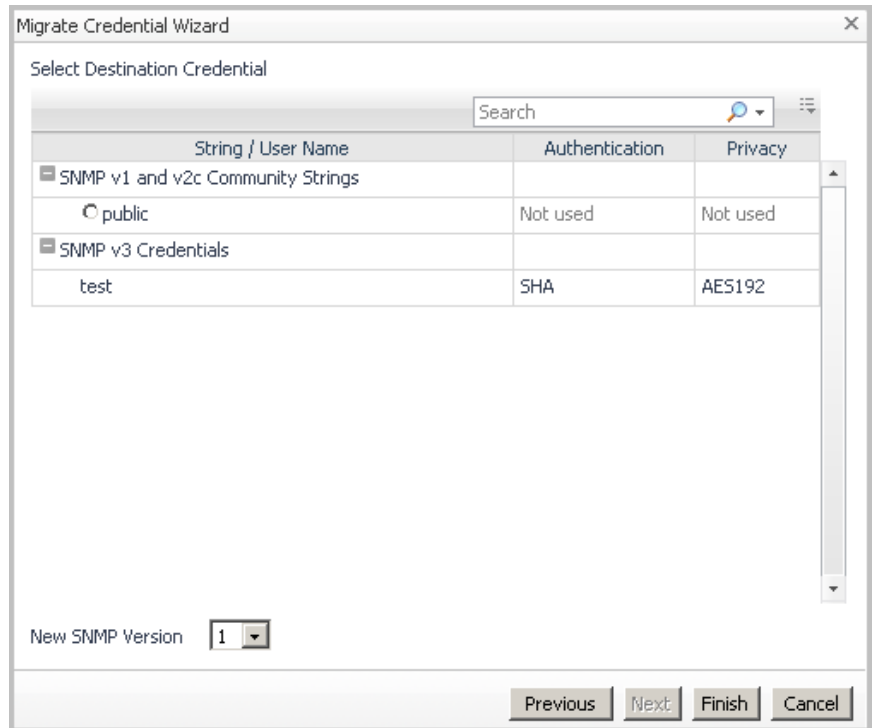


- 2 In the column at the left, click the check boxes for the devices you want to migrate.

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

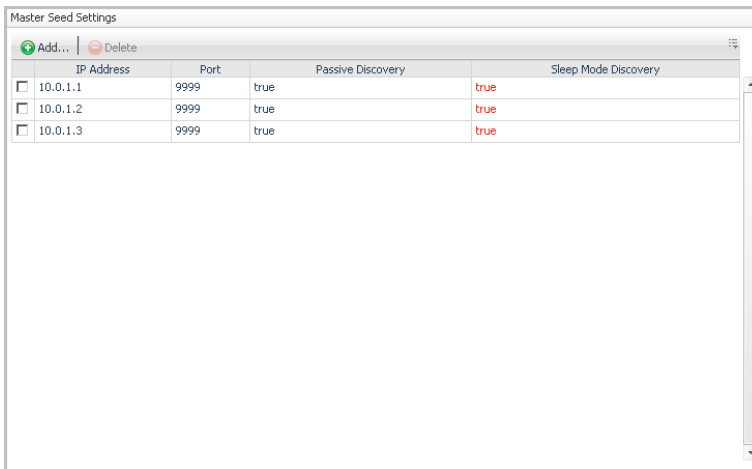
Use the Search tool at the top right of the appropriate table to search for a specific SNMP Community String or set of credentials. For instructions on how to use the Search tool, see “Working with Tables” in the *PulseNET Quick Start Guide*.

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 39.
- 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. Note 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 PulseNET Collection Scheduler interface. At the top, the breadcrumb navigation reads "Administration > Collection Configuration > Collection Management" and the date/time is "Feb 11, 2011 12:59:28 AM EST".

The first section is titled "Collection Scheduler for MDS Devices". It features a search bar and a table with the following data:

| Type | Role | Schedule Configuration | Interval | |
|----------------------------|-------------|------------------------|------------------|-----------------|
| | | | Performance | Availability |
| Mercury 3650 Access Points | AccessPoint | | Every 5 minutes | Every 1 minutes |
| Mercury 900 Access Points | AccessPoint | | Every 5 minutes | Every 1 minutes |
| Mercury 1800 Access Points | AccessPoint | | Every 5 minutes | Every 1 minutes |
| iNET 900 Access Points | AccessPoint | | Every 5 minutes | Every 1 minutes |
| iNET-II 900 Access Points | AccessPoint | | Every 5 minutes | Every 1 minutes |
| Mercury 3650 Remotes | Remote | | Every 5 minutes | Every 1 minutes |
| Mercury 900 Remotes | Remote | | Every 5 minutes | Every 1 minutes |
| Mercury 1800 Remotes | Remote | | Every 5 minutes | Every 1 minutes |
| iNET 900 Remotes | Remote | | Every 5 minutes | Every 1 minutes |
| iNET-II 900 Remotes | Remote | | Every 5 minutes | Every 1 minutes |
| Intrepids | Backhaul | | Every 10 minutes | Every 8 minutes |

The second section is titled "Collection Scheduler for DLink Devices". It features a search bar and a table with the following data:

| Type | Schedule Configuration | Interval | | Schedule Configuration Enable |
|---------------|------------------------|------------------|--------------|-------------------------------|
| | | Performance | Availability | |
| DLink Devices | | Every 15 minutes | | |

The Collection Scheduler lists the devices that PulseNET can monitor.

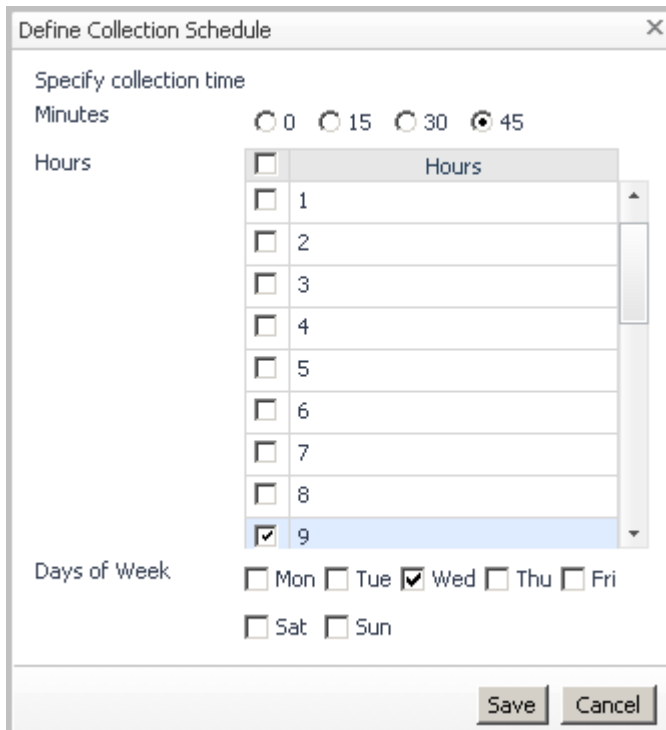
You can configure the sample frequency of data collection for each.

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 48.

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" contains the following elements:

- Specify collection time**
- Minutes:** Radio buttons for 0, 15, 30, and 45. The 45-minute option is selected.
- Hours:** A list box with a scroll bar, containing hours 1 through 9. Each hour has a checkbox to its left. The checkbox for 9 is checked.
- Days of Week:** Checkboxes for Mon, Tue, Wed, Thu, Fri, Sat, and Sun. The checkbox for Wed is checked.
- Buttons:** "Save" and "Cancel" buttons at the bottom right.

- 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 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 65.

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.

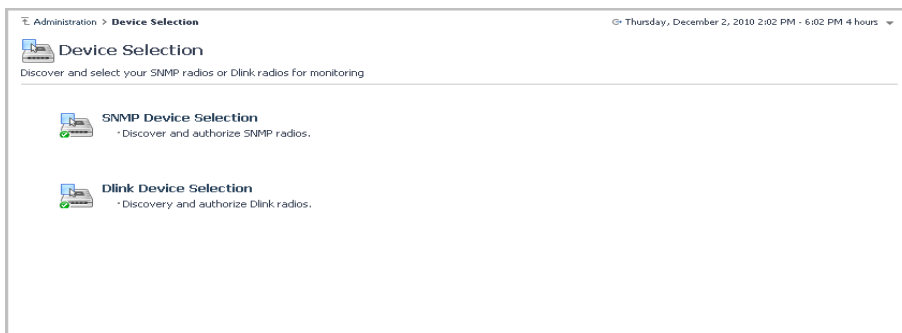
If you change the collection frequency to 1 hour, an SNR change warning alert, if required, will be raised 3 hours after the first time the 2 dB threshold is noticed.

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](#)
- [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"/> 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 30.

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 34.

- 4 Click **Next**.

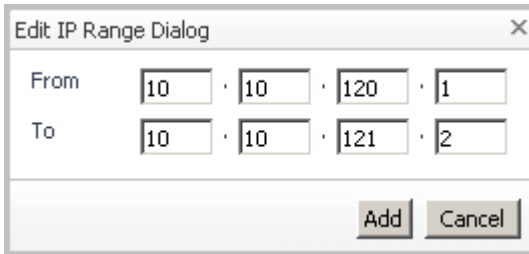
Note At any time you can click **Previous** to go back to the previous step.

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

The screenshot shows the 'Discovery Wizard' window 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 window, 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.



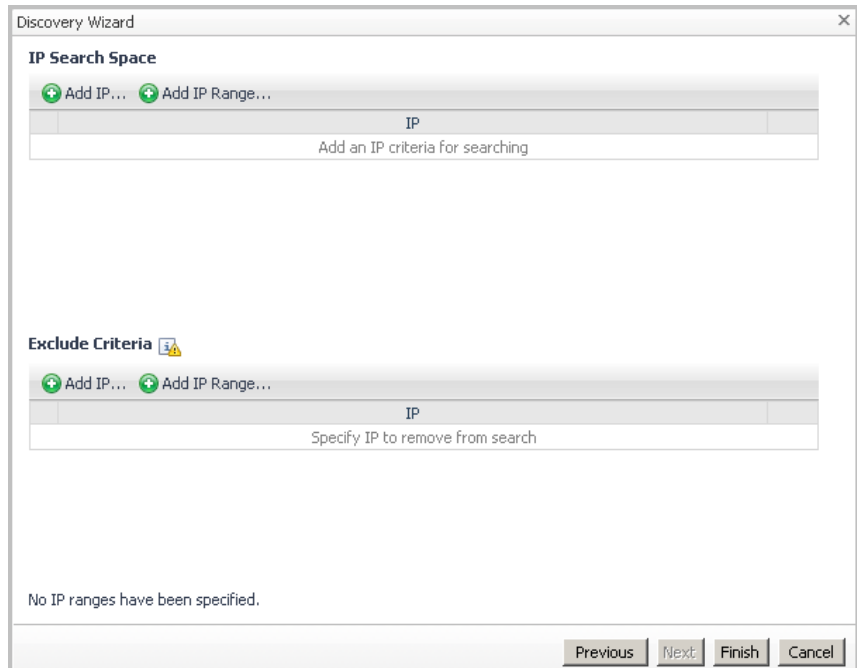
The screenshot shows a dialog box titled "Edit IP Range Dialog" with a close button (X) in the top right corner. The dialog contains two rows of input fields. The first row is labeled "From" and contains four input boxes with the values "10", "10", "120", and "1". The second row is labeled "To" and contains 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 34.

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 60. 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.

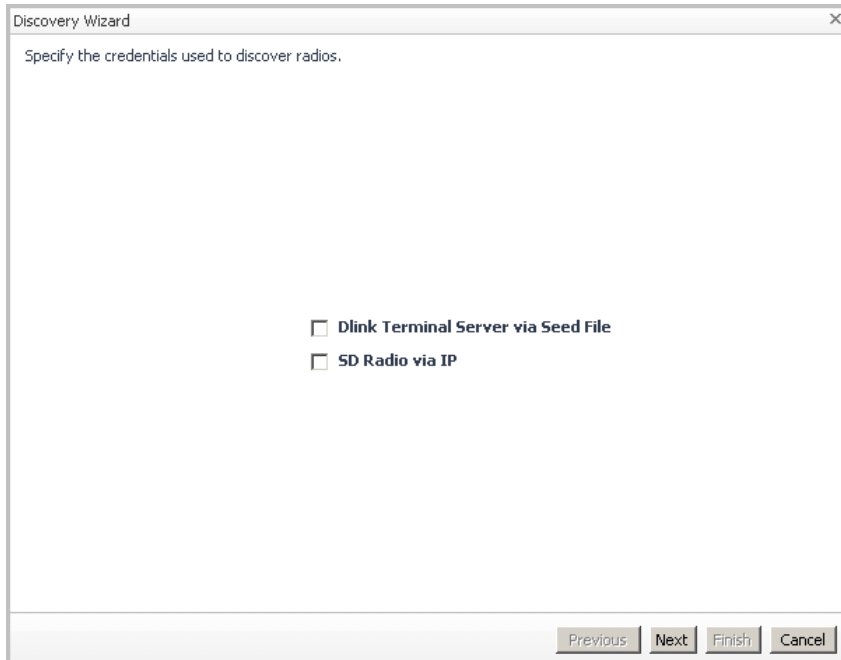
Perform discovery to find the devices you want PulseNET to monitor.

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 38.

- 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 a window titled "Discovery Wizard" with a close button (X) in the top right corner. The window is divided into two main sections: "IP Search Space" and "Exclude Criteria".

IP Search Space

At the top of this section are two buttons: "Add IP..." and "Add IP Range...". Below these is a table with a header row containing the text "IP". The table body is currently empty, with the text "Add an IP criteria for searching" centered below the header.

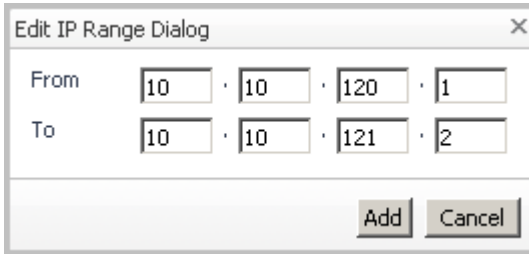
Exclude Criteria

At the top of this section are two buttons: "Add IP..." and "Add IP Range...". Below these is a table with a header row containing the text "IP". The table body is currently empty, with the text "Specify IP to remove from search" centered below the header.

At the bottom of the window, there is a status bar that reads "No IP ranges have been specified." and a set 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.



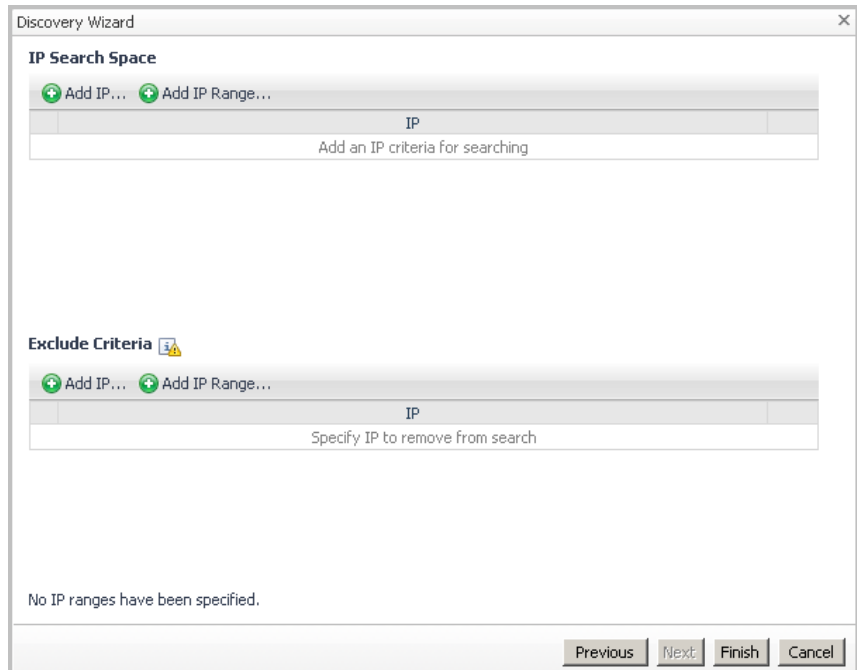
The screenshot shows a dialog box titled "Edit IP Range Dialog". It contains two rows of input fields. The "From" row has four fields containing the values "10", "10", "120", and "1". The "To" row has four fields containing the values "10", "10", "121", and "2". At the bottom right of the dialog are 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 41.

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 60.

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 26.

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:

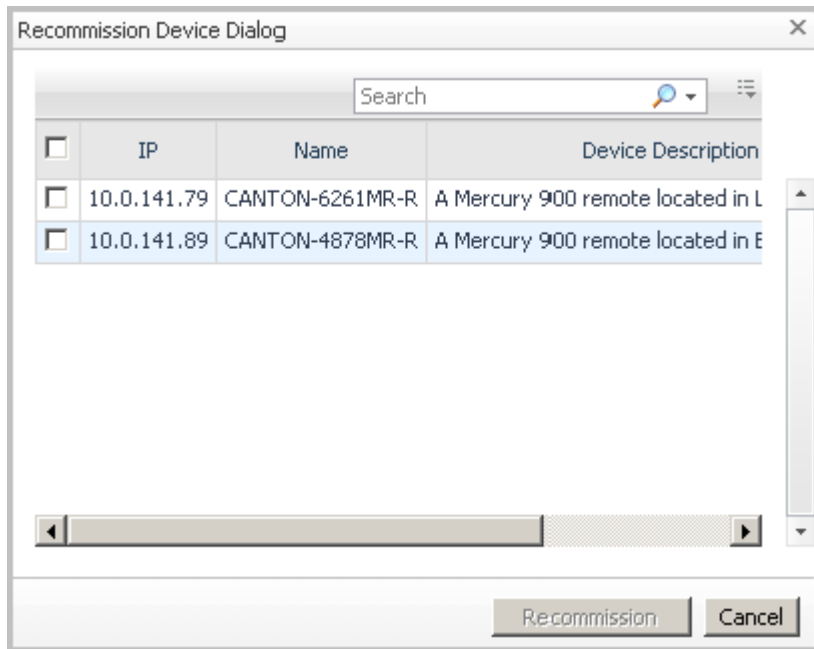
- 1 Perform discovery. For instructions on how to perform discovery, see “[Discovering SNMP Devices](#)” on page 50.

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 'Administration > Device Selection > Device Selection' interface. It features three main sections: 'Discovered Devices', 'Ineligible Devices', and 'Monitored Devices'. The 'Discovered Devices' section is currently empty, showing a search bar and a message: 'No devices have been discovered. Run "Discover Devices" to find devices.' The 'Ineligible Devices' section is also empty, with a message: 'There Is No Data To Display'. The 'Monitored Devices' section is expanded, displaying a table of devices with columns for Device Name, Device Description, Device Contact, IP, Mac, Model Number, Device Location, Serial Number, and Decommission Device. The table contains 12 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 50 and “[Discovering Dlink Devices](#)” on page 55.

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](#)

Administration > Rules and Alerts Dec 8, 2010 12:42:01 PM EST

| Name | Type | Description | Enabled | Email | | | | Threshold |
|-------------------------|----------------------------|---|---------|--------|---------|----------|-------|-----------|
| | | | | Normal | Warning | Critical | Fatal | |
| Bad Access Point health | INET 900 Access Points | Bad Access Point health detected. | — | 0 | 0 | 0 | 0 | |
| Bad Access Point health | INET-II 900 Access Points | Bad Access Point health detected. | — | 0 | 0 | 0 | 0 | |
| Bad Access Point health | Mercury 1800 Access Points | Bad Access Point health detected. | — | 0 | 0 | 0 | 0 | |
| Bad Access Point health | Mercury 3650 Access Points | Bad Access Point health detected. | — | 0 | 0 | 0 | 0 | |
| Bad Access Point health | Mercury 900 Access Points | Bad Access Point health detected. | — | 0 | 0 | 0 | 0 | |
| Bad Access Point health | Dlink Access Points | Bad Access Point health detected. | — | 0 | 0 | 0 | 0 | |
| Device Unavailable | INET 900 Access Points | The INET-I Access Point is not available. | ● | 0 | | | 0 | |
| Device Unavailable | INET 900 Remotes | The INET-I Remote is not available. | ● | 0 | | | 0 | |
| Device Unavailable | INET-II 900 Access Points | The INET-II Access Point is not available. | ● | 0 | | | 0 | |
| Device Unavailable | INET-II 900 Remotes | The INET-II Remote is not available. | ● | 0 | | | 0 | |
| Device Unavailable | Intrepids | The Intrepid Device is not available. | ● | 0 | | | 0 | |
| Device Unavailable | Mercury 1800 Access Points | The Mercury 1800 Access Point is not available. | ● | 0 | | | 0 | |
| Device Unavailable | Mercury 1800 Remotes | The Mercury 1800 Remote is not available. | ● | 0 | | | 0 | |
| Device Unavailable | Mercury 3650 Access Points | The Mercury 3650 Access Point is not available. | ● | 0 | | | 0 | |
| Device Unavailable | Mercury 3650 Remotes | The Mercury 3650 Remote is not available. | ● | 0 | | | 0 | |
| Device Unavailable | Mercury 900 Access Points | The Mercury 900 Access Point is not available. | ● | 0 | | | 0 | |
| Device Unavailable | Mercury 900 Remotes | The Mercury 900 Remote is not available. | ● | 0 | | | 0 | |
| Device Unavailable | Dlink Access Points | The Dlink Device Access Point is not available. | ● | 0 | | | 0 | |
| Device Unavailable | Dlink Remotes | The Dlink Device Remote is not available. | ● | 0 | | | 0 | |
| Poor Response Time | INET 900 Access Points | Poor ICMP round trip time detected. | — | 0 | 0 | 0 | 0 | |
| Poor Response Time | INET 900 Remotes | Poor ICMP round trip time detected. | — | 0 | 0 | 0 | 0 | |
| Poor Response Time | INET-II 900 Access Points | Poor ICMP round trip time detected. | — | 0 | 0 | 0 | 0 | |
| Poor Response Time | INET-II 900 Remotes | Poor ICMP round trip time detected. | — | 0 | 0 | 0 | 0 | |

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

| Rule | Description | Severity |
|-------------------------|--|--------------------------|
| 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 |
| 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

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**.

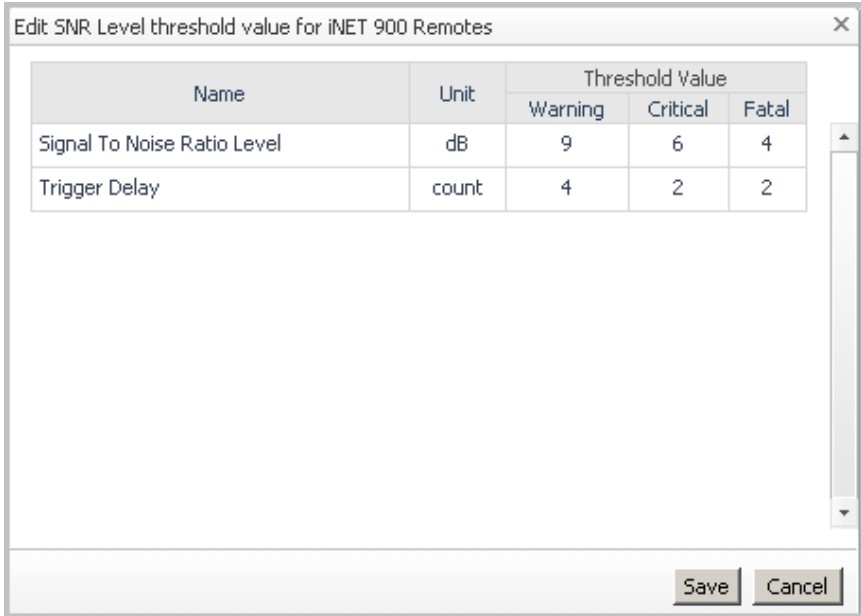
Configuring Rule Thresholds

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

To configure the threshold(s) for a rule:

- 1 Click the Threshold icon for the rule.

An Edit dialog box appears.



- 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 48.

- 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.

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.

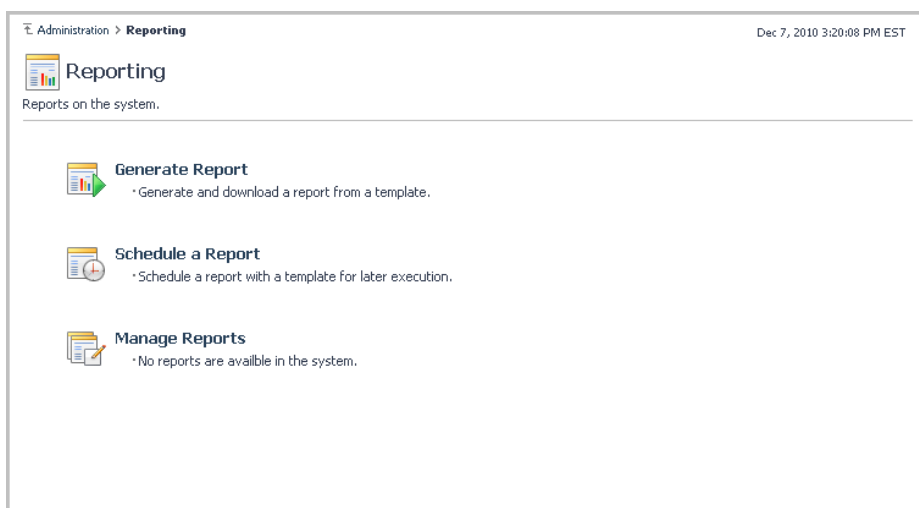
Note If you have not configured PulseNET email settings, the confirmation dialog box will ask you if you want to do that now. For information about how to configure email settings, see Chapter 2, “Configuring E-mail Settings”.

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

Working with Reports

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

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



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... |

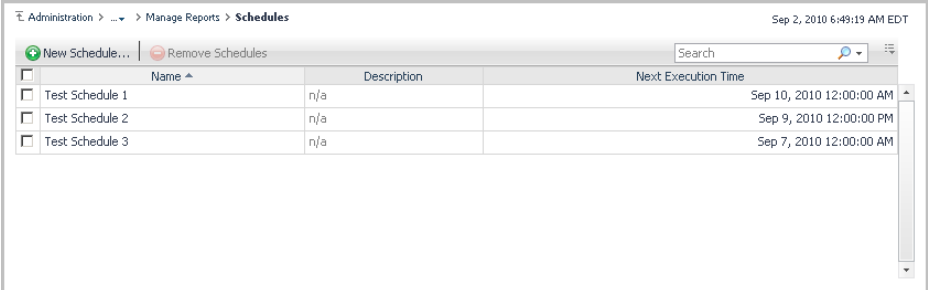
You can use the Manage Reports view to perform a number of report-related tasks.

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](#)

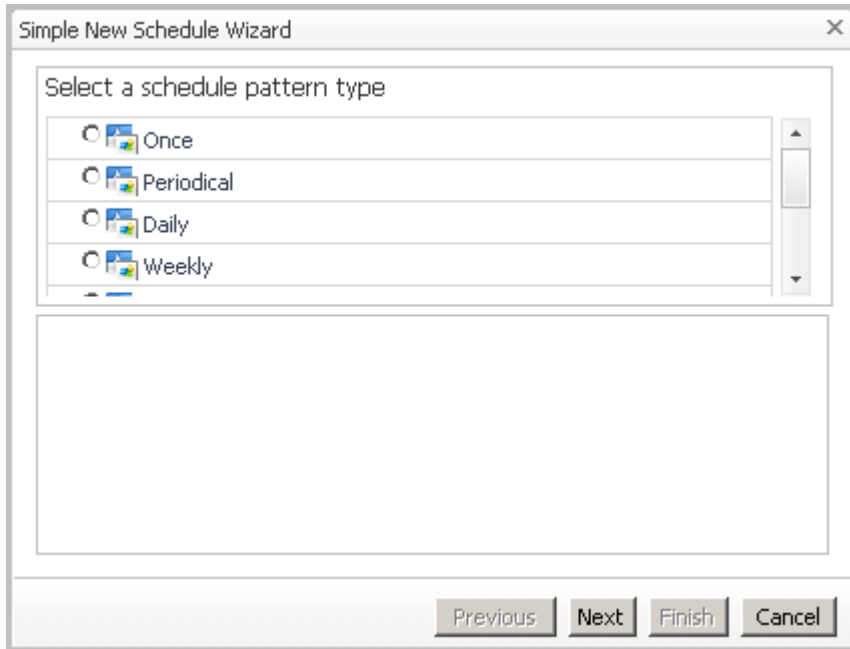
Note The schedules that are provided with PulseNET cannot be deleted.

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**.

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 82.

- 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.

New User

Select a group to assign to **Operator 1**

Search

Group Names ▲

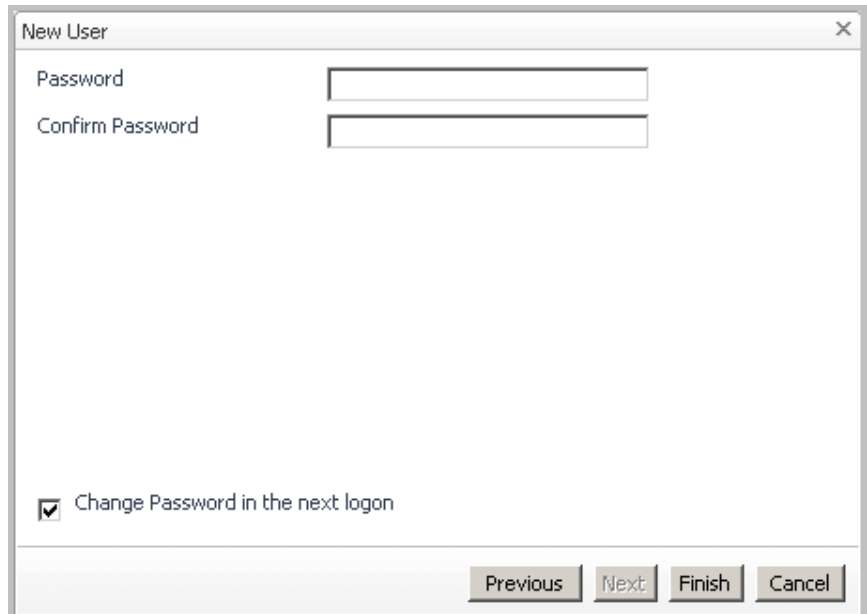
| | |
|-----------------------|-------------------------|
| <input type="radio"/> | PulseNET Administrators |
| <input type="radio"/> | PulseNET Operators |

Previous Next Finish Cancel

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 88.



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, 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 82.

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**.

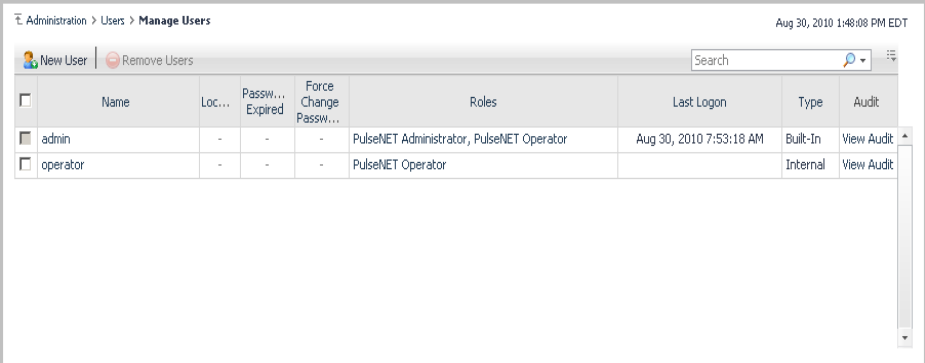
If only one user name matches what you entered, the details for that user appear. If more than one user name matches what you entered, a dialog box, listing the user names that match, appears.

- 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 78.

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

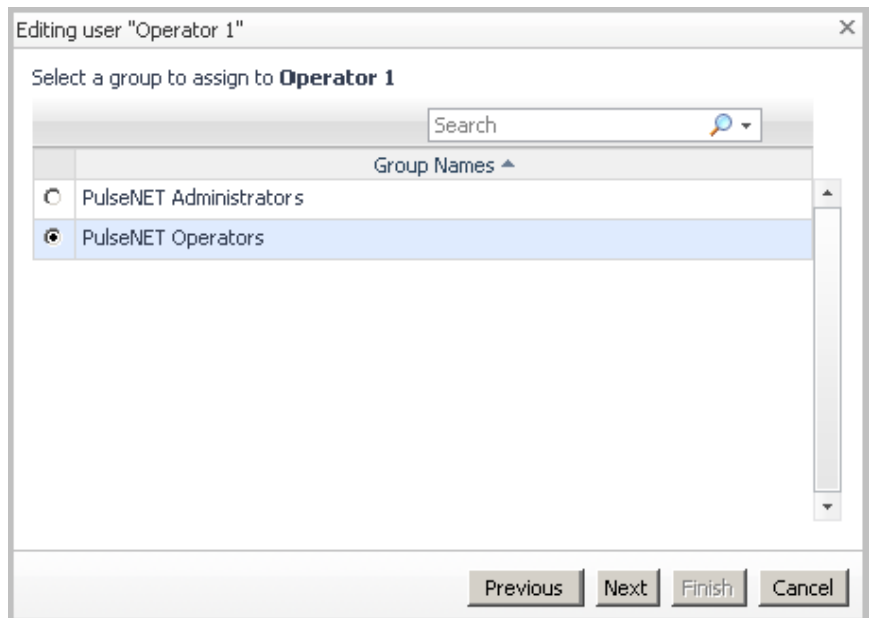
To edit the configuration of an existing user:

- 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.

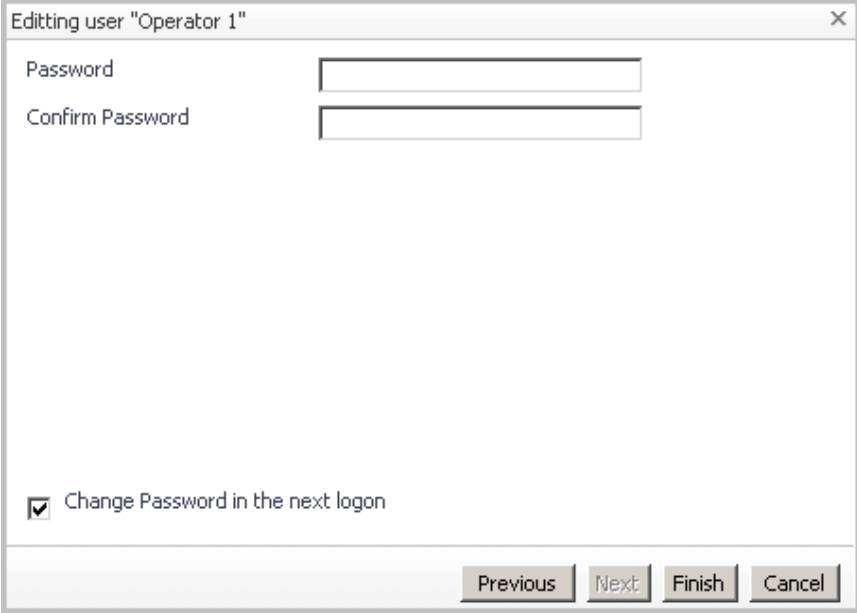


Note A user can be an administrator or an operator, but not both. Administrators have access to all operator functionality.

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 88.



Editing user "Operator 1" ✕

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**).

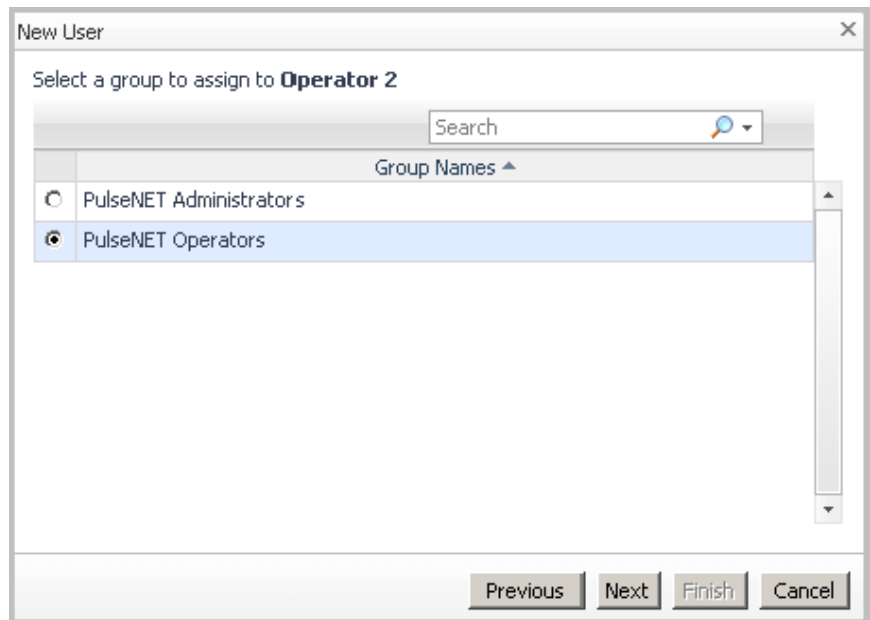
Copy the Configuration of an Existing User for Creating a New User

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.

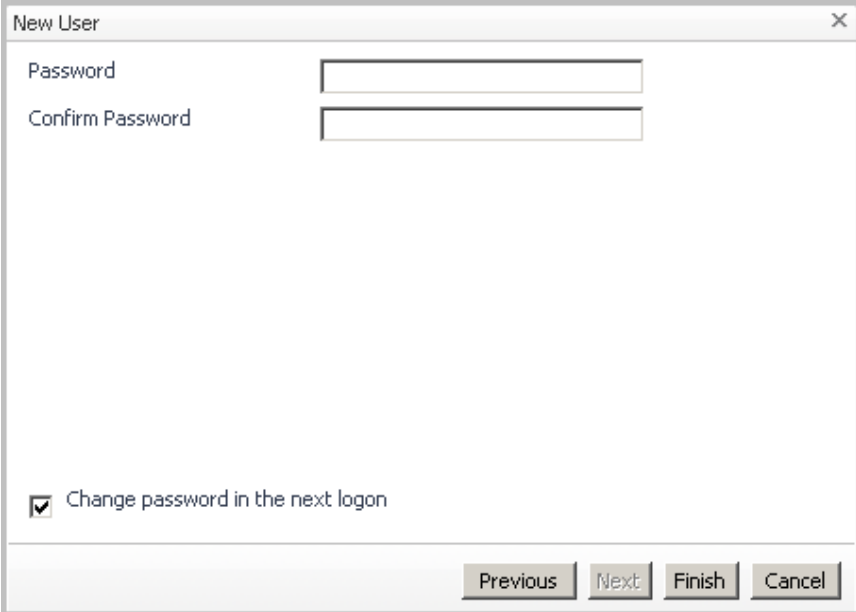


Note A user can be an administrator or an operator, but not both. Administrators have access to all operator functionality.

- 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 88.



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"> • 1: password must be seven or more characters in length and contain at least one alpha and one numeric character • 2: password must be seven or more characters in length and contain at least one alpha, one numeric, and one upper case character • 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 | 1 |

| Password Setting | Default Setting |
|--|-----------------|
| Admin password complexity level <ul style="list-style-type: none">• 1: password must be seven or more characters in length and contain at least one alpha and one numeric character• 2: password must be seven or more characters in length and contain at least one alpha, one numeric, and one upper case character• 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 | 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**.

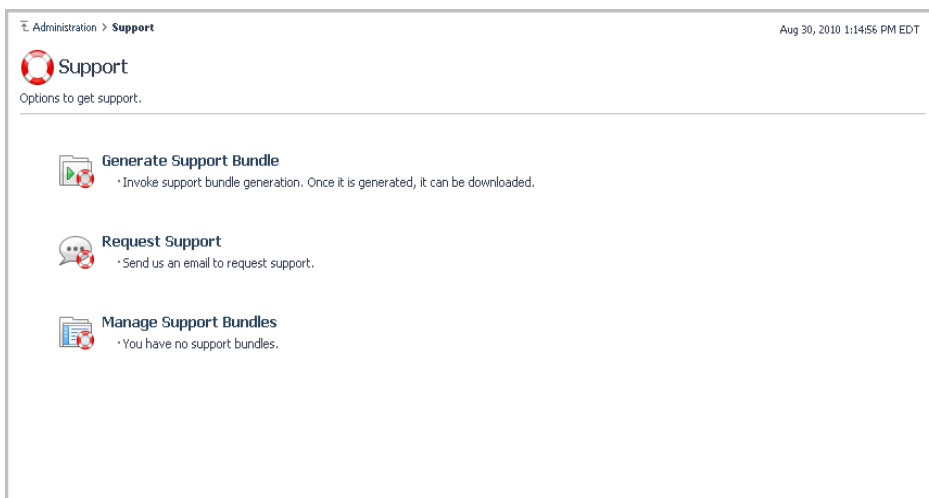
The Change User Session Timeout dialog box appears.

- 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 94.

Requesting Support

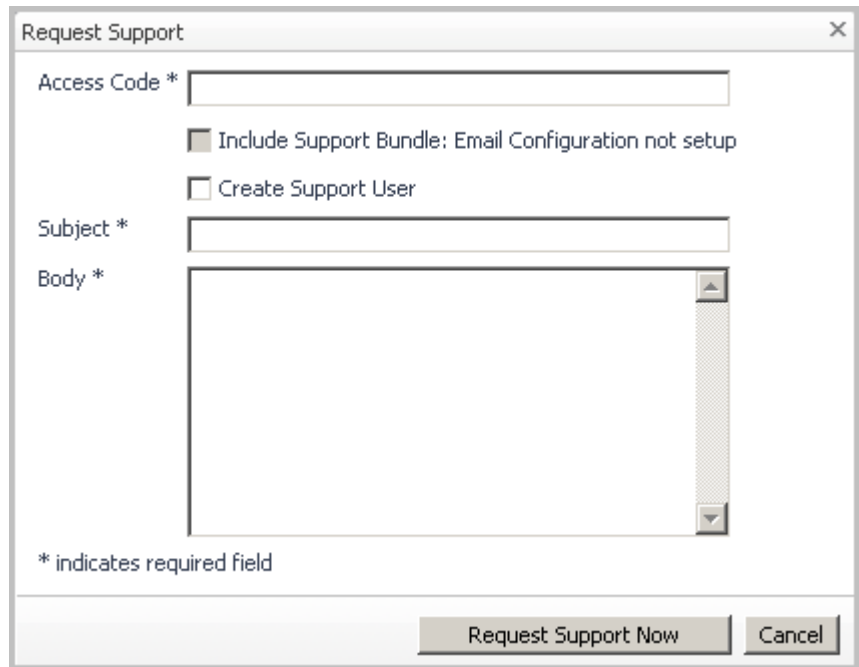
You can request support for PulseNET through email.

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 E-mail 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.



Request Support

Access Code *

Include Support Bundle: Email Configuration not setup

Create Support User

Subject *

Body *

* indicates required field

Request Support Now Cancel

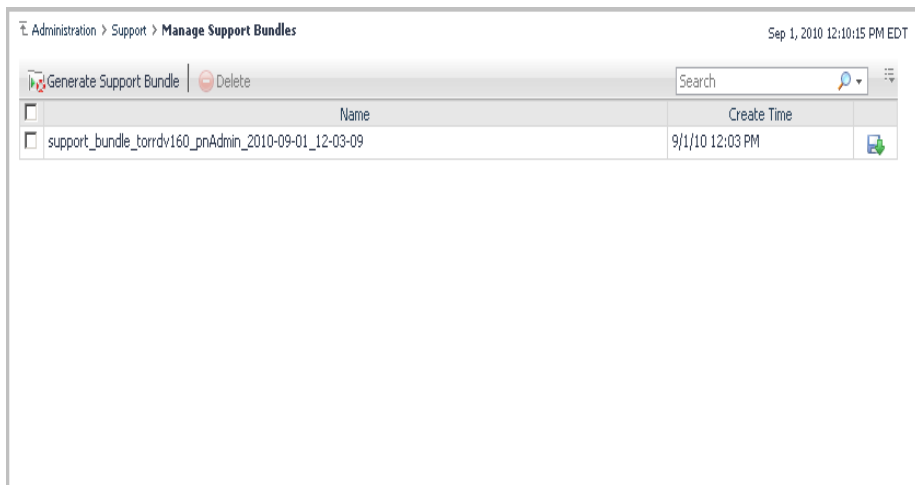
- 2 Type your customer number in the field provided.
- 3 Leave the **Include Support Bundle** check box selected if you want to include a support bundle.
A support bundle will be generated and included in the support request.
- 4 Leave the **Create Support User** check box cleared, unless the Support 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 92.

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**.

Index

A

Administration Home dashboard 14

Administrator

role 9

alerts

working with 65

authorizing devices 49, 60

availability

data collection 48

C

Collection Configuration view 29

Collection Scheduler view 45

community string

adding 31

deleting 31

configuration

change

discovery 54, 60

data collection sample frequency 29, 45, 46

Dlink 29

email settings 17, 19

rule thresholds 67

SNMP 29, 30, 38

Configure Password Settings view 88

configuring

user password settings 77, 88

copying

user configuration 85

creating

report schedules 74

users 77, 78, 82

credentials

adding 32

deleting 33

editing 33

D

dashboards

Administration Home 14

data collection

availability 48

specifying an interval 47

configuring sample frequency 29, 45, 46

frequency 48

performance 48

specifying an interval 47

decommissioning

devices 61

decommissioning devices 49

deleting

licenses 25

report schedules 75

support bundles 96

Device Selection view 49, 63

devices

authorizing 49, 60

configuration

change 54, 60

- decommissioning 49, 61
 - summary statistics* 61
- discovery 49, 64
- Dlink discovery 55
- filtering a list 64
- ineligible 54
- Ineligible Devices List 55
- managing 49, 63
- recommission
 - discovery* 54, 60
- recommissioning 61
- searching for 64
- SNMP discovery 50
- sorting a list 63

discovery

- configuration
 - change* 54, 60
- devices 49, 64
- Dlink devices 55
- progress 54, 60
- recommission
 - devices* 54, 60
- SNMP devices 50

Dlink

- adding a master seed 39
- configuring 29
 - advanced settings* 41
- deleting a master seed 40
- editing master seed settings 40

Dlink Configuration view 38**Dlink devices**

- schedule configuration
 - disabling* 47

downloading

- support bundles 95

E**editing**

- user configuration 82

email settings

- configuring 17, 19
- properties 18

exporting

- Ineligible Devices List 55

F**filtering**

- device lists 64
- Manage Users List 82
- master seed tables 45
- SNMP tables 38
- Support Bundles List 95

G**generating**

- reports 71, 72
- support bundles 91, 92, 95

I**ineligible devices** 54**Ineligible Devices List**

- exporting 55

installing

- licenses 21, 23, 25

L**licenses**

- deleting 25
- installing 21, 23, 25
- managing 21, 24
- migrating devices 26
- order, when authorizing devices 26
- requesting 21
- working with 21

Licensing view 21**logging in to PulseNET** 13

M

- Manage Licenses view** 24
- Manage Reports view** 72
- Manage Support Bundles view** 94
- Manage Users List**
 - filtering 82
 - searching 82
 - sorting 81
- Manage Users view** 81
- managing**
 - devices 49, 63
 - licenses 21
 - report schedules 73
 - reports 71, 72
 - support bundles 91, 94
 - users 77, 81
- managing licenses** 24
- master seed**
 - adding 39
 - deleting 40
 - editing settings 40
- master seed tables**
 - filtering 45
 - searching 45
 - sorting 44
- migrating devices**
 - licenses 26
 - SNMP credentials 36

O

- Operator**
 - role 9

P

- password**
 - changing for a user 87
 - configuring user settings 77, 88
 - expiring for a user 87
- performance**

- data collection 48

properties

- email settings 18

R**recommission**

- devices
 - discovery* 54, 60

recommissioning

- devices 61

removing

- users 87

report schedules

- creating 74
- deleting 75
- managing 73

Reporting view 71**reports**

- generating 71, 72
- managing 71, 72
- scheduling 71, 72

requesting

- licenses 21
- support 91, 92

roles

- Administrator 9
- Operator 9

rule email notification

- turning on or off 68

rule thresholds

- configuring 67

rules

- descriptions 65
- disabling 67
- email notification 68
- enabling 67
- thresholds 67
- working with 65

Rules view 65

S**schedule configuration**

- Dlink devices
 - disabling* 47

scheduling

- reports 71, 72

searching

- device lists 64
- Manage Users List 82
- master seed tables 45
- SNMP tables 38
- Support Bundles List 95
- users 77, 80

server

- starting 10
- stopping 12

session

- user
 - timeout* 77, 89

SNMP

- adding a community string 31
- adding credentials 32
- configuring 29, 30, 38
- configuring advanced settings 34
- deleting a community string 31
- deleting credentials 33
- editing credentials 33
- migrating devices 36

SNMP Configuration view 30**SNMP tables**

- filtering 38
- searching 38
- sorting 37

sorting

- device lists 63
- Manage Users List 81
- master seed tables 44
- SNMP tables 37
- Support Bundles List 95

starting the server 10**stopping the server** 12**support**

- requesting 91, 92

support bundles

- deleting 96
- downloading 95
- generating 91, 92, 95
- managing 91, 94
- searching for 95

Support Bundles List

- filtering 95
- sorting 95

Support view 91**T****timeout**

- user session 77, 89

trigger delay value 48**U****users**

- changing a password 87
- configuring password settings 77, 88
- configuration details 82
- copying a configuration 85
- creating 77, 78, 82
- editing a configuration 82
- expiring a password 87
- Manage Users List 81, 82
- managing 77, 81
- removing 87
- searching for 77, 80

Users view 77**V****views**

- Collection Configuration 29
- Collection Scheduler 45
- Configure Password Settings 88

- Device Selection 49, 63
- Dlink Configuration 38
- Licensing 21
- Manage Licenses 24
- Manage Reports 72
- Manage Support Bundles 94
- Manage Users 81
- Reporting 71
- Rules 65
- SNMP Configuration 30
- Support 91
- Users 77

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

FAX: 585 242-8369

Web: www.gemds.com

