User Guide

Pulse Network Management System

iDirect Pulse ® Release 2.3.x

Rev. B

September 14, 2017

VT iDirect® is a global leader in IP-based satellite communications providing technology and solutions that enable our partners worldwide to optimize their networks, differentiate their services and profitably expand their businesses. Our product portfolio, branded under the name **iDirect®**, sets standards in performance and efficiency to deliver voice, video and data connectivity anywhere in the world. **VT iDirect®** is the world’s largest TDMA enterprise VSAT manufacturer and is the leader in key industries including mobility, military/government and cellular backhaul.

Company Web site: www.idirect.net ~ Main Phone: 703.648.8000
TAC Contact InforPulse Network Management Systemmation: Phone: 703.648.8151 ~ Email: tac@idirect.net ~ Web site: tac.idirect.net

Pulse Network Management System

iDirect Government™, created in 2007, is a wholly owned subsidiary of iDirect and was formed to better serve the U.S. government and defense communities.

Company Web site: www.idirectgov.com ~ Main Phone: 703.648.8118
TAC Contact Information: Phone: 703.648.8111 ~ Email: tac@idirectgov.com ~ Web site: tac.idirectgov.com

Document Name: UG_Pulse_NMS_User_Guide_RevB_091417.pdf

Document Part Number: T0000856

Revision History

The following table shows all revisions for this document. To determine if this is the latest revision, check the Technical Assistance Center (TAC) Web site. Refer to *Getting Help* on page xx for TAC access information.

Revision	**Date**	**Updates**
A	05/05/2017	Initial document release for Pulse Release 2.3 *Note*: Some fields that appear in the Pulse production environment, may not appear in an associated screenshot or text in this release of the Pulse User Guide. These fields are not necessary for system operation.
B	09/14/2017	Updated for Pulse Release 2.3.1

Contents

Figures

Tables

About

Purpose

The *iDirect Pulse® NMS User Guide* provides detailed information and instructions necessary to understand and use the Pulse NMS Web User Interface for working with iDirect Networks.

Audience

This document is intended for use by network engineers and operators, as well as other personnel responsible for configuring, monitoring, and operating iDirect Velocity™ networks.

Getting Help

The iDirect Technical Assistance Center (TAC) and the iDirect Government Technical Assistance Center (TAC) are available to provide assistance 24 hours a day, 365 days a year. Software user guides, installation procedures, FAQs, and other documents that support iDirect and iDirect Government products are available on the respective TAC Web site:

- Contact iDirect
  - TAC Web site at http://tac.idirect.net
  - Telephone: 703.648.8151
  - E-mail: tac@idirect.net
- Contact iDirect Government
  - TAC Web site at http://tac.idirectgov.com
  - Telephone: 703.648.8111
  - Email: tac@idirectgov.com

At iDirect and iDirect Government we strive to produce documentation that are technically accurate, easy to use, and helpful to our customers. Please assist us in improving this document by providing feedback. Send comments to:

- iDirect: techpubs@idirect.net
- iDirect Government: techpubs@idirectgov.com

For sales or product purchasing information contact iDirect Corporate Sales at the following telephone number or e-mail address:

- Telephone: 703.648.8000
- E-mail: sales@idirect.net

Related Document Set

The following iDirect documents are available at http://tac.idirect.net and contain information relevant to installing and using iDirect satellite network software and equipment.

- *Installation, Support, and Maintenance Guide*
- *Terminal Web User Interface User Guide*
- *iDirect Velocity™ Software Release Notes*
- *iDirect Pulse® Software Release Notes*
- *iDirect Pulse® NMS User Guide*
- *iDirect Velocity™ Network Operations Using Pulse*

1 Getting Started with the Pulse User Interface

This chapter provides a general overview of getting started with the Pulse Network Management System (NMS). Understanding the various visual, functional, and navigational elements of the Pulse user interface, as described in this chapter, will enhance your experience of working with the NMS and performing Pulse activities in an iDirect network.

The following topics are covered in this chapter:

1.1 The User Session

This section briefly provides information on establishing a Pulse NMS session as well as properly terminating a session.

1.1.1 Supported Browsers

You may use the following supported browsers to establish a Pulse user session.

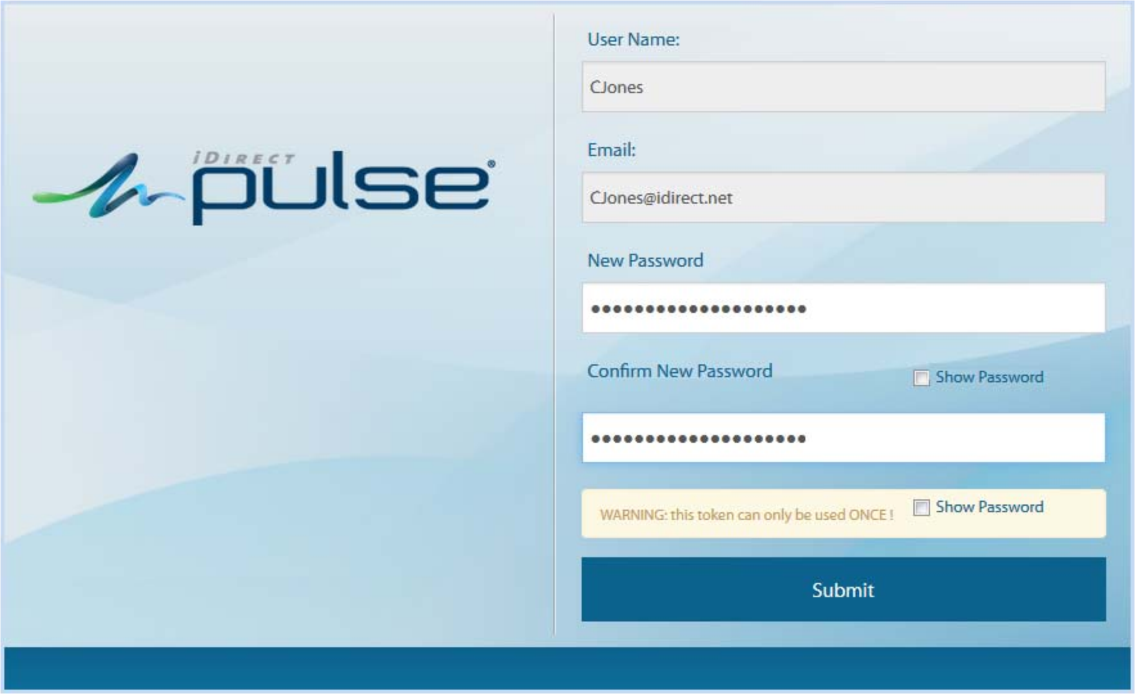
- Mozilla Firefox (two latest versions)
- Google Chrome (two latest versions)

To access the NMS using a Web browser:

1. Launch your Web browser of choice.
2. In the address field, enter the target IP Address of the target NMS — for example `http://nnn.nnn.nnn.nnn`; or the host name — for example nms.example.com.
3. Proceed to the user login dialog. A valid user name and password is required.

1.1.2 Initial User Login

When a new account is created or the password is reset, the NMS sends an account activation or reset token link to the user email account. The e-mail contains a public (http) or secure (https) link, depending on the client request. The link must be used immediately, as the token expires within 24 hours. When the link is followed, the initial user login screen is opened.



User Name: CJones

Email: CJones@idirect.net

New Password: ••••••••••••••••••••

Confirm New Password: ••••••••••••••••••••

WARNING: this token can only be used ONCE !

Figure 1-1. Initial User Login - Change Password Dialog

After entering, confirming and submitting the new password, the account is activated and the normal login dialog is presented.The following guidelines should be observed when creating or changing a user password:

- Common dictionary words are not allowed
- Must contain at least eight characters
- Must contain at least one numeral (0-9) and one special character (~!@#$%^&*+<>?=)
- Passwords expire after 30 days and must be reset by the account owner
- The last three passwords used to access an account may not be reused

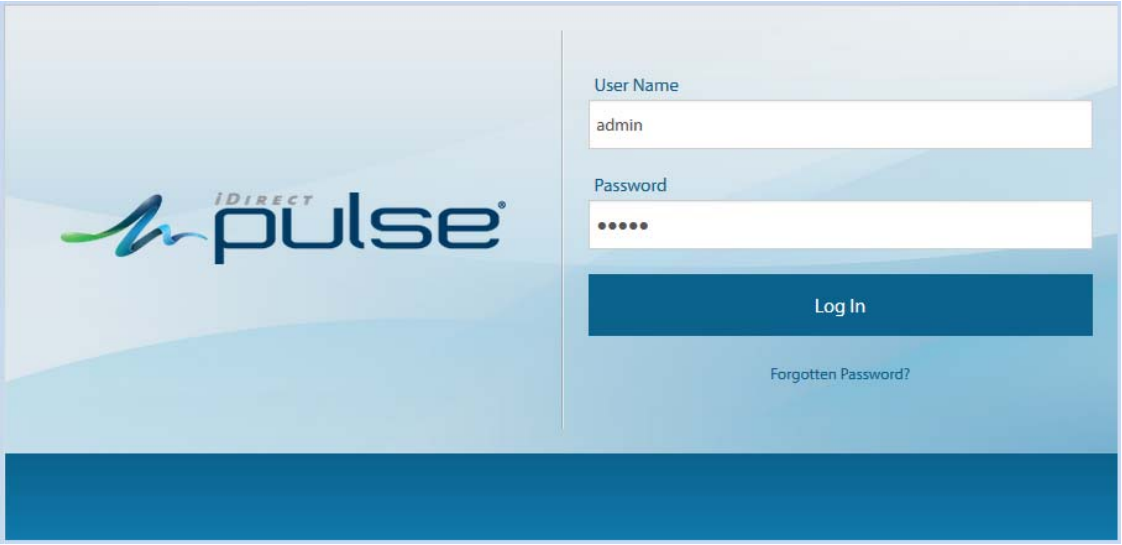
1.1.3 User Login

After the initial NMS login, the user interface is opened to the **Welcome** landing page and login dialog. You must enter your assigned user name and password to be authenticated.

An NMS user session is established after the user name and password are entered correctly.

To login to the Network Management System Web User Interface:

1. Enter the assigned **User Name** and **Password**.
2. Click **Log In** to submit the authentication credentials to the NMS.



User Name: admin

Password: •••••

Figure 1-2. iDirect Pulse™ Welcome page - NMS User Login Dialog

1.1.4 User Session

After successfully entering a user name and password, users are authenticated by the system, the NMS establishes a *user session*, and the user interface opens to the configured landing page. The user account or group determines the landing page to which the NMS opens.

User sessions in which there is no activity for 30 minutes, or some other configured duration, are automatically terminated and logged out. On the next login, the session is restored to the NMS page where it was last terminated.

1.1.5 Logging Out

When terminating a user session it is important to do so correctly, by clicking the "User Profile" link and logging out. Simply closing the browser may result in not being able to login again without some delay. Such may be the case if the session is terminated by closing the browser in a system where the automatic termination and log out feature is enabled. If the browser is closed without logging out, it may be necessary to wait for the session to expire before it is possible to re-establish another connection.

The **User Profile** menu is labeled with the user name of the current session and is located to the far right of the Main Navigation bar. In the screenshot shown below, "**admin**" is the current user.

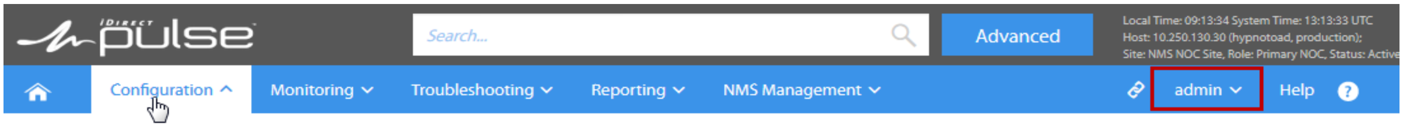

iDirect pulse
Search...
Advanced
Local Time: 09:13:34 System Time: 13:13:33 UTC
Host: 10.250.130.30 (hypnotoad, production);
Site: NMS NOC Site, Role: Primary NOC, Status: Active
Configuration
Monitoring
Troubleshooting
Reporting
NMS Management
admin
Help

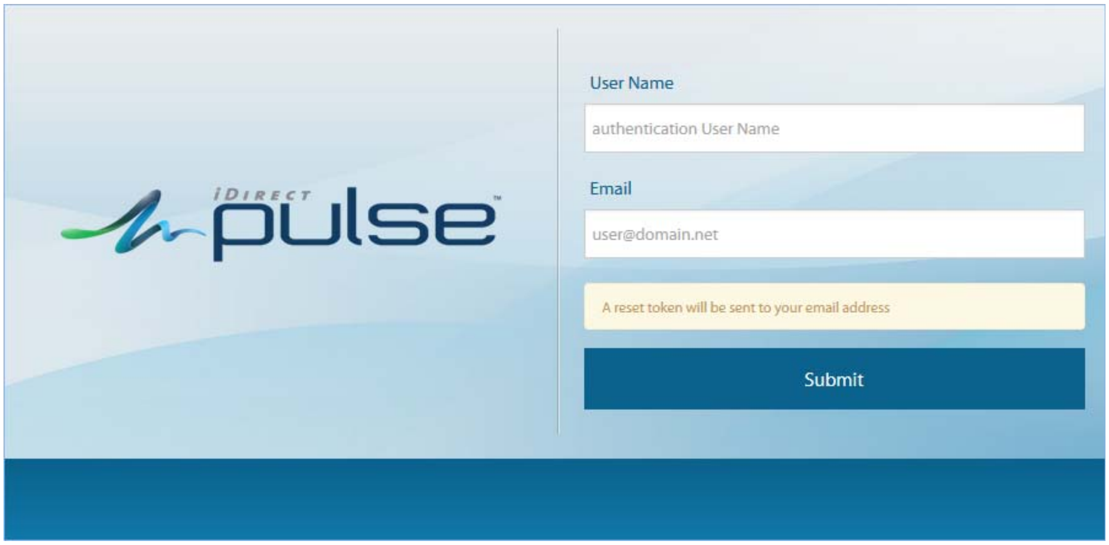
Figure 1-3. User Profile - Log Out

1.1.6 Account Lockout

During any login, a user account may become locked if login credentials are incorrectly submitted on several attempts. If the account becomes locked, any further login attempts will be unsuccessful until an authorized system administrator unlocks the account.

1.1.7 Forgotten User Name or Password at Login

If a user name or password is forgotten, recovery may be possible, but only if the feature is enabled. Otherwise, a user that is locked out will need to contact an authorized user administrator or an individual with the appropriate system-level access.



A reset token will be sent to your email address

Figure 1-4. Recover User Password/User Name

To recover a user account password:

1. Click the **Forgotten Password** link that is displayed on the login dialog.
2. Type the **User Name and E-mail** address that was configured for the NMS user account.
3. Click **Submit.** If the account is found, a reset token link is sent to the e-mail address. Otherwise, a message is displayed if the user name or e-mail address is not found.
4. Click the reset token link, received in the email. The **Change Password** dialog is presented.
5. Type a **New Password** and re-type to **Confirm New Password**.
6. Click **Submit**, and the normal NMS login dialog is presented.
7. Enter the **User Name** and newly created **Password**.
8. Click **Log In**.

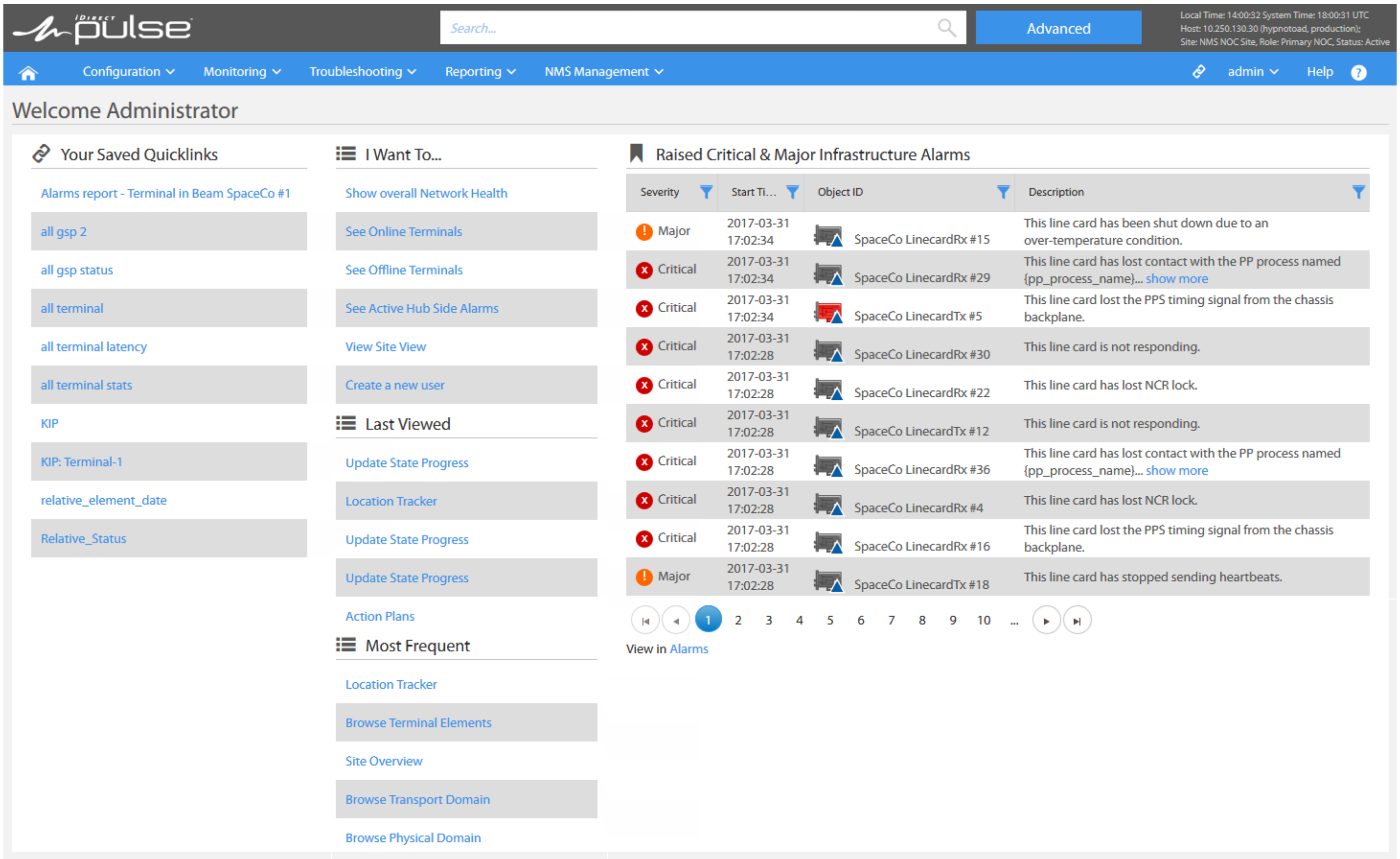
1.2 Home Page

The “Home Page” is the default user page, opened on each Pulse login, regardless of the login device, for all users. A dashboard view of a collection of commonly used Pulse tools as well as specific navigation links that appear based on the previous usage by the user. The Welcome page can be re-displayed, from any other page, by clicking the Pulse® logo in the top left page corner or by clicking the Home icon located on the blue navigation bar.

A click on the element icon of any alarm opens the Key Information Panel (KIP) to view additional information about the alarm.

Items that may be seen on the page include the following:

- **Your Saved Quicklinks** — user-saved links to specific monitoring/reporting operations
- **I Want To…** — list of links to your most commonly used NMS tools
- **Last Viewed** — list of links to your most recently used NMS pages -starting with last used
- **Most Frequent** — list of links to your most visited NMS pages
- **Raised Critical & Major Infrastructure Alarms** — critical/major alarms of the last 24 hrs


iDirect pulse
Search...
Advanced
Local Time: 14:00:32 System Time: 18:00:31 UTC
Host: 10.250.130.30 (hypnotoad, production);
Site: NMS NOC Site, Role: Primary NOC, Status: Active
Configuration
Monitoring
Troubleshooting
Reporting
NMS Management
admin
Help

Welcome Administrator

Your Saved Quicklinks

- Alarms report - Terminal in Beam SpaceCo #1
- all gsp 2
- all gsp status
- all terminal
- all terminal latency
- all terminal stats
- KIP
- KIP: Terminal-1
- relative_element_date
- Relative_Status

I Want To...

- Show overall Network Health
- See Online Terminals
- See Offline Terminals
- See Active Hub Side Alarms
- View Site View
- Create a new user

Last Viewed

- Update State Progress
- Location Tracker
- Update State Progress
- Update State Progress
- Action Plans

Most Frequent

- Location Tracker
- Browse Terminal Elements
- Site Overview
- Browse Transport Domain
- Browse Physical Domain

Raised Critical & Major Infrastructure Alarms

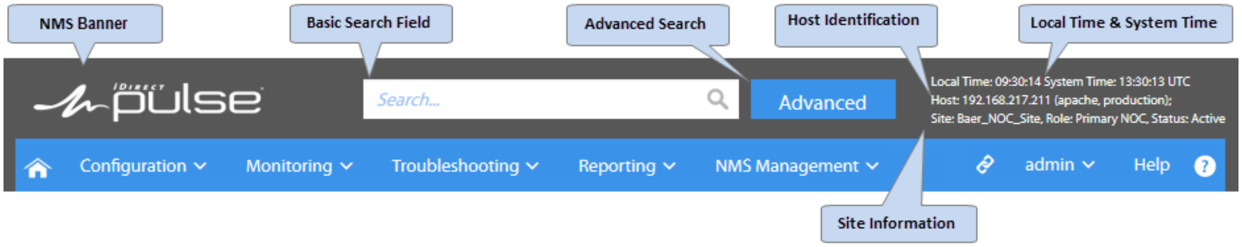
Severity	Start Ti...	Object ID	Description
Major	2017-03-31 17:02:34	SpaceCo LinecardRx #15	This line card has been shut down due to an over-temperature condition.
Critical	2017-03-31 17:02:34	SpaceCo LinecardRx #29	This line card has lost contact with the PP process named {pp_process_name}... show more
Critical	2017-03-31 17:02:34	SpaceCo LinecardTx #5	This line card lost the PPS timing signal from the chassis backplane.
Critical	2017-03-31 17:02:28	SpaceCo LinecardRx #30	This line card is not responding.
Critical	2017-03-31 17:02:28	SpaceCo LinecardRx #22	This line card has lost NCR lock.
Critical	2017-03-31 17:02:28	SpaceCo LinecardTx #12	This line card is not responding.
Critical	2017-03-31 17:02:28	SpaceCo LinecardRx #36	This line card has lost contact with the PP process named {pp_process_name}... show more
Critical	2017-03-31 17:02:28	SpaceCo LinecardRx #4	This line card has lost NCR lock.
Critical	2017-03-31 17:02:28	SpaceCo LinecardRx #16	This line card lost the PPS timing signal from the chassis backplane.
Major	2017-03-31 17:02:28	SpaceCo LinecardTx #18	This line card has stopped sending heartbeats.

View in Alarms

Figure 1-5. Pulse Welcome Page.

1.3 Pulse Banner

The Pulse *banner* is the dark gray area across the top of each Pulse page. The banner is also referred to as the *global header*, since it appears on every Pulse page.



Local Time: 09:30:14 System Time: 13:30:13 UTC
Host: 192.168.217.211 (apache, production);
Site: Baer_NOC_Site, Role: Primary NOC, Status: Active

Figure 1-6. Pulse NMS Banner

A a brief overview of each of Pulse banner elements is provided below:

- **Search** — Use to perform a quick NMS database search for any element, by Element Name or IP address. Results start to display after typing a few characters, and are continually displayed and filtered as characters are typed.
- **Advanced** — Use to perform refined searches throughout the NMS database for any element. Custom queries built using Boolean operators AND/OR may be combined with compare arguments to return complex search results into a new browser tab.
- **Site information** — Information about the NMS site.
  - **Local Time** — Displays the current local time of the user’s local workstation.
  - **System Time** — Displays the Coordinated Universal Time (UTC) of the NMS.
  - **Host** — The Host IP address of the server where the user is logged in.
  - **Site** — The Site at which the NMS is located. For example, Teleport, NOC, or EAP.
  - **Role** — The current operational role of the Site at which the NMS is located. For example, Primary, or Backup.
  - **Status** — The current status of the site. For example, Active, and Standby.

1.4 Main Navigation Tabs and Menus

Just below the Pulse banner, the main navigation tabs stretch across the top of each page. These tabs are the primary start points for navigating Pulse operations. Each tab supports access to one of the main functional areas of the Pulse NMS and the various pages and operations that comprise the functional area.

Clicking a menu tab displays a sub-menu of the operations available to the user, based on defined permissions. A single click on a tab, for example **Monitoring**, displays the associated Monitoring operations sub-menus. A second click on the tab hides the menu. With a menu displayed, a single click on an operation opens the page.

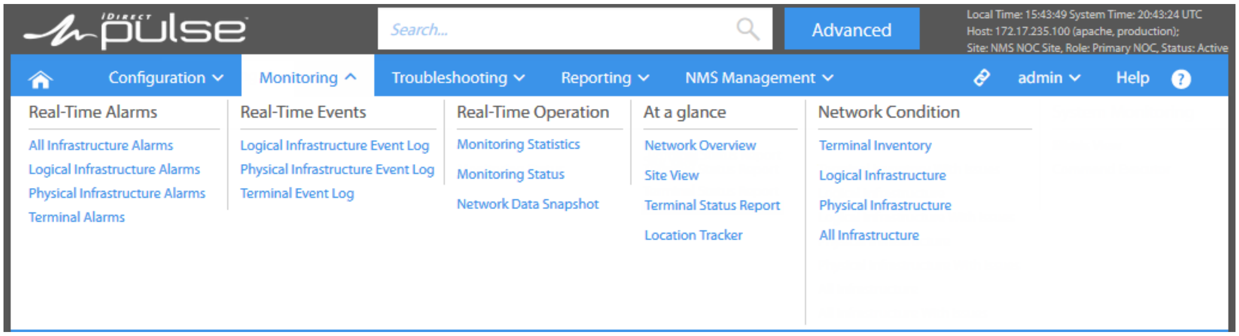


Figure 1-7. Main Navigation Tabs - Monitoring Menus

A brief overview of each of the main navigational tabs is provided below:

- **Home Icon** — From any Pulse page, click to display the user home page.
- **Configuration** — Provides access to Pulse NMS pages and menus used to configure the various elements of each element domain, for the purpose of building a network. These element domains include Physical, Transport, Network, Service, and Terminal.
- **Monitoring** — Provides access to Pulse pages and menus used to generate a variety of real-time reports on all network events, alarms, and incidents.
- **Troubleshooting** — Provides access to NMS Probe Commands for NMS and PP Clusters, Line Cards, and Terminals; and an Debug Console for shell window access to elements.
- **Reporting** — Provides access to Pulse NMS pages and menus used to generate a variety of historical reports on all network events, alarms, and incidents.
- **NMS Management** — Provides access to NMS pages and menus used to configure and manage User Administration and System Administration domain elements.
- **Load Query Icon** — Displays a menu of saved Configurator queries. Clicking on a query loads the Configurator with the parameters of a previously saved query and performs the associated operation.
- **User Profile Menu** — Click the user name to display the User Profile menu, or to terminate the current session.
- **Help Menu** — Click **Help** or the Help icon (?) to display available Pulse help options. For example, **Alarms Help**, **Icon Help**, or **Configuration - Getting Started Guide**, which is a PDF download document that outlines building a Velocity Network.

1.5 Using the Load Query Icon

The Load Query icon is displayed on the Main Navigation Bar. Clicking on the **Load Query** icon displays a list of user-created queries that are saved in the user's profile. If the query was saved using **Save Query Only**, then it can be used with a different tool, or from anywhere within Pulse; if the query was saved using **Save Query and Tool**, then it can be used to recreate the exact report, and used from the Configurator.

Clicking on a specific query, from the menu, opens to the Configurator panel and loads the parameters saved when the query was created. See *Saving a Query*.

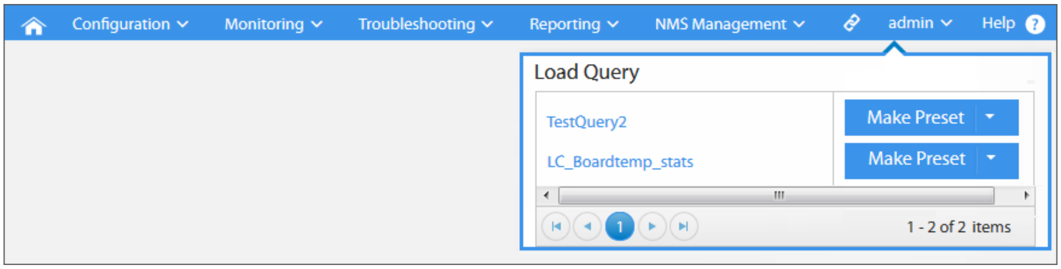


Figure 1-8. Using the Load Query Icon

To load a query from the Load Query menu:

1. Click the **Load Query** icon on the current Pulse banner.
2. If necessary, use the next and previous buttons to traverse through the list of queries.
3. Click on the hyperlink of the desired query from the list of queries. Pulse navigates to the Configurator and loads the stored parameters. The operation is executed.

To make a preset from a query:

1. Click the **Load Query** icon on the Pulse banner.
2. Use the next and previous navigator buttons to traverse through a list of queries.
3. With the desired query displayed, click the **Make Preset** button. The query is re-saved. The result of making a preset is that the query is no longer shown in this list, as these quicklinks are tied to a specific Pulse tool. The saved query is then available for use in all tools across Pulse where there is a Load Query option.

To rename or delete a saved query:

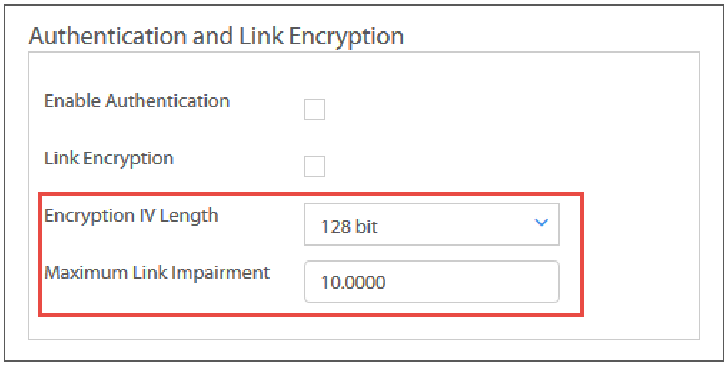
1. Click the **Load Query** icon to display the **Load Query** dialog.
2. If necessary, use the next and previous buttons to traverse through the list of queries.
3. Click the **Make Preset** drop-down list of the desired query. The **Make Preset**, **Rename,** and **Delete** options are displayed. Use one of the following procedures:
   a. Click **Make Preset** to use the currently selected query to make a preset.
   b. Click **Delete**, and when prompted, respond with '**Yes'** to remove the saved query from the user profile.
   c. Click **Rename** to enable renaming of the query. Rename the query as desired, and press the **Enter** key to save the renamed query.

1.6 General Editing

The following section describes basic editing features such as default values, required and optional fields, as well as other editing features seen on screen throughout the Pulse NMS.

1.6.1 Default Value Fields

Throughout the various NMS element configuration pages, many data fields, including check boxes and drop-down selections, are preset with a *default value*. These values, which generally represent a typical setting or selection, in most cases can be modified to suit the specific requirements of the element that is being configured.



Authentication and Link Encryption

Enable Authentication ☐

Link Encryption ☐

Encryption IV Length: 128 bit

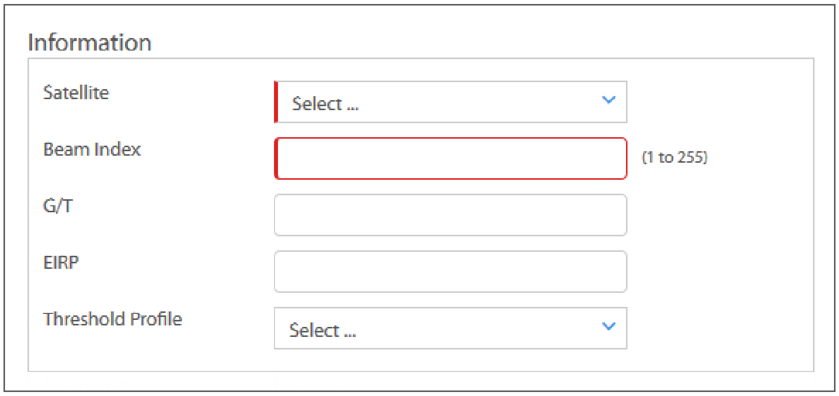
Maximum Link Impairment: 10.0000

Figure 1-9. Default Value Fields

1.6.2 Required and Optional Fields

Many of the NMS pages contain one or more fields that require data entry in order to complete the configuration of the element, and for the configuration to be applied. All such fields are considered *required fields*. Required, fields are generally outlined in red, but are indicated with a red line on the left edge, in the case of drop-down selection fields.

A field that may be edited, but does not require data input is considered an *optional field.* These optional fields are outlined in gray and may or may not contain a default value.



Information

Satellite: Select ...

Beam Index: (1 to 255)

G/T

EIRP

Threshold Profile: Select ...

Figure 1-10. Optional and Required Fields

1.6.3 Enabled/Disabled Fields

Some fields are only displayed and can be written to if a related and controlling field is enabled. If the controlling field is disabled, dependent fields are also not displayed.

In the left screen shot, the RTP Compression check box is not selected. In the right screen shot, the RTP COmpression check box is checked and the associated dependent fields are displayed and enabled.

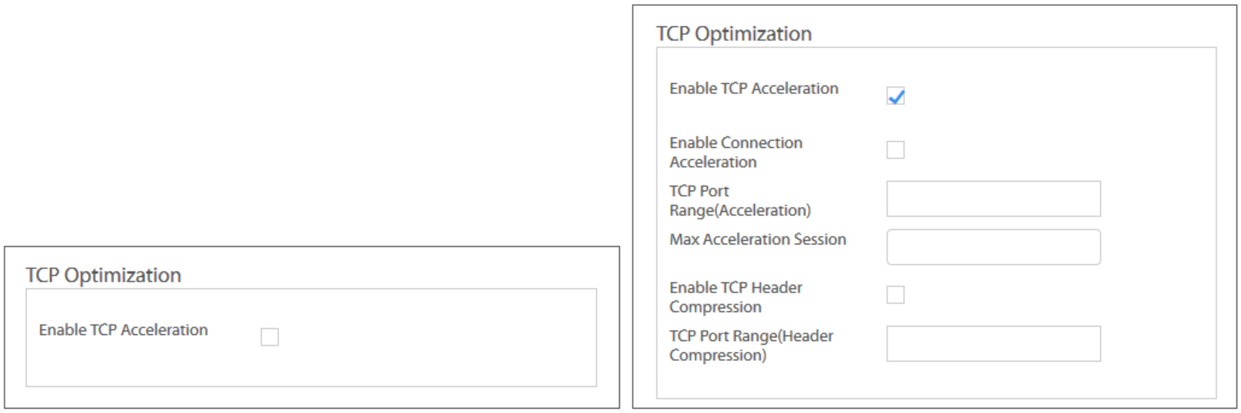

TCP Optimization
Enable TCP Acceleration ☐
TCP Optimization
Enable TCP Acceleration ☑
Enable Connection Acceleration ☐
TCP Port Range(Acceleration)
Max Acceleration Session
Enable TCP Header Compression ☐
TCP Port Range(Header Compression)

Figure 1-11. Enabled/Disabled Fields

1.6.4 Predictive Search Filtering Fields

Some fields that involve making a selection from among many choices use *predictive search filtering* to simplify finding the exact choice. By default, an entire list of possible selections is displayed, but as each character is typed the list is narrowed by matching the characters, in order, to list items. Currently, this feature is case-sensitive.

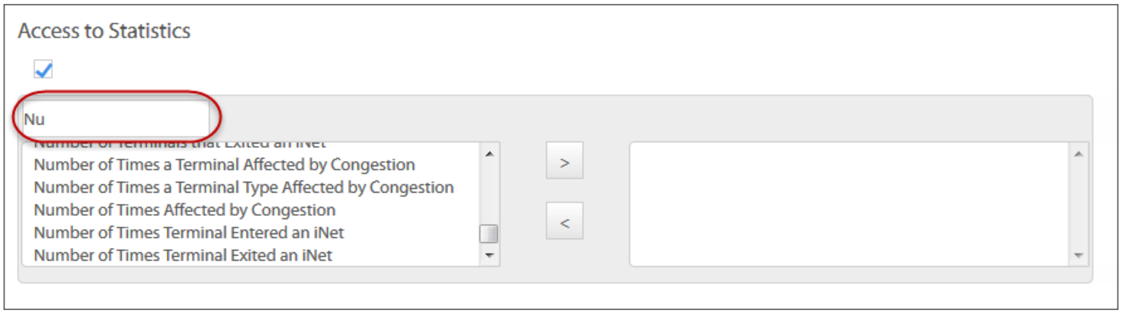
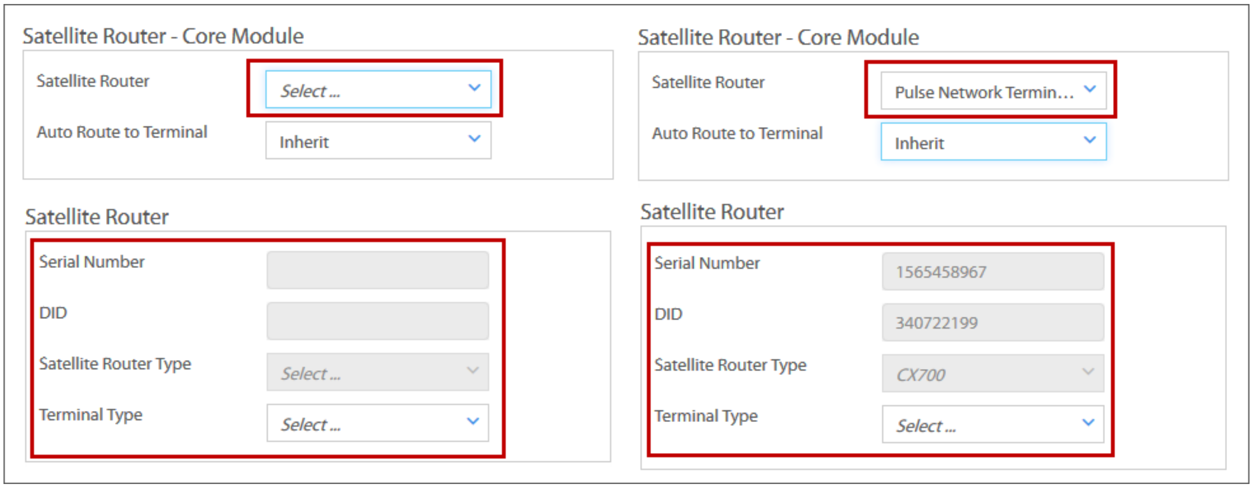

Access to Statistics
☑
Nu
Number of Terminals that Exited an iNet
Number of Times a Terminal Affected by Congestion
Number of Times a Terminal Type Affected by Congestion
Number of Times Affected by Congestion
Number of Times Terminal Entered an iNet
Number of Times Terminal Exited an iNet
>
<

Figure 1-12. Field with Predictive Search Filtering

1.6.5 System Generated Fields

In Pulse, *system generated fields* are derived by the NMS and typically involve a unique numeric value such as a derived identifier (DID) or a text value, such as a name.

System generated field values are typically automatically populated upon entry of a specific related field. In the example, the first screen shot shows the **Serial Number** and the **DID** fields are originally blank; when the user selects a value in the **Satellite Router** field, as shown in the second screen shot, both fields are generated.



Satellite Router - Core Module

Satellite Router: Select ...
Auto Route to Terminal: Inherit

Satellite Router

Serial Number:
DID:
Satellite Router Type: Select ...
Terminal Type: Select ...

Satellite Router - Core Module

Satellite Router: Pulse Network Termin...
Auto Route to Terminal: Inherit

Satellite Router

Serial Number: 1565458967
DID: 340722199
Satellite Router Type: CX700
Terminal Type: Select ...

Figure 1-13. System Generated Field

1.6.6 Configuration Save Buttons

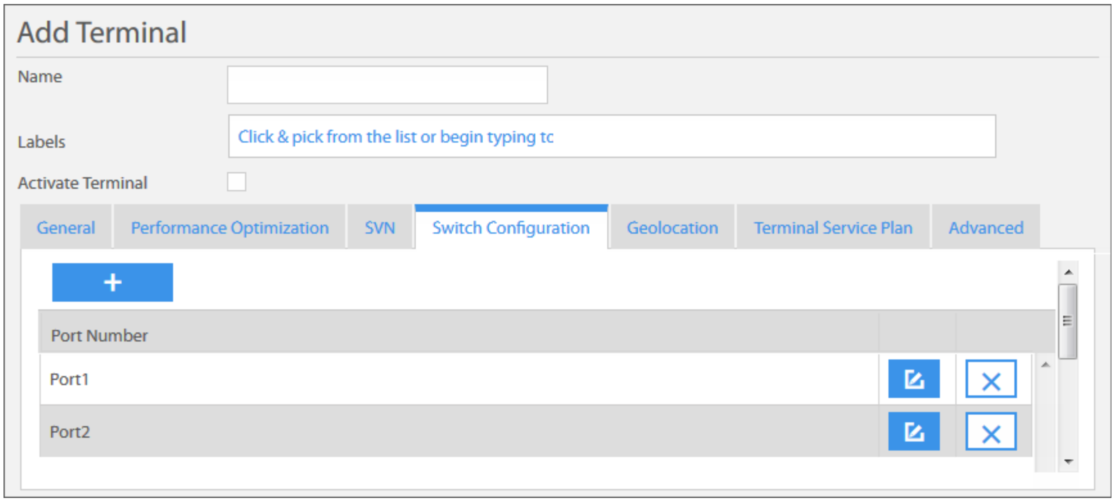
Each Pulse NMS configuration dialog contains the following buttons. The actions of these buttons are briefly described in the table below:

Table 1-1. Save and Close Button Descriptions

Button Name	Button	Description
Save	Save	Saves the parameters of the current configuration page and leaves the dialog open to the Modify Object page.
Save and View Impact	Save and View Impact	Saves the open configuration page and re-directs to the Review Impact Analysis page to see the impact of the most recent configuration changes. See *Reviewing Impact Analysis of Applying Changes*.
Save and Close	Save and Close	Saves the open configuration page with the most recent changes, closes the dialog. and redirects to the associated Browse page. For example, using Save and Close after adding a new user redirects to Browse Users.
Cancel	Cancel	Causes any unsaved configuration parameters of the current configuration page or tab to be discarded. The most recent changes are not saved and the user is re-directed to the associated Browse page.

1.6.7 Data Record Buttons

The configuration for some network elements, in addition to having several discrete parameters, may also include a table component where multiple records may be added. For example, the Terminal **Switch Configuration** contains a table of the **Port Number** records. Satellite Terminals also have **SVN** records as part of its SVN configuration; and **Terminal Service Plan** component records, as part of the Terminal Service Plan configuration.



Name

Labels: Click & pick from the list or begin typing tc

Activate Terminal ☐

Port Number
Port1
Port2

Figure 1-14. Satellite Terminal Switch Configuration Data Records

The button icons shown and described in Table 1-2, are found on some NMS pages where an element configuration includes data records. These buttons support the entry of data records, as well as the editing and removal of records. Once the fields of a record are entered, clicking the **Update** button accepts the record entry. After a record entry is updated, the **Update** button is immediately replaced by the **Edit** record button, and the **Delete** record button.

Table 1-2. Data Record Buttons

Button Name	Icon	Description
Add Record	+	Insert a new record into a data table. For example, a new **Inroute Group or Inroute Group Composition** record.
Update Record	✓	Update/accept the edited configuration parameters for the selected record. The record is updated in memory, but is not saved until the current configuration file is saved.
Edit Record	✎	Modify the configuration for the selected record. To accept the modified record, click the **Update** button to insert the record in memory.
Delete Record	✕	Remove the selected record from the table. The record removal is updated in memory, but not saved until the configuration file is saved
Export Data Records	CSV Export	Click to open the data records in a compatible application, such as Excel, or save the records to the file system.

1.7 Group Editing of Multiple Elements

In an iDirect Network system, NMS users with appropriate permission can simultaneously edit multiple elements of the same type. This operation might include modifying the parameters of any number of terminals, receive line cards, transmit line cards, or any other elements.

When performing a multiple edit operation, the modification may involve any of the visible fields that are common to the selected elements. This feature might be used, for example, to change the maximum transmit power value of 100 terminals, all in a single operation.

1.7.1 Group Edit Requirements

- **Select Multiple Elements** — the **Group Actions** button is only enabled if multiple elements are selected. For example, select tow or more elements in the Browse Physical Domain results list.
- **Select Elements of Same Type** — all elements must be of the same domain, for example **Physical Domain**, **Transport Domain**, or **Terminal Domain**; and the same element type. For example, Line Cards only, PP Servers only, or Users only.

1.7.2 Editing Multiple Elements Simultaneously

After a list of elements is returned in a Browse window, it is possible to find and select a group of elements for which a group edit operation can be performed.

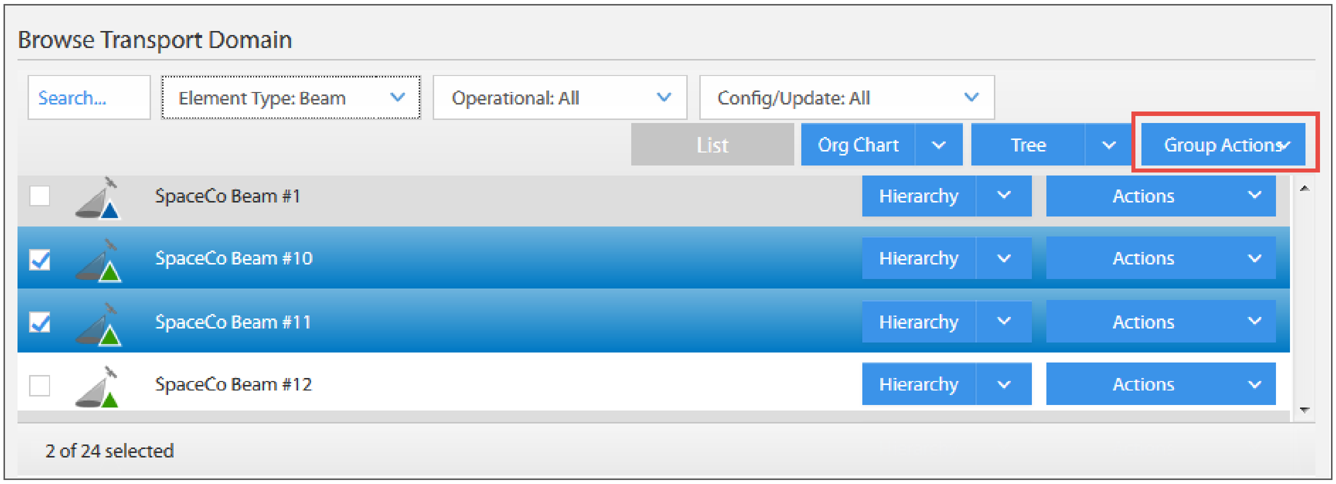
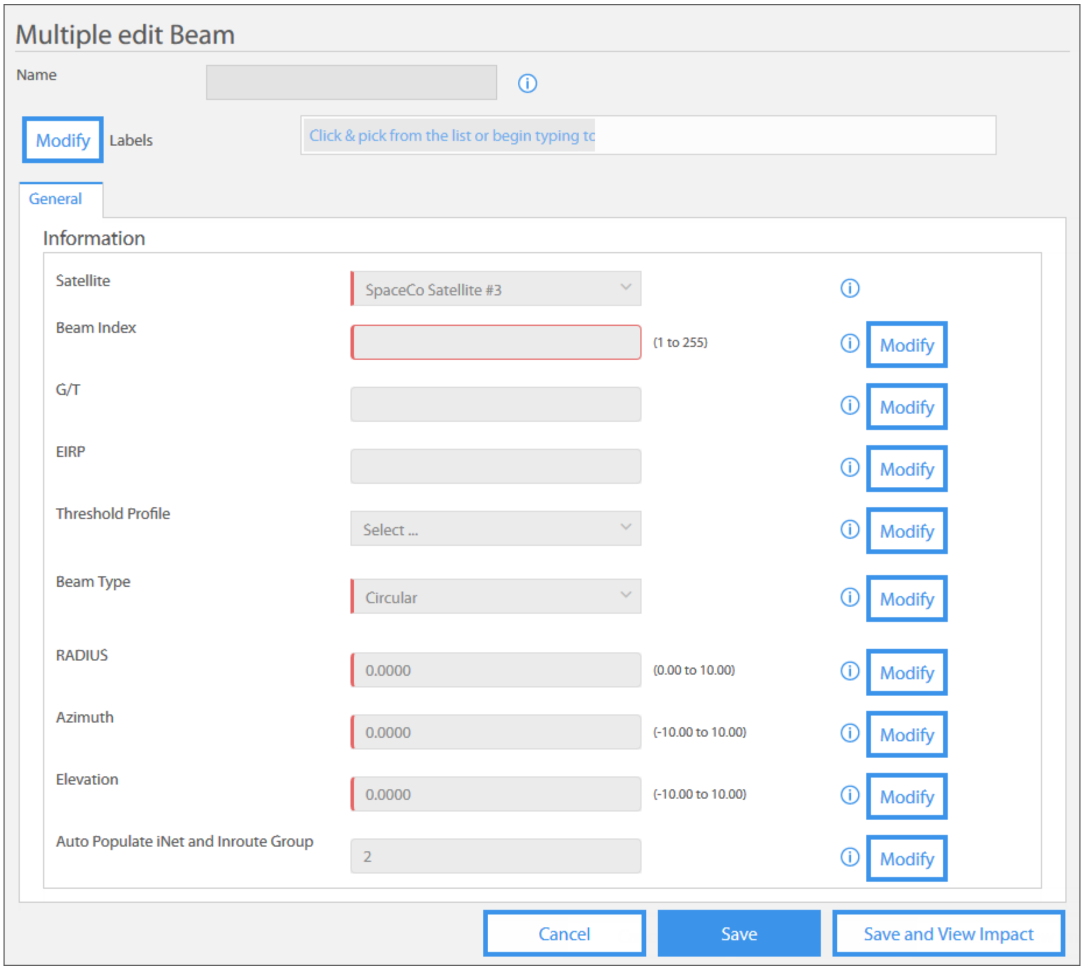


Figure 1-15. Browse Elements Results

To edit multiple elements of the same type:

1. From the desired domain, select the appropriate **Browse** command to return a list of the target elements. For example, **Browse Physical Domain** to perform a group edit on multiple Line Cards; or **Browse Terminals** to perform a group edit on multiple terminals.
2. With elements displayed, use the **Element Type** drop-down list and choose an element type to filter the display. For example — select **Linecard** to display line cards only.

3. Select multiple elements or click the **Select All** link to select all elements in the browse window. The **Group Actions** button is disabled if less than two elements are selected.
4. Click the **Group Actions** button to show a context-sensitive list of possible actions based on the selected elements.
5. Select **Edit** to perform a group edit on the selected elements. The group edit dialog is displayed. Each field that can be modified, as a group, has an adjacent **Modify** button.
6. Hover over the information icon adjacent to an element to view field information.
7. Click the **Modify** button adjacent to a field to edit the field. Multiple fields may be modified. Respond "**Yes**" when prompted, to modify the fields. The field is enabled.
8. Modify the field, as required, or click **Cancel** to abort the edit.
9. With the **Multiple Edit** page still open, click **Cancel** to disable a field that was initially enabled for editing. The field is left unmodified.
10. Click **Save** to save changes or click **Save and View Impact** to see impact of the change.



Name

Labels: Click & pick from the list or begin typing tc

Satellite: SpaceCo Satellite #3

Beam Index: (1 to 255)

G/T

EIRP

Threshold Profile: Select ...

Beam Type: Circular

RADIUS: 0.0000 (0.00 to 10.00)

Azimuth: 0.0000 (-10.00 to 10.00)

Elevation: 0.0000 (-10.00 to 10.00)

Auto Populate iNet and Inroute Group: 2

Figure 1-16. Group Edit - PP Example

1.8 Element Labels

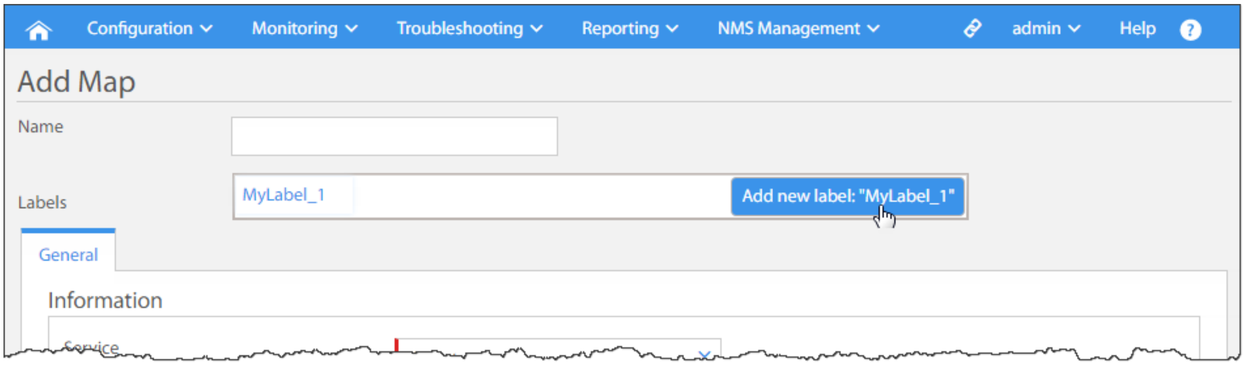
Starting with Pulse 2.3, users can create string labels that can be assigned to any element. A label is an alphanumeric string, that once created, can be associated with one or more elements. Once assigned, labels can be used to search and return all elements to which the label has been assigned.

This feature lets users search for and return a group of elements that are not necessarily associated with the same domain, but may be in any number of domains.

1.8.1 Creating and Assigning Labels

Some general guidelines for creating and assigning labels are given below:

- A label can be created for or assigned to any physical or logical network element
- A new label can be created and assigned to an element as the element is being created.
- A label can be created with the same spelling and using different case — for example, “LaBeLs” “labels” and “lAbElS” are all treated as the same label.
- Labels spelled the same, regardless of case, are returned in the labels list. A results list of a query for “label” — for example, might show “LaBeL”, “label”, and “lAbEl”.
- Labels may contain spaces and other non-alphabetical characters—for example, !@#$%&.
- Labels are returned if the typed string is contained anywhere in the saved labels — for example, type “abe” and the results show “labels” and “label”.



Labels: MyLabel_1

Figure 1-17. Creating Labels using an Element Add Dialog

To create a new label:

1. With a dialog open to add or modify an element, click in the **Labels** field and start typing the name of a new label, and when you have entered the label click the **Add new Label** button at the end of the **Labels** field. **See Note**
2. Repeat the process to create additional labels for this element.
3. To remove a label from an element, click in the field to show the labels, then click the “**X**” on a specific label to remove the label. The lablel is not removed from the database, but only from the element.

To assign one or more labels to an element:

1. With a dialog open to add or modify an element, click in the **Labels** field to reveal a list of the labels that have been created in the NMS. **See Note**.
2. Click on a label to assign it to the element. You may assign additional labels by repeating the process.
3. To remove a label from an element, click in the field to show the labels, then click the “X” on a specific label to remove the label. The label is not removed from the database, but only from the element.

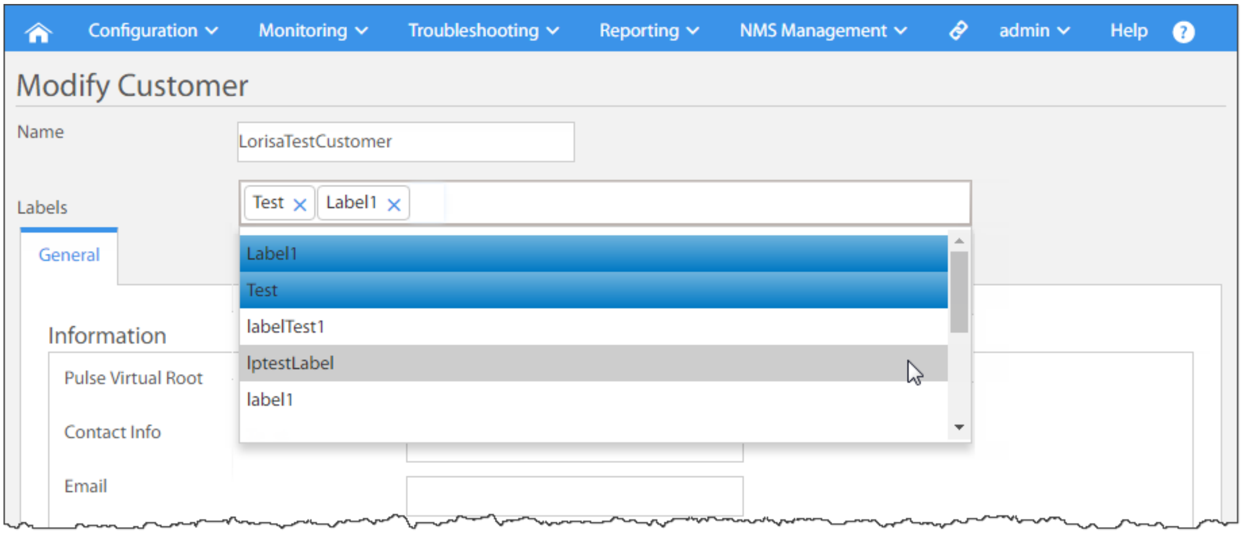


Figure 1-18. Assigning Labels in Element Create (Add) Dialogs

NOTE: When working with a given element, labels already assigned to the element are shown selected in blue.

2 Pulse Element Domains

In Pulse, each of the various elements of an iDirect Network are contained in one of several Pulse element domains. Element domains — for example, physical domain, transport domain, network domain, service domain, and terminal domain all serve to give structure to the physical and logical components of an iDirect Network. This structure aids network operators in mentally organizing and managing large networks.

The logical grouping of elements, by domain, is seen in every aspect of the Pulse NMS, including the configuring, controlling, monitoring and reporting, troubleshooting and diagnosing of network elements.

Pulse element domains are introduced in the following topics:

- *The Element Domain Hierarchy* on page 20
- *Physical Domain Elements* on page 21
- *Transport Domain Elements* on page 22
- *Network Domain Elements* on page 23
- *Service Domain Elements* on page 24
- *Terminal Domain Elements* on page 25
- *User Administration Domain Elements* on page 26
- *System Administration Domain Elements* on page 27
- *Element Domains & the Pulse User Interface* on page 28

2.1 The Element Domain Hierarchy

To simplify the setup, organization, and operation of complex networks, iDirect Pulse employs a hierarchical element model in which configurable network elements are grouped into logically related collections called *Element Domains*.

Of the different Pulse element domains, represented in the NMS, the P*hysical*, *Transport*, *Network*, and *Service domains* form the primary infrastructure of an iDirect Network. Together, these domains provide essential services to the *Terminal Domain*, which in turn, provides IP connectivity between each remote LAN and the Velocity SAS equipment.

In working with an iDirect Network System, via the Pulse NMS, these four primary domains, as well as others, will contain the various elements that you will encounter. Other domains—for example, include *User Administration Domain*, and *System Administration Domain*. A brief overview of each element domain is presented in the remaining sections of this chapter.

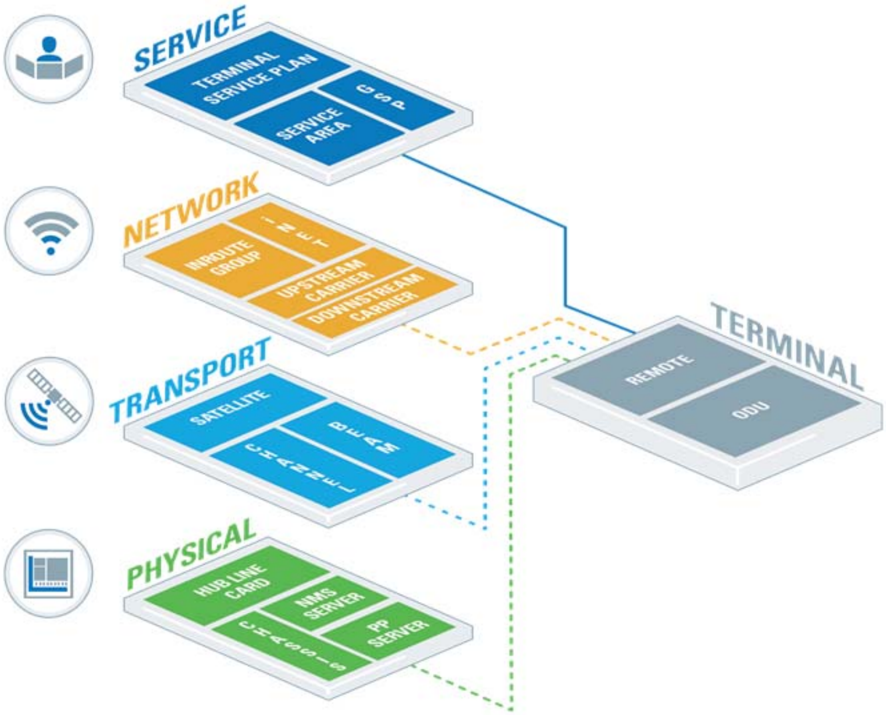


Figure 2-1. NMS Element Domains

2.2 Physical Domain Elements

The Physical Domain provides the physical infrastructure of an iDirect Network — it is the lowest level of NMS layered hierarchy of elements, and represents physical elements such as line cards, chassis, NMS and protocol processor clusters and servers, and the physical sites at which these physical elements are located.

Collectively, the physical domain encompasses both the physical elements and addressing structure to support the building out of the ground segment of the iDirect network. It includes NMS and PP clusters and servers at the SAS and NOC sites — subsystems that are responsible for network management, communication between the hub and satellite terminals, and global bandwidth management.

See *iDirect Velocity Network Operations Using Pulse*, for details on configuring the physical domain elements in a network.

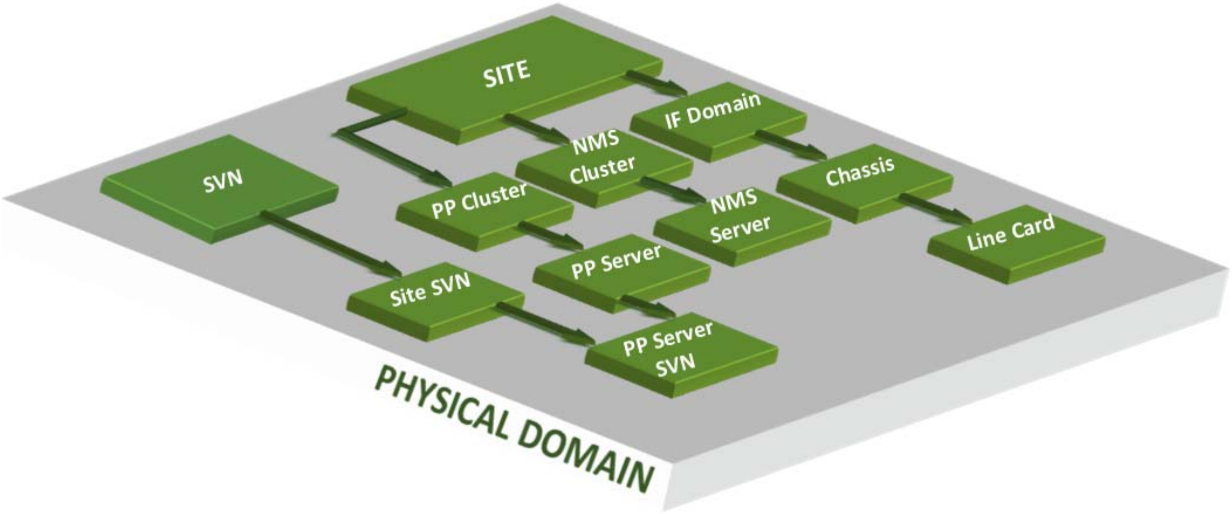


Figure 2-2. Physical Domain Elements

2.3 Transport Domain Elements

The Transport Domain is the second level of NMS hierarchy of elements — it is composed of elements that include satellites, beams, channels, and iNets. These elements, which support the transfer of network traffic, rely on configured Physical Domain elements, and are a subset of the total logical infrastructure of an iDirect Network.

Collectively, transport elements represent the space segment of the iDirect network, and the logical connections between the hub-side of the network and the connected terminals. In short, configuration of transport domain elements create the *over-the-air* communications channels and the satellite (space)-to-ground connectivity of the iDirect network.

See *iDirect Velocity Network Operations Using Pulse*, for details on configuring the transport domain elements in a network.

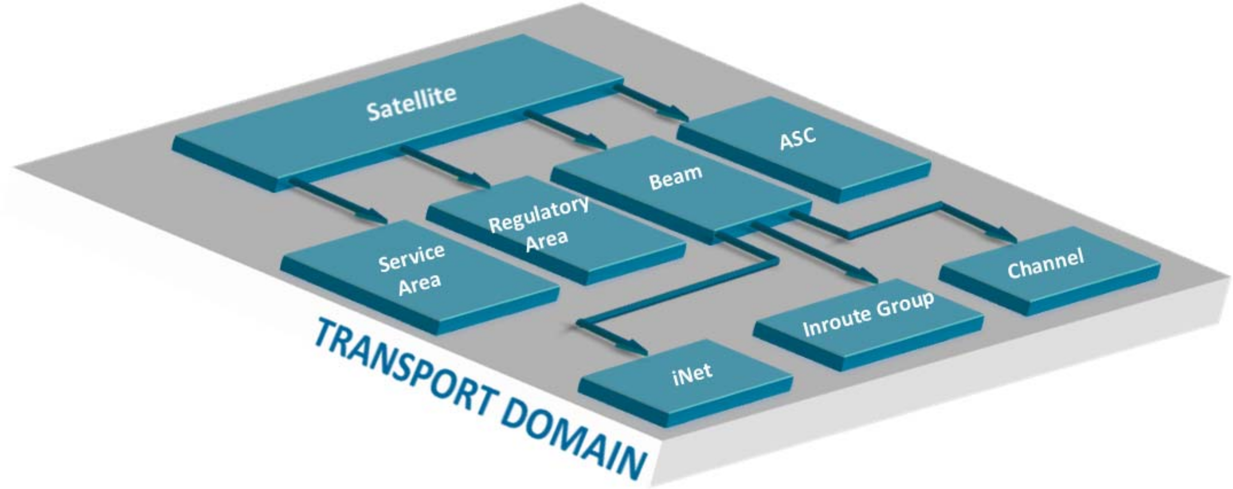


Figure 2-3. Transport Domain Elements

2.4 Network Domain Elements

The Network Domain — the third level of NMS hierarchy of elements — is composed of elements that include iNet Profiles, Inroute Group Profiles, and the associated upstream and downstream carriers. This domain supports the services provided by the Transport domain and how its resources are applied in supporting the connection to satellite terminals.

Collectively, Network Domain elements are a subset of the total logical infrastructure of an iDirect Network. It serves to provide a robust and adaptable data link between satellite terminals and hub systems. In operation, elements of the Network Domain are dynamically allocated to adjust the iDirect network data path to minimize negative impact due to changing weather conditions.

See *iDirect Velocity Network Operations Using Pulse*, for details on configuring network domain elements.

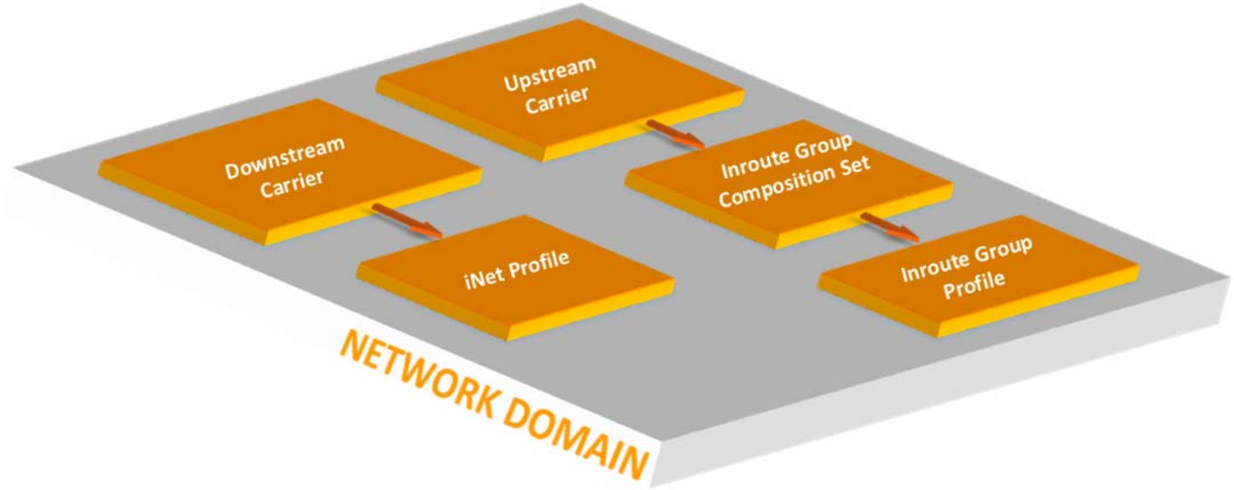


Figure 2-4. Network Domain Elements

2.5 Service Domain Elements

The Service Domain is at the highest level of NMS hierarchy of element domains — it represents elements such as Geographic Regions, unicast and multicast Group Service Plans and Subscriber Service Plan Profiles. These service domain elements provide the means by which bandwidth is allocated and managed throughout an iDirect Network through service providers and the service that they offer.

Collectively, this domain supports the creation of the application services that occur over the iDirect Network, as well as the allocation and management of bandwidth used by those services. These functions are facilitated through service plans and service plan profiles; and through *Group Quality of Service (GQoS)* and fair access policy (FAP) implementations.

In short, the Service Domain represents the service infrastructure of the iDirect network, which supports user traffic over various network applications.

See *iDirect Velocity Network Operations Using Pulse*, for details on configuring service domain elements in a network.

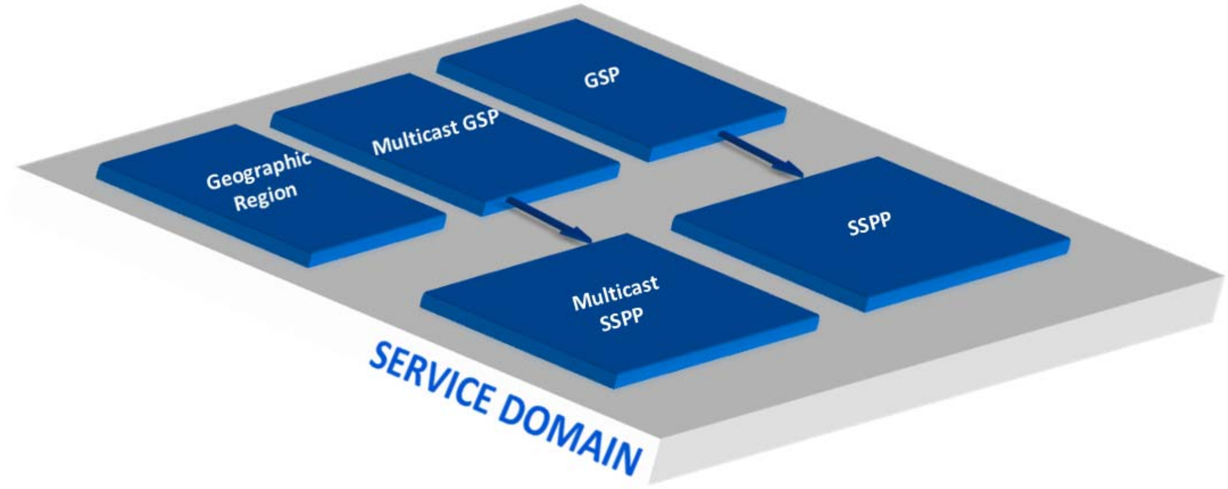


Figure 2-5. Services Domain Elements

2.6 Terminal Domain Elements

The Terminal Domain consists of both physical and logical infrastructure elements of an iDirect network. All other element domains support the Terminal domain. In Pulse, elements of the Terminal Domain fall into two categories — Terminal Components and Terminal Elements.

Terminal Components consists of the block up converter (BUC), low noise block (down) converter (LNB), antenna control unit (ACU), satellite router, and terminal type. Terminal Elements refer to Satellite Terminals.

See *iDirect Velocity Network Operations Using Pulse*, for details on configuring terminal domain elements in a network.

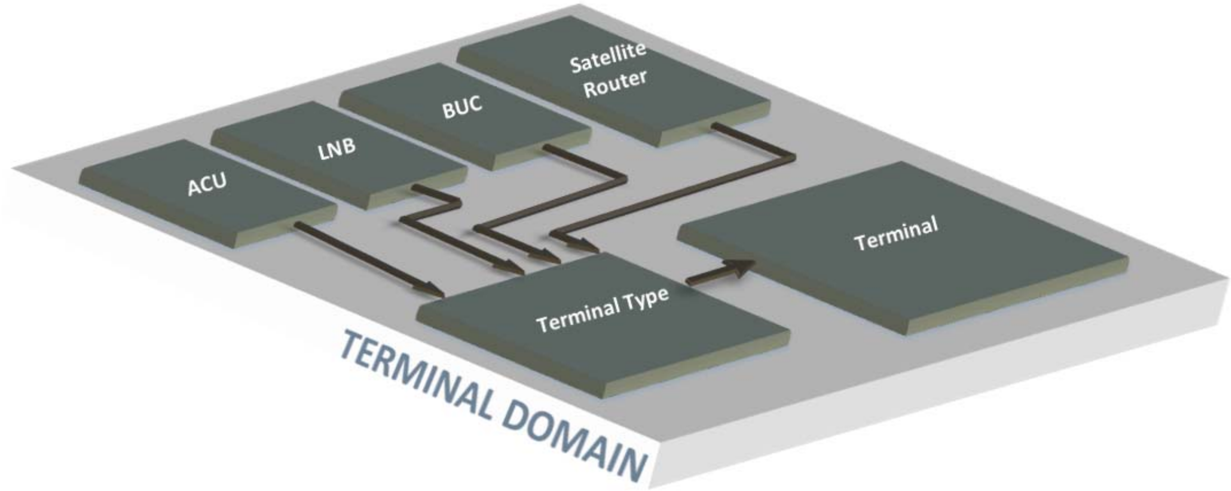


Figure 2-6. Terminal Domain Elements

2.7 User Administration Domain Elements

The Pulse User Administration Domain represents those NMS elements that support creation and management of user groups, user accounts, user roles, and that assigns permission-based access to the visibility and control of the iDirect Network.

Authorized users can access the NMS using the Web User Interface or via the Web Services API. This machine-machine API supports the creation of user roles, user groups, and user accounts, as well as define what access permissions are assigned to users and groups.

See Chapter 6, *Configuring & Managing User Settings*, for a complete description of these elements, along with step-by-step configuration instructions creating each in the NMS.

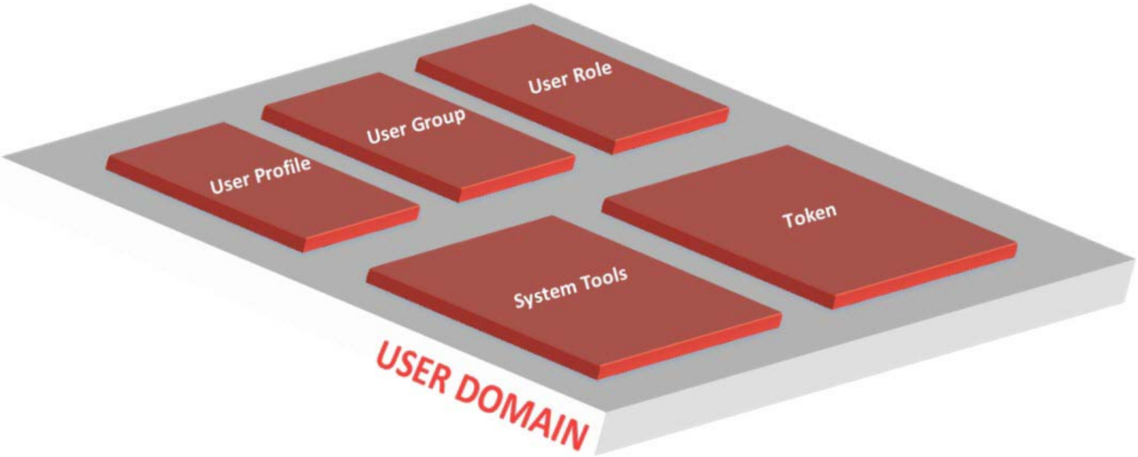


Figure 2-7. User Administration Domain Elements

2.8 System Administration Domain Elements

System Administration domain elements includes elements associated with NMS back-end operations, as well as those elements that support secure and efficient operation of an iDirect Network. This domain contains elements that support element authentication, license management, job scheduling, software upgrades and version management, as well as other system related elements that support network management.

For complete descriptions for System Administration Domain element see the following:

- Chapter 8, *NMS Services & System Management*
- Chapter 9, *NMS Element Security Management*
- Chapter 10, *NMS Software Installs & Upgrades*

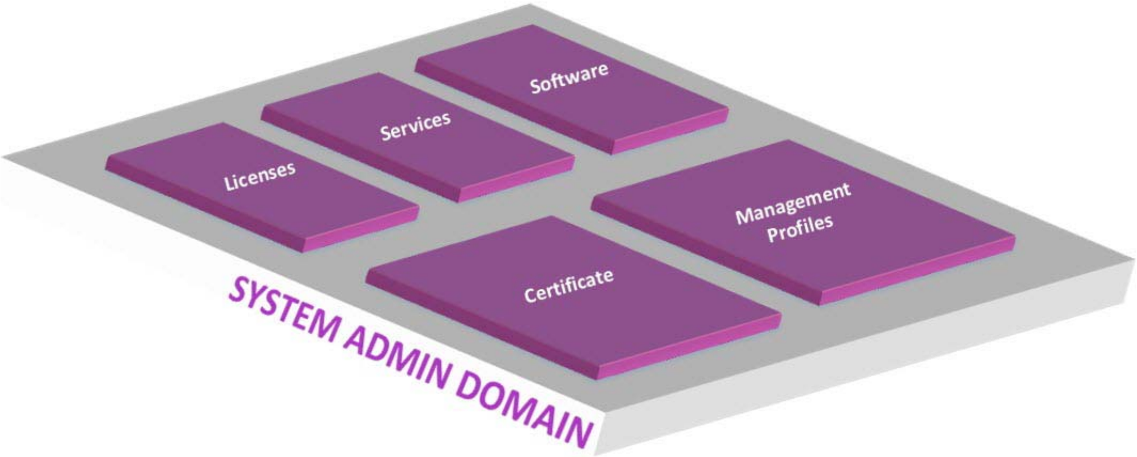


Figure 2-8. System Administration Domain Elements

2.9 Element Domains & the Pulse User Interface

Pulse element domains map directly to the top level menus of the Pulse user interface. The menu operations of the **Configuration** tab, for example, are partitioned according to the Terminal Domain, Service Domain, Physical Domain, Transport Domain, and Network Domain.

The **Configuration** tab provides access to these primary element domains, from which both physical and logical network elements must be configured when building an iDirect network.

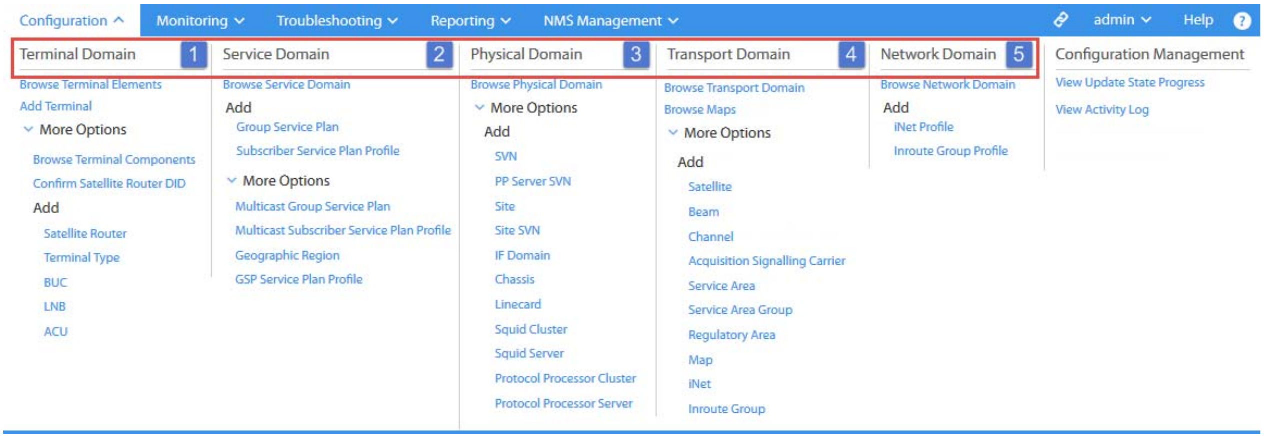


Figure 2-9. Pulse Web User Interface Main Menus and Element Domains

Pulse User Administration Domain and the System Administration Domain contain the operations for configuring and managing users and user access as well as for configuring and managing system operations. These network administration domains are both accessed from the Pulse **NMS Management** tab.

From this tab, you can access pages and tools for configuring the elements of these domains as well as tools for browsing, viewing, modifying and other operations

.

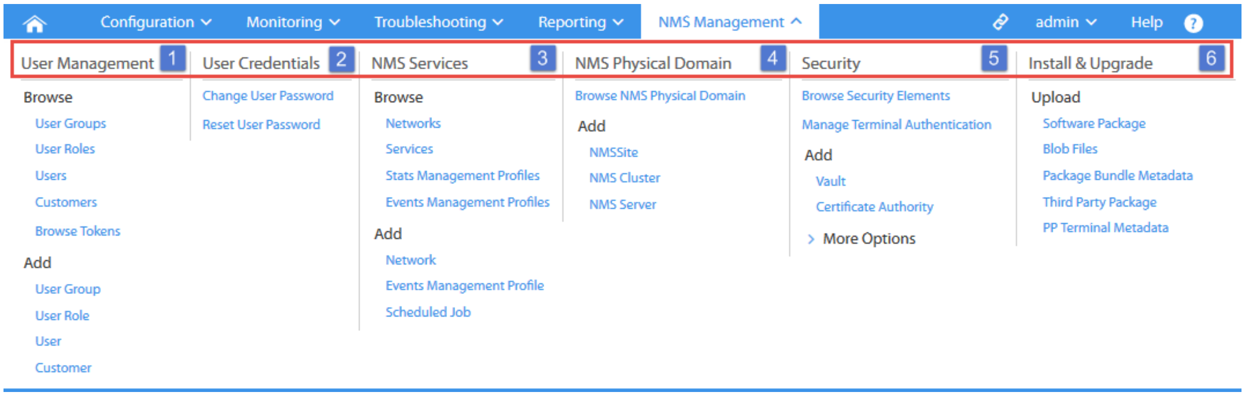


Figure 2-10. NMS Management Tab Operations

This relationship of element domains and Pulse user interface organization is carried throughout the Pulse pages and operations.

For additional information on the NMS element domains, see the following topics:

- *NMS Object Types* on page 146
- *NMS Element Icons* on page 147
- *NMS Element Management States* on page 148

3 Pulse Operations Overview

This chapter presents a brief overview of the Pulse NMS operations and tools for configuring, controlling, monitoring and reporting of iDirect Network elements.

An overview of Pulse operations are covered in the following topics:

3.1 Configure Pulse Element Domains

From the Pulse NMS **Configuration** menu, operators can access the various pages for configuring and managing the elements for each element domain, including the Terminal Domain, Service Domain, Physical Domain, Transport Domain, and Network Domain.

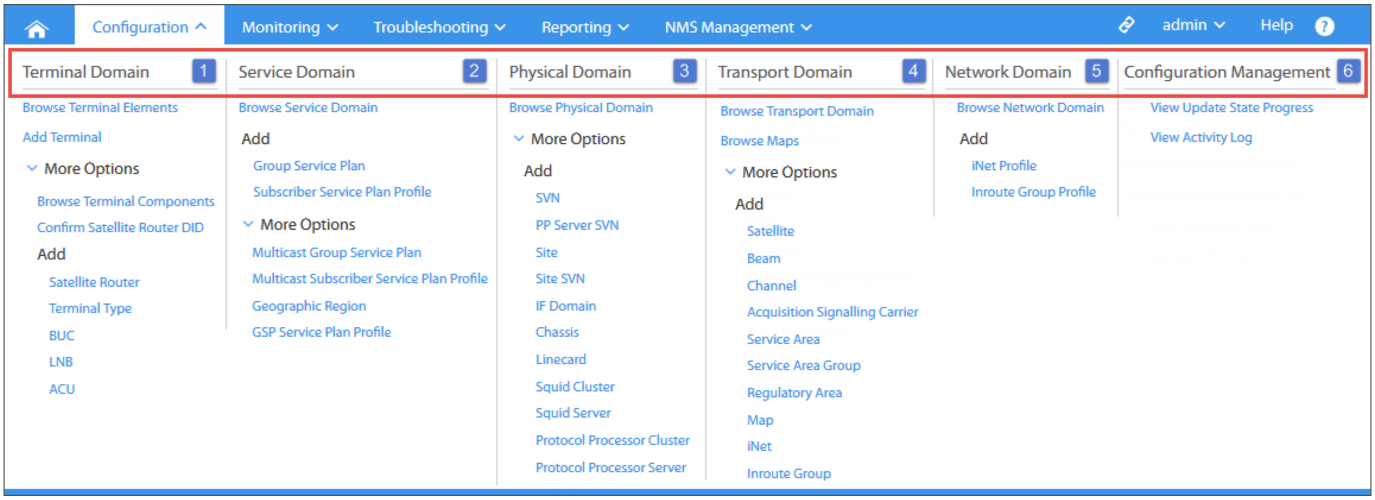


Figure 3-1. NMS Configuration Tab Sub-Menus — by Element Domains

The operations categories of the Configuration sub-menus are briefly described as follows:

- **Configuration** — Use these operations to add and configure new elements for each of the element domains, when building or adding to your network. For procedures on how to configure the elements of each domain, see *Velocity Network Operations Using Pulse*.
- **Browse Domains** — Use these operations to browse and list all of the configured elements found in the NMS for each element domain. The browse list can be filtered by Element Type, Config/Update State or State.

  From the Browse window, other operations, called Actions, can be performed on each element. Typical operations include View Element, Modify Element, Copy Element, and Delete Element. See Chapter 4, *Search and Browse*.
- **Configuration Management** — Use these operations to access tools for working with and managing key aspects of network element configurations, during the actual configuration process. See Chapter 11, *Network Configuration Management*.

3.2 Configure and Manage User Settings

In Pulse all operations for creating and managing network users, and defining access permissions to NMS operations are accessed from the NMS Management tab. These operations are grouped under the **User Management** and **User Credentials** sub-menus.

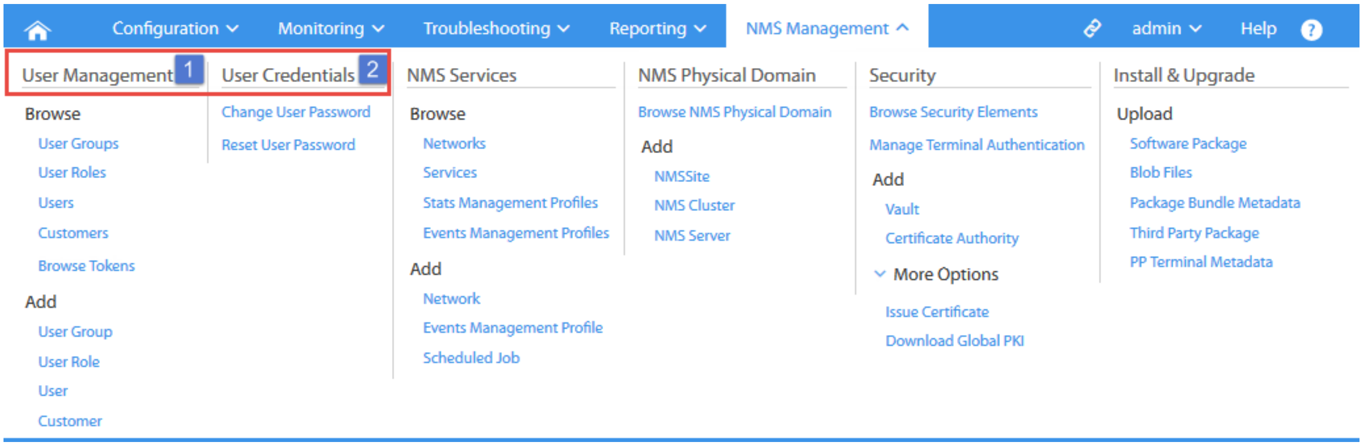


Figure 3-2. Pulse NMS Management — User Administration Menu Operations

The operations categories of the **NMS Management** User Administration sub-menus are briefly described as follows:

- **User Management** — User Groups, User Roles, User Accounts and Customers are created and managed from this sub-menu. Each user, whether an individual or external entity, via API, will require an authenticated user account prior to gaining access to the Pulse NMS.

  Using the operations of this sub-menu administrators can exercise precise control over the iDirect network elements and operations to which a user has visual or functional access. See Chapter 6, *Configuring & Managing User Settings*.

- **User Credentials** — From this sub-menu, user account credentials can be modified or reset by authorized users.

3.3 Configure and Manage System Settings

In addition to Pulse User Administration operations, the **NMS Management** menu also contains System Administration operations. The system settings and operations are accessed and managed under four sub-menus — **NMS Services**, **NMS Physical Domain**, **Security**, and **Installs & Upgrades**.

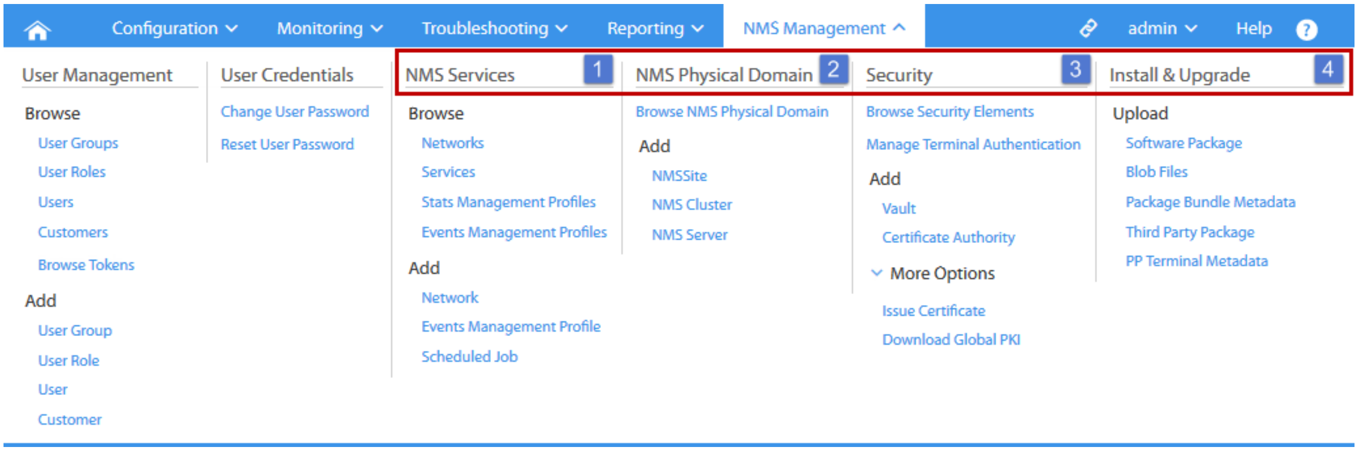


Figure 3-3. NMS Management — System Administration Menu Operations

The operations categories of the **NMS Management** System Administration sub-menus are briefly described as follows:

- **NMS Services** — These tools provide access to the various services that run on the NMS, and to the Pulse tools used to create the network elements associated with each of these services. See Chapter 8, *NMS Services & System Management*.
- **NMS Physical Domain** — Use these operations to add and configure the physical domain infrastructure that defines the Pulse Network Management System. NMS clusters are generally located a both the SAS and NOC sites. For procedures on how to configure the NMS site, cluster, and servers, see *Velocity Network Operations Using Pulse*.
- **Security** — These tools support creation and management of the tokens, certificates, and other elements that are applied to the various physical and logical infrastructure elements of the iDirect Network. See Chapter 9, *NMS Element Security Management*.
- **Install & Upgrade** — These tools support the various NMS tools associated with the management of the software components and versions that are installed on iDirect network elements. See Chapter 10, *NMS Software Installs & Upgrades*.

3.4 Pulse Network Monitoring Operations

Pulse NMS **Monitoring** menu operations, support a variety of operations that provide real-time access to iDirect Network Alarms, Events, and other information for both physical and logical network elements.

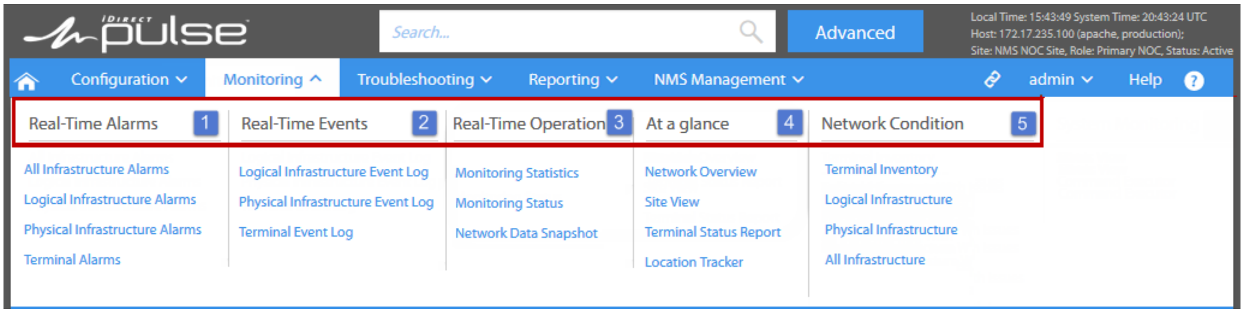


Figure 3-4. Pulse Monitoring Menu Operations

The operations of the **NMS Monitoring** tab are divided into five sub-menus. These operations categories are briefly described as follows: See Chapter 12, *Monitoring Operations*.

- **Real-Time Alarms** — These operations are used to automatically obtain a report of current network alarms based on the selected operation — for example, all alarms; all physical infrastructure alarms; a logical infrastructure elements; or all terminal alarms.
- **Real-Time Events** — These operations are used to automatically obtain a report of current network events for the selected object type — for example, all logical infrastructure events; all physical infrastructure events; or all terminal events.
- **Real-Time Operation** — With these tools you can monitor the real-time discrete status of any one or more elements, for example terminal Fan Status, current beam, or current channel; capture operational statistics of one or more elements, for example, total data volume transmitted, or total data volume received; and produce a Network Data Snapshot report of any one or more satellite terminals.
- **At a Glance** — These operations are used to access a variety of real-time snapshot views of the status of network infrastructure elements — for example from a complete network overview, a remote-side view, a hub-side view, or a location tracker view for terminals.
- **Network Condition** — These operations provide quick access point to shortcuts to browse listings of network infrastructure and terminal elements.

3.5 Pulse Network Reporting Operations

Pulse NMS **Reporting** supports user-customizable reports, using Report-Builder operations to access archived network information, as well as Pre-Defined Reports operations. Using the Configurator Panel, users can specify parameters like **Date Range**, **Elements**, **Metrics**, **Report Preferences**, as well as other key parameters, to generate Alarms or Events History Reports, Historical Statistics and Historical Status Reports.

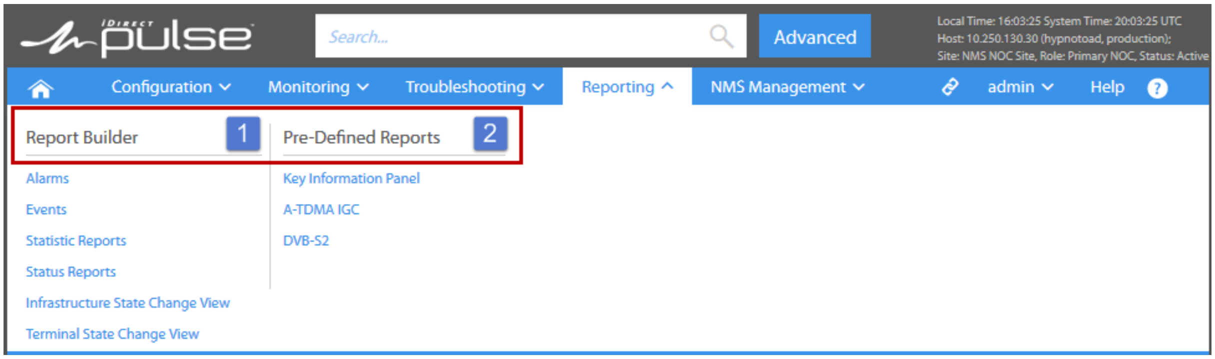


Figure 3-5. Pulse Reporting Menu Operations

Pulse Reporting operations support the following types of historical report requests:

- **Alarms** — Use this operation to manually specify Configurator settings such as Date Range, Elements, and Severity to return a customized history report of network alarms during a specified period. See *Generating an Alarms History Report*.
- **Events** — Use this operation to manually specify settings such as Date Range, Elements, and Severity to return a customized history report of network events during a specified period. See *Generating an Events History Report*.
- **Statistics Reports** — Manually specify settings to generate an historical statistics report for one or more elements based on specific metrics. For example, report IP traffic statistics for one or more terminals over a given period. See *Generating a Statistics History Report*.
- **Status Reports** — Use this operation to manually specify settings to generate an historical Status report for one or more elements, based on specific metrics. For example, report Falcon State or FLL Lock, for one or more line cards over a specified period. See *Generating a Status History Report*.
- **Infrastructure State Change View** — Obtain a change-of-state history report for one or more infrastructure elements over a specified period. These elements include hub-side components PP Cluster, PP Server, NMS Cluster, NMS Server, Line Card, and Chassis; and RF components, Satellite, Beam, Channel, iNet, Inroute Group, Downstream and Upstream Carrier. See *Infrastructure State Change Report*.
- **Terminal State Change View** — Obtain a change-of-state history report for any one or more satellite terminals during a specified period. See *Terminal State Change Report*.
- **Pre-Defined Reports** — In addition to the standard customizable history reports of the report Builder, several pre-defined reports that require minimal user input are available.

3.6 Troubleshooting and Diagnostics

Pulse Troubleshooting menu operations are briefly described as follows. For full details, see Chapter 15, *Troubleshooting Operations*.

- **Probe Commands** — Probe commands support real-time interaction with the operating system of iDirect Terminals, Line Cards, and Clusters. Each of these infrastructure elements support a set of commands that allow users, with permission, to access and manipulate specific operations or behaviors of the element.

  Probe commands also support access to configured Group Service Plans (GSPs), and to Subscriber Service Plan Components (SSPCs), to affect some specific aspect of these objects in the NMS.

- **Engineering Debug Console** — Using Engineering Debug Console users have direct access to a selected element, using a shell window for debugging purposes. Network elements that are accessible using this tool include Line Cards, Terminals, NMS and PP Servers, and the Chassis Controller.

4 Search and Browse

Browse and Search are two of the most used Pulse operations. The Browse operation is used to return a list of elements, found in the NMS, from any user-specified domain. These domains are the NMS elements associated with the physical and logical components of an iDirect network. As such, there are several browse operations — for example Browse Physical Domain, Browse Transport Domain, Browse Terminal Domain, and Browse Service Domain.

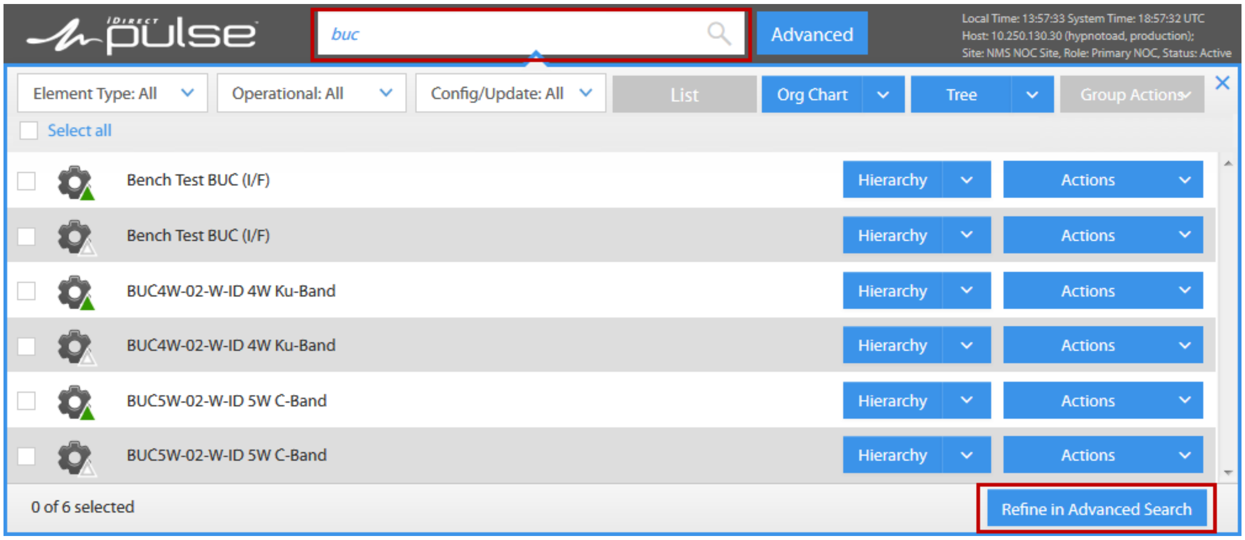
Search operations, on the other hand, fall into two categories — Basic Search and Advanced Search. Using these tools, you can use very simple or more advanced methods to search the entire NMS for any element.

Pulse search and browse operations are covered in the following topics.

4.1 Using the Basic Search

Using the *Basic Search* function, also called *global search*, users can perform a quick search throughout the NMS database for any element. The tool, which searches by **Element Name**, **Serial Number** or **IP address**, starts to list results after the first character is typed. The results are continually displayed and filtered as additional characters are typed.

After initiating a basic search, and a list of elements is returned in the results window, you may use one of three filters to make the list more manageable.



buc

Local Time: 13:57:33 System Time: 18:57:32 UTC
Host: 10.250.130.30 (hypnotoad, production);
Site: NMS NOC Site, Role: Primary NOC, Status: Active

☐ Bench Test BUC (I/F)
☐ Bench Test BUC (I/F)
☐ BUC4W-02-W-ID 4W Ku-Band
☐ BUC4W-02-W-ID 4W Ku-Band
☐ BUC5W-02-W-ID 5W C-Band
☐ BUC5W-02-W-ID 5W C-Band

0 of 6 selected

Figure 4-1. Basic Search Field and Results Window

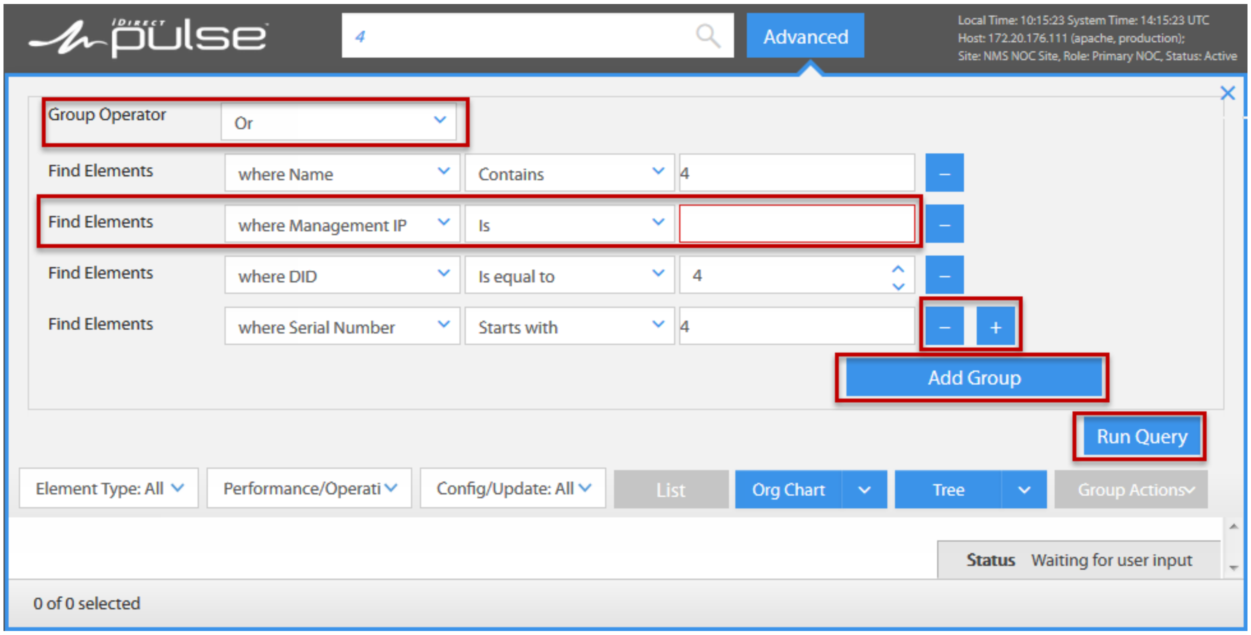
To search using the basic search field:

1. Start typing the name of the desired element in the **Search** field on the Pulse banner. A results list will start to appear based on the typed characters.
2. With the search results listed, select the desired element, if in view, or use one of the following filters to narrow the search results.
    a. Use the **Element Type** drop-down to display only the elements of a selected type.
    b. Use the **Operational** drop-down to only display elements currently in the selected operational state. For example — only elements that are **Online**.
    c. Use the **Config/Update** drop-down to only display elements currently in the selected configuration state. For example — only list elements that have **Changes Pending**.
3. Click the **Actions** button of an element to select an action to perform on the element — for example **View Terminal** or **Modify Terminal.**
4. Click the **Hierarchy** button to show the parent/child relationship of the element.
5. See *Using the Pulse Browse Operation* for additional details on working with elements listed in the Browse Results window or in the Search Results list.

4.2 Using the Advanced Search

Using the *Advanced Search* tool, users can construct a *custom query* to perform complex element searches throughout the NMS database. The query supports a combination of multiple search clauses. Each clause is composed of conditional attributes that refine the search criteria for finding an element. Query clause groups are combined using Boolean **AND/OR** operators to construct complex query logic for finding an element.

The **Advanced Search** tool is accessed directly, using the Advanced button on the Pulse banner, or by extending a search that was initiated using the **Basic Search** tool. When the basic tool is open, the search can be extended using the **Refine in Advanced Search** button.



Local Time: 10:15:23 System Time: 14:15:23 UTC
Host: 172.20.176.111 (apache, production);
Site: NMS NOC Site, Role: Primary NOC, Status: Active

Group Operator: Or
Find Elements: where Name | Contains | 4
Find Elements: where Management IP | Is |
Find Elements: where DID | Is equal to | 4
Find Elements: where Serial Number | Starts with | 4

Status: Waiting for user input
0 of 0 selected

Figure 4-2. Advanced Search Default Dialog

Components of the Advanced Search Dialog:

- A custom query is composed of one or more **Find Elements** clause groups
- A **Find Element** clause group is composed of one or more **Find Elements** clauses
- A Find Element clause is composed of the element search criteria and match criteria
- A query group is constructed of one or more clauses
- The **Group Operator** AND/OR specifies how clauses are to be logically combined
- The **+ sign** icon is used to insert additional clauses to a group
- The **- sign** icon is used to remove a clause from the group
- The **Add Group** button is used to insert an additional clause group
- The **Remove Group** button is used to remove a clause group from the query
- The **Run Query** button executes the defined query and generates the results

Use the following general guidelines to build a custom query:

1. Click the **Advanced** button on the Pulse banner to open the **Custom Query** dialog.
2. Specify the **Group Operator** setting as **OR**, or **AND**, to set how clauses should be combined.
3. Modify the default **Find Elements** clauses and match criteria, as required to define one or more search clauses. Remove Find Element clauses that are not required.
4. Click the **+ icon**, at the end of a clause, to insert an additional **Find Element** clause.
5. Click the **- icon**, at the end of a search clause, to remove the clause.
6. Click the **Add Group** button if a previous clause group is to be combined with an new group. Use the **Remove Group** button to delete a clause group.
7. Click **Run Query** to trigger the search after the query is defined.
8. After an initial element results list is returned, the list can be further filtered using the **Element Type** or the **Config/Update** drop-down.

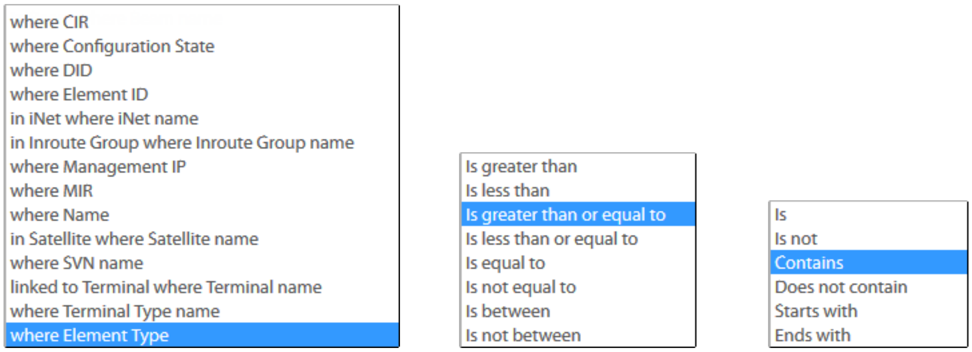


Figure 4-3. Numerical and Text Compare Condition Attributes

NOTE: The use of double quotes and other array syntax such as commas, braces, etc are not supported methods of searching in the global lookup or search box.

4.3 Using the Pulse Browse Operation

Using the appropriate Pulse browse command, a complete list of the configured elements for a given domain can be viewed. The elements found in the NMS are listed in the Browse Results window, in the default "**List View.**"

Once browse results are listed, users may find and select a specific element to work with or in some cases it may be necessary to perform a task simultaneously on multiple elements of the same type.

The following browse commands are available from the Pulse **Configuration** menus:

- **Browse Physical Domain** — View a list of configured physical elements such as NMS and PP cluster and servers, line cards, chassis, and other physical domain elements.

- **Browse Transport Domain** — View a list of configured logical infrastructure elements such as satellites, beams, channels, iNets and other transport domain elements.
- **Browse Network Domain** — View a list of configured network domain elements such as iNet Profiles and Inroute Group Profiles.
- **Browse Service Domain** — View a list of configured service elements such as Group Service Plans, Multicast Group Service Plans, and other service domain elements.
- **Browse Terminal Elements** — View a list of configured terminals and terminal service plan components.
- **Browse Terminal Components** — View a list of configured terminal components, such as ACUs, BUCS, LNBs, Satellite Routers, and Terminal Types.

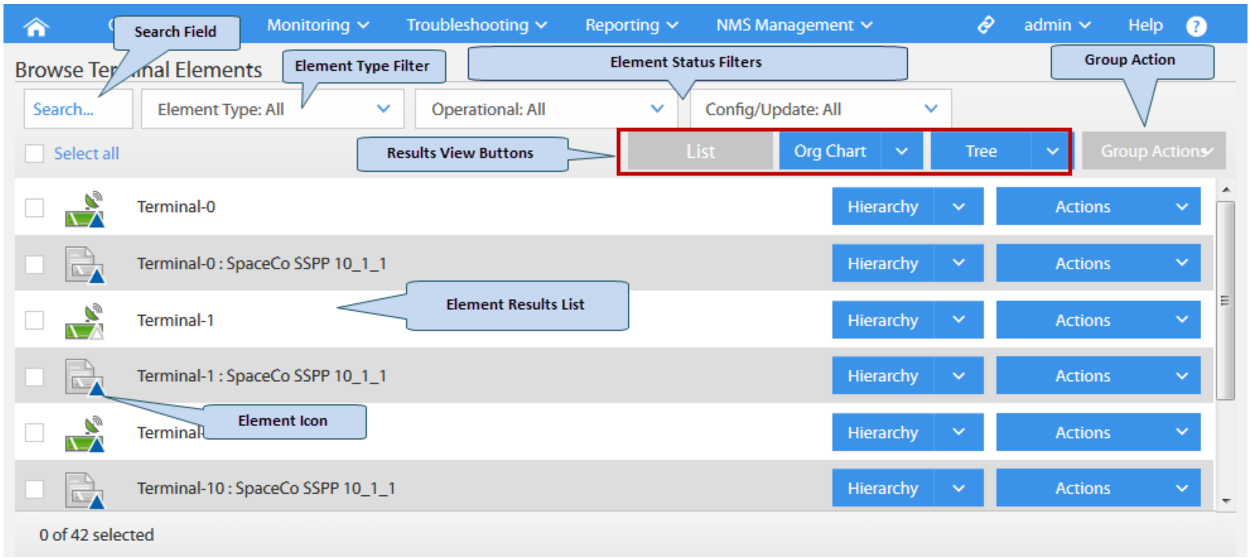


Figure 4-4. Browse/Search Results Window

To search using the basic search field:

1. From the **Configuration** tab or the **NMS Management** tab, choose the desired **Browse** command. A list of the elements found in the NMS, based on the command, is displayed.
2. With the browse results listed, select the desired element, if in view, or use one of the following additional filters to narrow the search results.
   a. Start typing the **Name** or **IP Address** of the desired element in the **Search** field.
   b. Use the **Element Type** drop-down to only display elements of a selected type.
   c. Use the **Operational** drop-down to only display elements currently in the selected operational state. For example — only **Online** elements.
   d. Use the **Config/Update** drop-down to only display elements currently in the selected configuration state. For example — only list elements that have **Changes Pending**.
3. Click the **Actions** button of an element to perform an action — for example **View Terminal**; or click any of the element buttons to apply the operation. For example, click **Alarm** to display the current alarms associated with the selected element.

4. See *Browse Window Search Filters and Buttons* for additional details on working with elements listed in the Browse Results window.

4.3.1 Browse Window Search Filters and Buttons

By default, the Pulse Browse Window displays the first 500 elements found in the NMS, based on the selected operation. You may need to filter the results in order to find a specific element. A brief description of the Browse Window search filters and buttons is provided.

Table 4-1. Browse Window Search Filters and Buttons

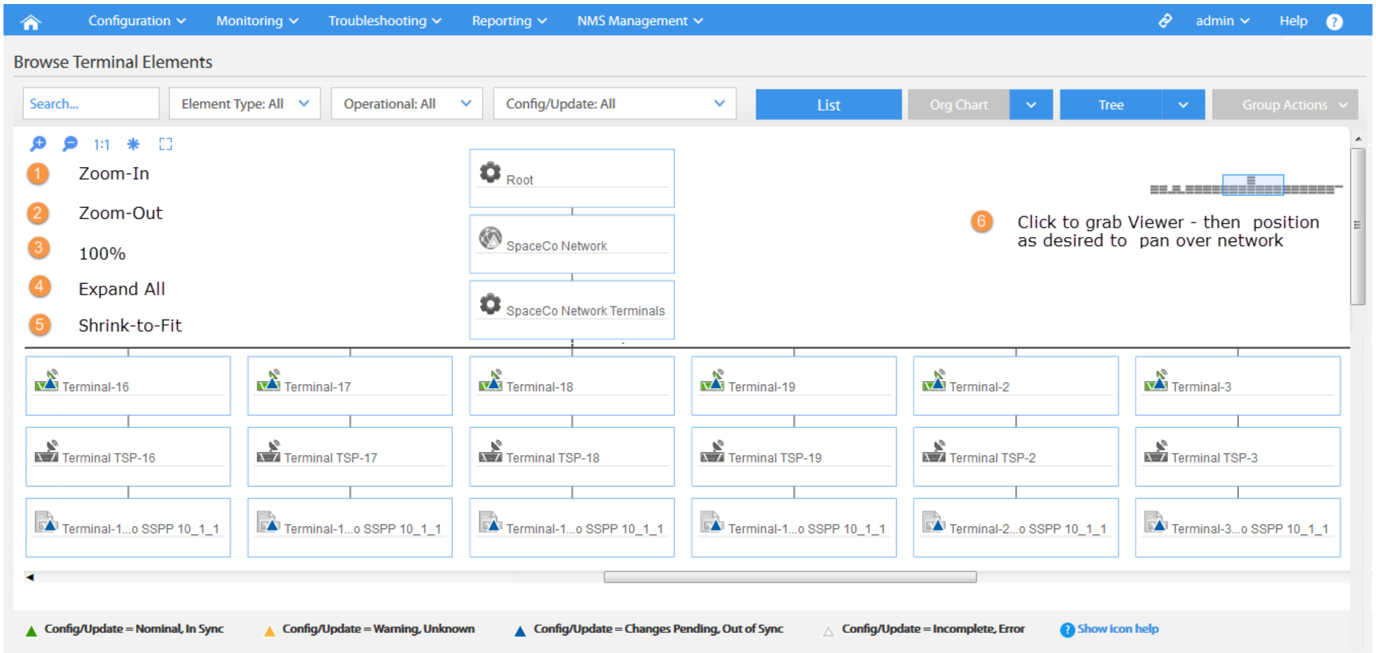
Page Element	Description
Search Field	Use to perform a quick search through the element results. The field, which supports a search by an Element Name, Serial Number or IP Address.
Element Type	Use drop-down options to filter the domain element list to a single element type. For example, filter the Transport domain for **Beams** or **Channels** only.
Operational Status Filter	Use to filter the results based on a selected operational status. For example, elements with status = **Online** only.
Select All Check Box	Click to select all of the listed elements.
Config/Update Filter	Use to filter element results based on the selected configuration or update manager status. For example, elements with **Incomplete** update status.
Element Icon	Click element icon to display current Config/Update status information, as well as other essential information about the selected element.
List Button	Display the element results in the standard list view. This is the default view of domain elements listed in the Browse Window.
Org Chart Button	Display an organization chart of the listed element domain, using a graphical view. Org Chart results can be displayed using the default graphical view, a dynamic view, or a physical tree view.
Tree Button	Display the currently listed element domain results in a tree view, which allows parent/child elements to be expanded/retracted to show/hide child elements.
Group Actions Button	Use to perform an action on selected items. For example **Edit Configuration**. (Active only if multiple elements of same type are selected.
Hierarchy Button	Displays hierarchy view of the selected element. The hierarchy starts with the root element, and shows any child elements.
Actions Button	Click to show a context-sensitive list of operations that can be performed on the selected element — for example, View element, or Copy element

4.4 Browse Results in Org Chart View

The *organization (Org) chart view* displays a more intuitive view of an entire element domain, for example the Physical Domain, by presenting a graphical hierarchy view of the elements as they are configured in the NMS.

The following are some key highlights of the organization chart view:

- view the relationship of domain elements in a graphical view that shows interconnections between domain elements - starting with the root node network.
- access the actions menu from within the Org Chart view, with the ability to invoke standard actions like add elements, and modify elements on any specific element.
- ability to zoom-in, zoom-out, and pan the organization chart.



① Zoom-In

② Zoom-Out

③ 100%

④ Expand All

⑤ Shrink-to-Fit

⑥ Click to grab Viewer - then position as desired to pan over network

Figure 4-5. Browse Window — Org Chart View

To view an Org Chart view of the domain, currently in the browse window, in its entirety:

1. Browse any element domain, for example, **Terminals**.
2. Without selecting any domain element in the Browse Window, click the **Org Chart** button to display an organization chart of all of the configured elements of the entire domain, starting with the root node network.
3. Use the five icons, positioned at the top left corner of the page, as follows:
   - **a.** No. 1 - click the zoom-in icon to increase the size of the chart.
   - **b.** No. 2 - click the zoom-out icon to decrease the size of the chart.
   - **c.** No. 3 - click the **1:1** icon to reset the chart size to 100%.
   - **d.** No. 4 - click the Expand-All Nodes icon to show all network nodes for entire domain.
   - **e.** No. 5 - click the shrink-to-fit icon **[ ]** to try to reduce the chart to fit a single page.
4. Click and grab the light blue transparent viewer element, No. 6, and position as desired to pan over a specific part of the Org Chart; or click on a specific node to refocus the chart to that position.
5. See *Browse Results in Tree View*, for more options when displaying the Org Chart.

4.5 Browse Results in Tree View

When results are listed in the Browse Window, clicking the “Tree” button displays the domain results in a hierarchical tree view, starting from the root node. This tree view is the same view seen when the **Hierarchy** button for a specific element is clicked. The difference is that the **Tree** button renders a tree view of the entire domain or of a filtered list of the domain.

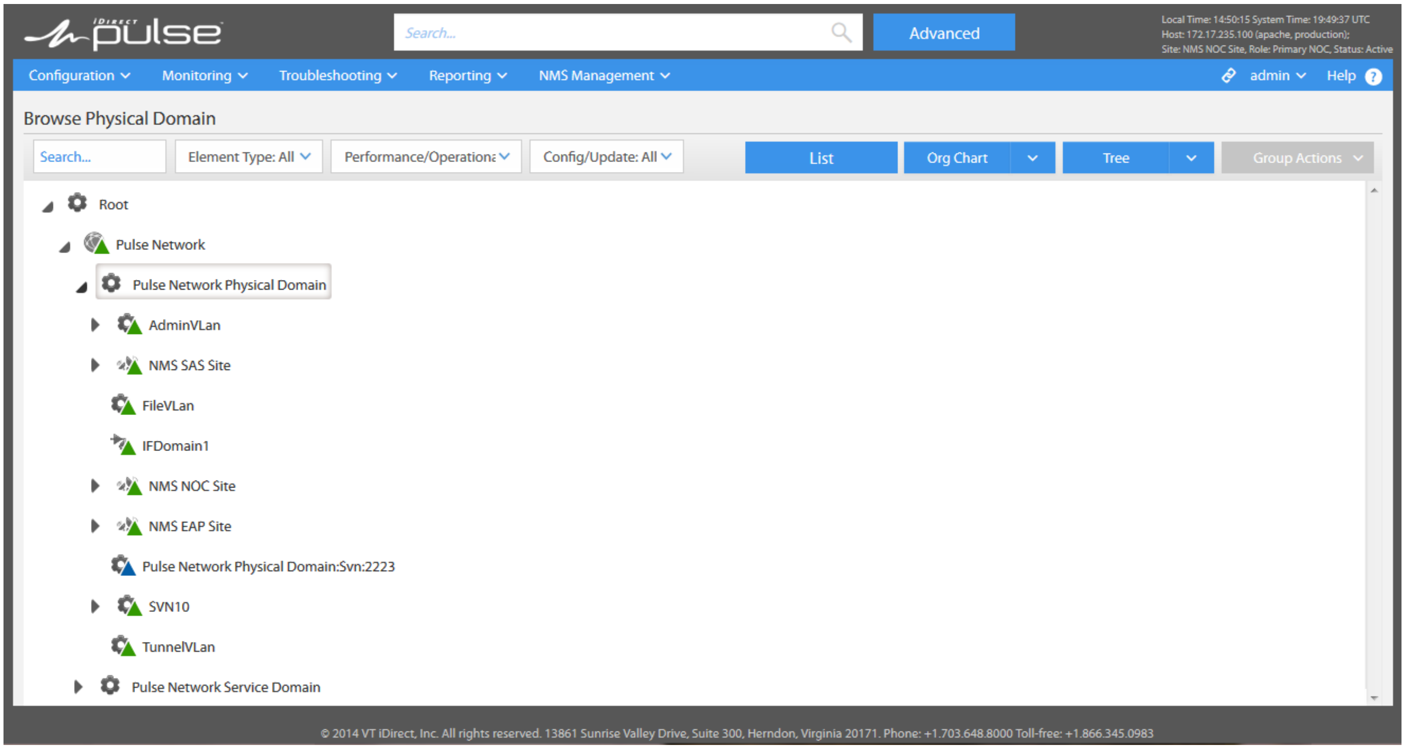

iDirect pulse
Search...
Advanced
Local Time: 14:50:15 System Time: 19:49:37 UTC
Host: 172.17.235.100 (apache, production);
Site: NMS NOC Site, Role: Primary NOC, Status: Active
Configuration
Monitoring
Troubleshooting
Reporting
NMS Management
admin
Help
Browse Physical Domain
Search...
Element Type: All
Performance/Operationa
Config/Update: All
List
Org Chart
Tree
Group Actions
Root
Pulse Network
Pulse Network Physical Domain
AdminVLan
NMS SAS Site
FileVLan
IFDomain1
NMS NOC Site
NMS EAP Site
Pulse Network Physical Domain:Svn:2223
SVN10
TunnelVLan
Pulse Network Service Domain
© 2014 VT iDirect, Inc. All rights reserved. 13861 Sunrise Valley Drive, Suite 300, Herndon, Virginia 20171. Phone: +1.703.648.8000 Toll-free: +1.866.345.0983

Figure 4-6. Browse Window — Tree View

The following are possible with the Tree View:

- view parent-child relationship of domain elements in a graphical view as opposed to the standard list view.
- view the entire domain or a filtered list.
- access the actions menu from within the Tree View, with the ability to invoke standard actions like add elements, and modify elements on any element.

To view an element domain, currently in the browse window, in tree view:

1. Browse any element domain, for example, the **Physical Domain**.
2. Click the **Tree** button to render a tree view of domain elements configured in the NMS.
3. See *Tree View Options*, for more options when displaying the Tree View.

4.5.1 Tree View Options

When elements are listed in the Browse window, the "tree view" options can be accessed using the **Tree** button or drop-down arrow, the **Org Chart** drop down button, or clicking the **Hierarchy** drop down for a selected element. These options are as follows:

- **Default Tree** — selecting this option renders the browse lists of elements as a "static" tree view list, where the list is inactive and only shows the hierarchical relationship of the selected element and its parent or child elements.

  Dynamic Tree — selecting this option renders the browse list of elements, as a "dynamic" tree view. The list is dynamic since the element icons in this view are active and can be used to access element Action commands such as Modify, Delete, and Apply Configuration. A full view of the element's Configuration History can also be opened.
- **Physical Tree** — selecting this tree view option renders the browse list of elements, in the default "static" tree view, while showing only the applicable physical elements.

5 The Configurator Panel

The *configurator panel* is a Pulse tool that assists operators with the tasks of generating various types of real-time and historical reports of iDirect network elements. In addition to monitoring and reporting operations, the Configurator assists operators with troubleshooting and diagnostic operations where the user must enter a set of required parameters.

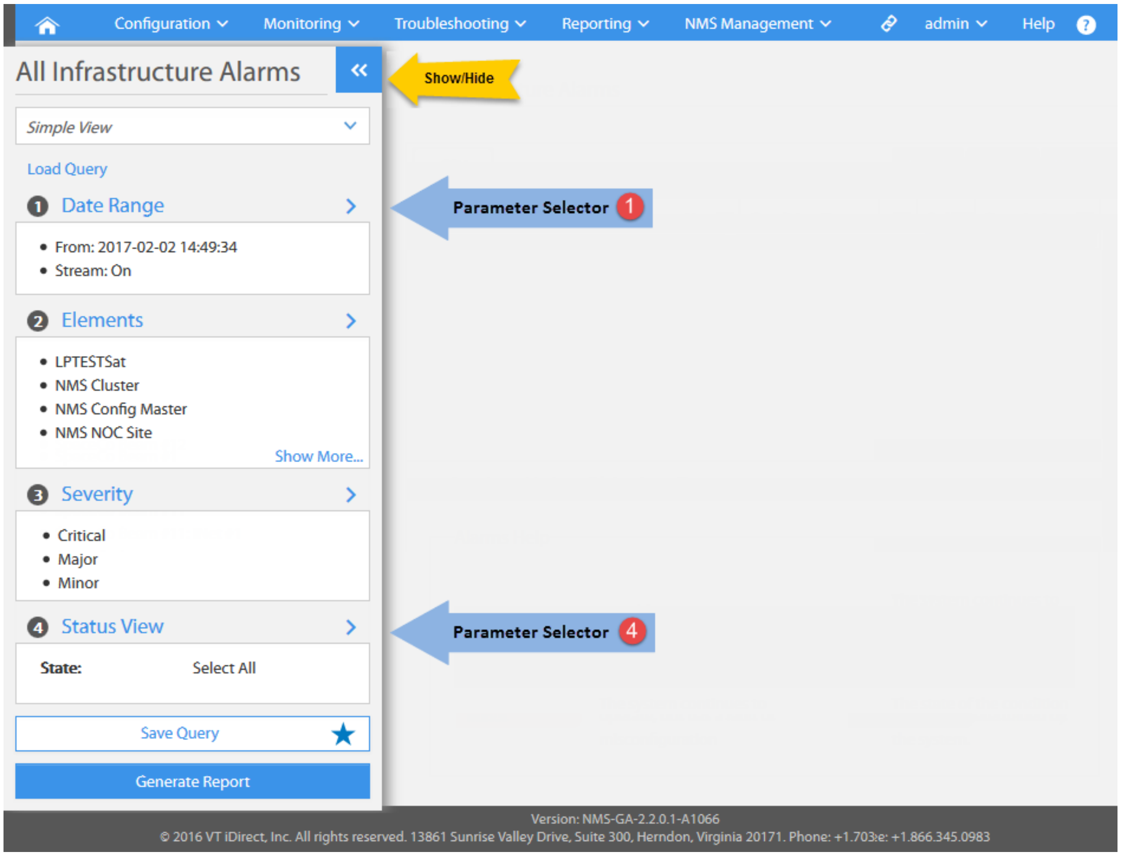
The Configurator components and operations are covered in the following topics:

5.1 About the Configurator Panel

The *configurator panel* assists users with generating real-time monitoring and historical reporting operations, as well as in performing troubleshooting and diagnostic operations. In using the Configurator, users must specify a set of parameters using context-sensitive fill-in-the blanks dialogs, and then trigger the operation. For the most part, Configurator operations, are accessed from Pulse **Monitoring**, **Reporting**, and **Troubleshooting** menus.

Each Configurator operation, when invoked, is opened with a set of numbered parameter selectors, many of which appear in most operations. Each selector, when clicked, opens the associated dialog, where user makes appropriate entries, and when done trigger the operation.

Once an operation is triggered, the requested report is generated and displayed to the right of the Configurator panel. The panel remains open, but can be hidden to allow a larger area for the report. The **Show/Hide** button toggles the panel between displayed and hidden.



- From: 2017-02-02 14:49:34
- Stream: On

- LPTESTSat
- NMS Cluster
- NMS Config Master
- NMS NOC Site

- Critical
- Major
- Minor

State: Select All

Version: NMS-GA-2.2.0.1-A1066
© 2016 VT iDirect, Inc. All rights reserved. 13861 Sunrise Valley Drive, Suite 300, Herndon, Virginia 20171. Phone: +1.703:e: +1.866.345.0983

Figure 5-1. Typical Form of Configurator Tool

NOTE: Whereas Pulse provides many useful pre-defined monitoring and reporting tools, the Configurator allows users to create and save their own customized real-time and historical reports for events, alarms, incidents, stats and statistics.

5.1.1 Configurator Use Title

When the Configurator is opened for a given operation, the title of the operation is displayed at the top of the panel. Some examples of other Configurator use titles are shown below.

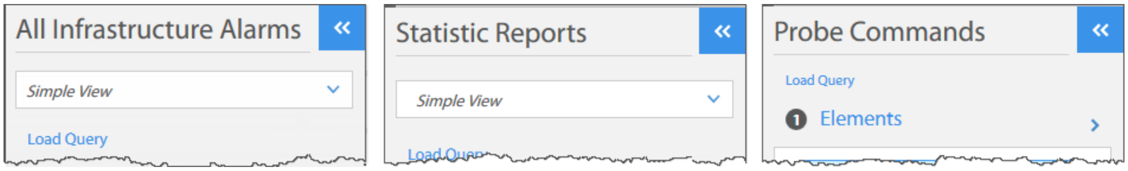
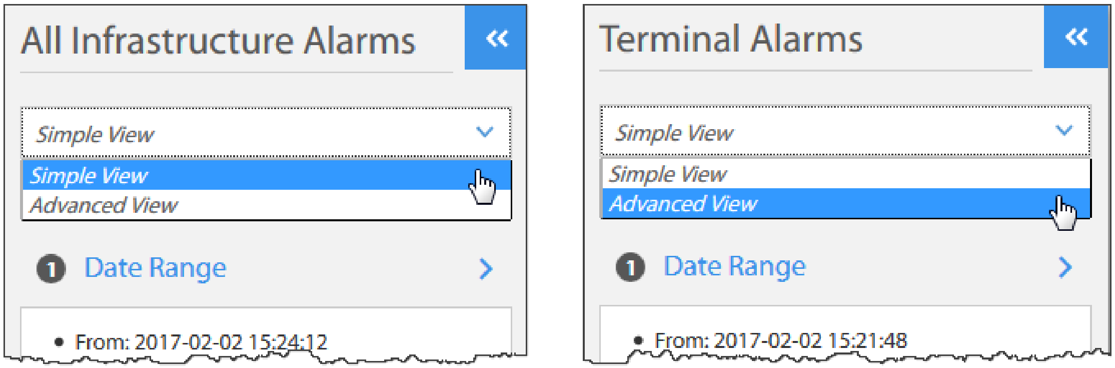


Figure 5-2. Configurator Use Titles Examples

5.1.2 Simple and Advanced View Options

Whenever the Configurator is opened, a default set of dialog options are available, and in some cases parameters are already preset based on the selected operation. These default dialog selections and settings are based on the Configurator default *simple view* option**.**

Alternatively, you may select the Configurator *advanced view*, which displays an extended set of dialog selectors, parameter fields, and attributes that are not shown in the simple view and can be applied to the operation. The advanced view offers greater granularity for setting parameters of the operation and thereby a greater control over the rendered output.



- From: 2017-02-02 15:24:12

- From: 2017-02-02 15:21:48

Figure 5-3. Configurator — Simple View or Advanced View Options

5.1.3 Save Query and Invoke Configurator Buttons

The last elements on the Configurator panel are generally a stack of two buttons. By clicking the **Save Query** button, which is displayed on all Configurator operations, you can save and name the parameter sets that are currently in the Configurator. See *Saving a Query*.

The second button, which triggers the operation, in most cases is the **Generate Report** button. Since the Configurator invokes non-report operations, the name of the button will vary depending on the operation. For example, the **Submit Probe Command** and the **Engineering Debug Console** are both **Troubleshooting** operations.

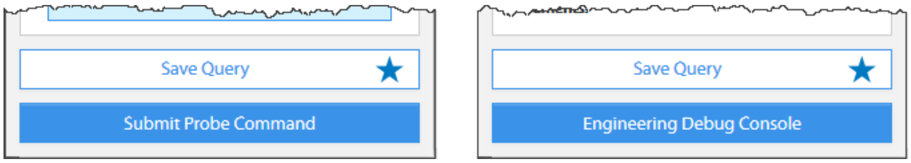
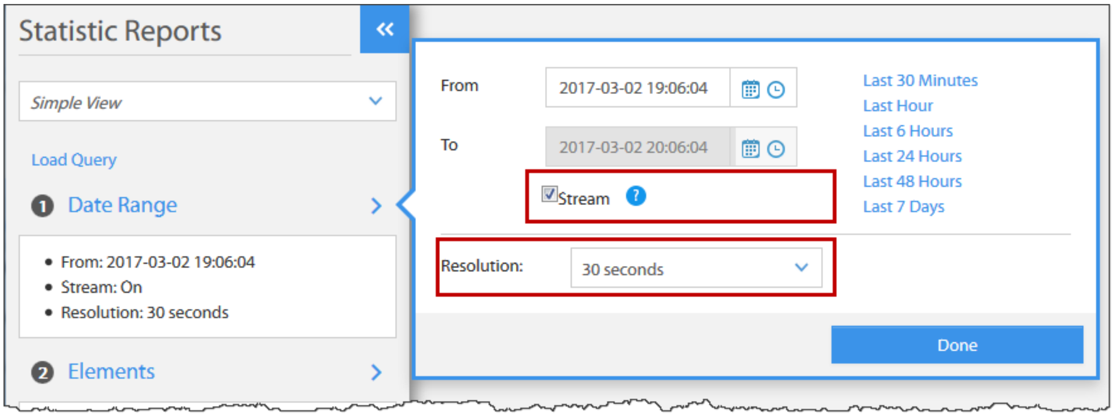


Figure 5-4. Configurator — Save Query and Generate Report Buttons

5.2 Date Range Selector

The **Date Range** selector is used in many Configurator operations to define a period for which data should be reported. The components of the dialog include a start date and time entry field; an end date and time entry field; a list of pre-defined periods for which the report can be captured — for example, **Last 30 Minutes**, **Last 24 Hours**, or **Last 7 Days**.

In some operations the dialog has a **Resolution** field that allows a sample frequency to be specified for capturing and displaying the data; and a **Stream** field that appears on some operations and can be enabled or disabled to display new report data as it occurs.



- From: 2017-03-02 19:06:04
- Stream: On
- Resolution: 30 seconds

From 2017-03-02 19:06:04
To 2017-03-02 20:06:04
☑ Stream
Resolution: 30 seconds

Figure 5-5. Configurator — Date Range Dialog

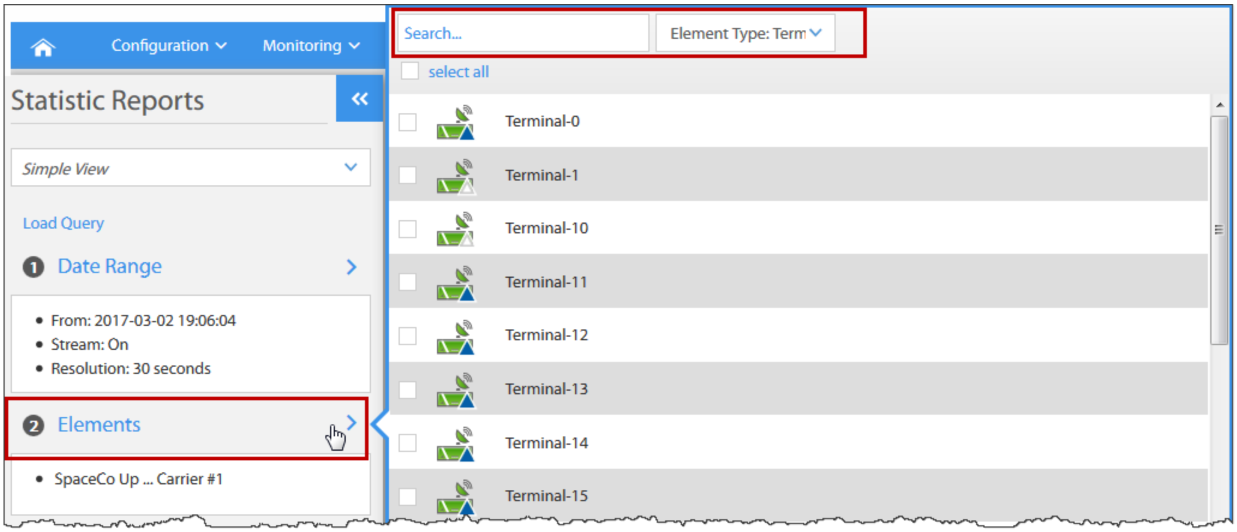
To enter the Date Range Parameters:

1. Click the **Date Range** selector, to open the **Select Date Range** dialog.

2. Use one or more of the following options to configure the **Select Date Range** dialog:
   - a. **From:** click the calendar icon to select a report start date; click the clock icon to select a report start time.
   - b. **To:** click the calendar icon to select a report end date; click the clock icon to select a report end time.
   - c. Click and select a pre-defined period for the report, instead of a start and end date.
   - d. **Resolution** (optional): use the drop-down to specify the resolution for collecting and displaying the report data — for example **1 minute** or **5 minutes**.
   - e. **Stream** (optional): select **Stream** to enable streaming of real-time data, which can be set to occur from a start date and time. If **Stream** is selected, the end date/time is disabled. Streaming begins with new data and continues until the report is closed.
3. Click **Add Date Range** to add the **Date Range** dialog parameters.

5.3 Elements Selector

Many of the Configurator **Monitoring**, **Reporting**, and **Troubleshooting** operations involve selecting one or more network elements for which the report should be based upon. These elements are specified from the **Elements** selector. Elements are found using the basic search tool and by filtering on certain criteria. A click on the **Elements** selector opens the search tool — and a second click closes the search tool.



- From: 2017-03-02 19:06:04
- Stream: On
- Resolution: 30 seconds

- SpaceCo Up ... Carrier #1

Figure 5-6. Configurator — Elements Selector

To select network elements:

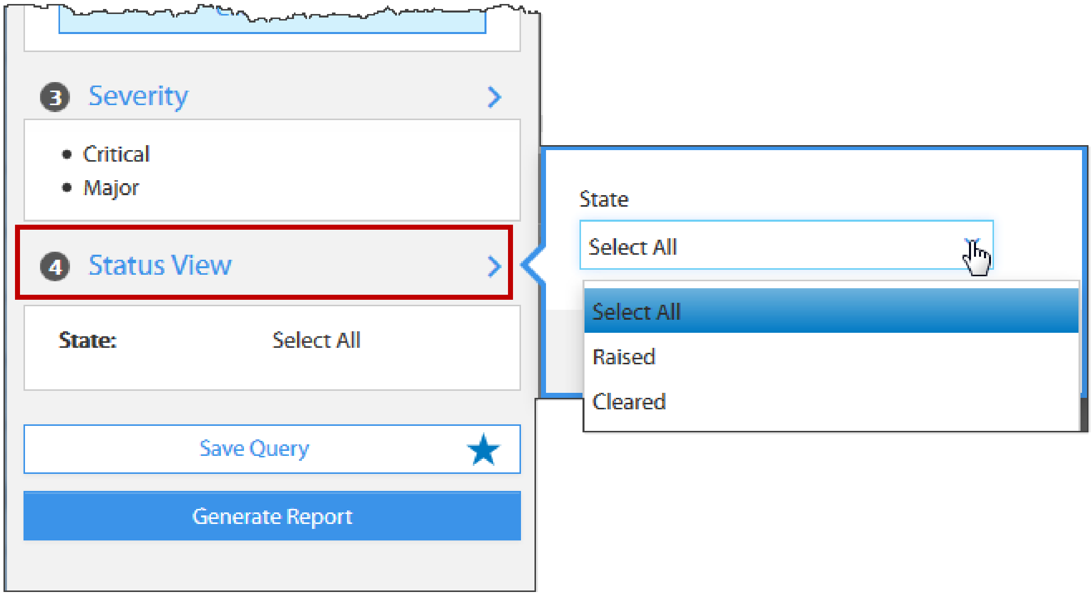
1. Click the **Element Selector** on the Configurator, to open the Basic Search tool.
2. Click in the **Search** field and start to type an **Element Name** or **IP Address**.
3. Select the desired element, if it is already displayed, or use one of the additional filtering methods to narrow the search results:
   a. Use the **Element Type** drop-down to select the type of element to list in the results — for example **Line Cards** only.
   b. Use the **Operational** drop-down list to list only elements currently in the selected operational state. For example — **Online** elements only.
   c. Use the **Config/Update** drop-down to list only elements currently in the selected configuration state. For example — only list elements that have **Changes Pending**.
4. Select a single element or select multiple elements; or click **Select All** to select all of the listed elements.
5. Click **Done** to add the selected elements to the Configurator.

5.4 Status View Selector

The **Status View** is the default on-screen display used for rendering a Pulse **Monitoring** or **Reporting** operation that involves network **Alarms**.

When an Alarm operation is invoked, the report rendering is based on default **Status View** preset parameters. For example, the **States** parameter is preset to the **Select All** option, to report all alarms in both the **Raised** and **Cleared** states. Other default Status View parameters are also preset, but can only be viewed by switching the Configurator to the Advanced View.

When the Configurator is in the Advanced View, all default Status View settings for Alarms reports can be viewed and modified. See *Modifying the Default Status View* on page 56.



State: Select All

Figure 5-7. Configurator Status View — Simple View Parameters Dialog

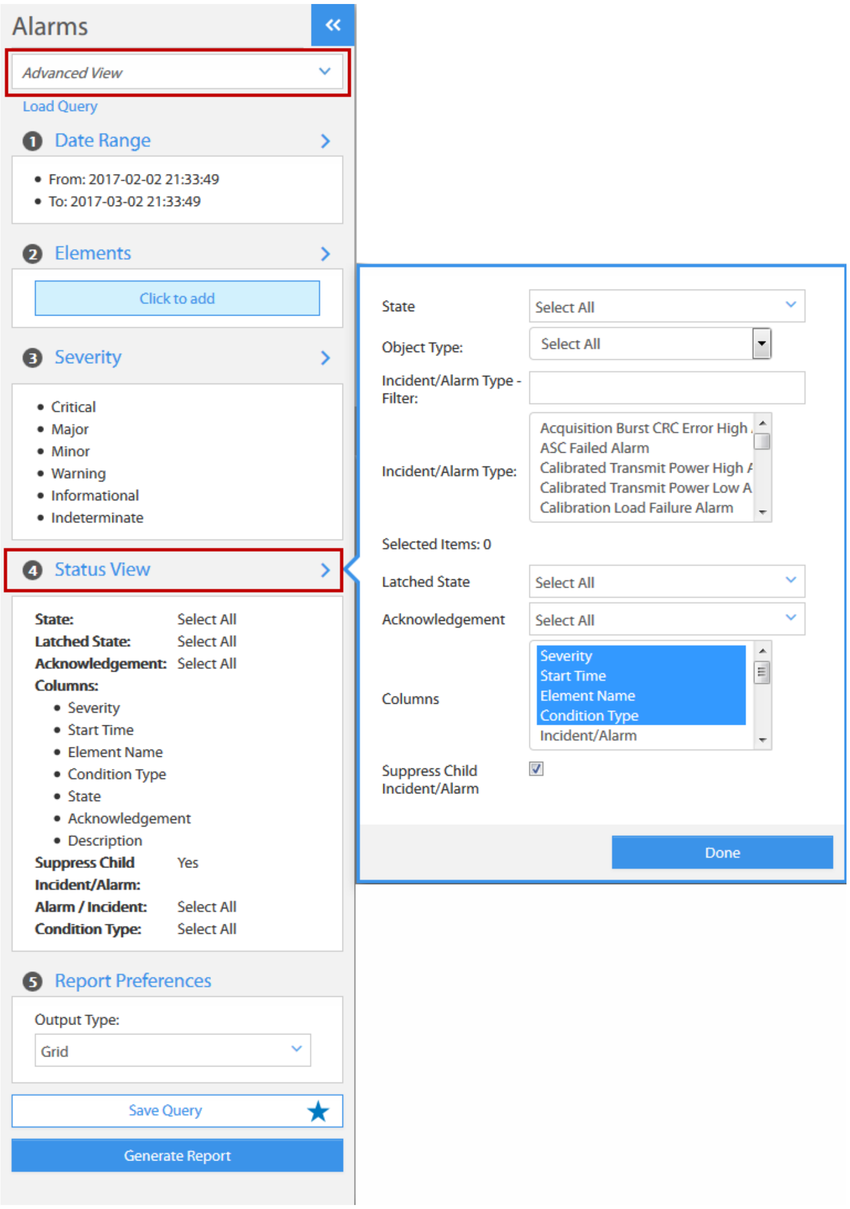
To select which Status View Alarm States to display in a monitoring/reporting operation:

1. Click **Status View** to open the **Alarm State** selection box and view the available alarm states that can be reported.
2. Select **Raised** to only list alarms that are still in the raised state; or select **Cleared** to only list alarms that have been automatically or manually cleared; or choose **Select All** to display both raised and cleared alarms.
3. Severity dialog settings also have default settings for the Status View. If required, click the **Severity** selector, to open and enable/disable any of the default severity levels settings. See *Severity Selector* on page 61.
4. Switch the Configurator to the **Advanced View** to make other changes to the Status View. See *Modifying the Default Status View* on page 56.
5. Click **Done** to add the modified **Alarm State** selections to the Configurator **Status View**.

5.4.1 Modifying the Default Status View

The initial on-screen display of any Alarms report is based on the default **Status View** dialog settings of the Configurator. Users with permission may modify the default settings, by first switching to the Configurator **Advanced View**, and then by modifying the Status View parameter field options for **State**, **Object Type**, **Incident/Alarm Type**, **Latch Type**, **Acknowledgment**, **Columns**, and **Suppress Child Incident/Alarm**.

Columns, for example, may be added or removed, or even dragged to a new location when the report is open.



- From: 2017-02-02 21:33:49
- To: 2017-03-02 21:33:49

- Critical
- Major
- Minor
- Warning
- Informational
- Indeterminate

State: Select All
Latched State: Select All
Acknowledgement: Select All
Columns:
- Severity
- Start Time
- Element Name
- Condition Type
- State
- Acknowledgement
- Description

Suppress Child Incident/Alarm: Yes
Alarm / Incident: Select All
Condition Type: Select All

Output Type: Grid

State: Select All
Object Type: Select All
Incident/Alarm Type - Filter:
Incident/Alarm Type:
Acquisition Burst CRC Error High
ASC Failed Alarm
Calibrated Transmit Power High A
Calibrated Transmit Power Low A
Calibration Load Failure Alarm
Selected Items: 0
Latched State: Select All
Acknowledgement: Select All
Columns:
Severity
Start Time
Element Name
Condition Type
Incident/Alarm
Suppress Child Incident/Alarm ☑

Figure 5-8. Configurator Advanced View — Status View Parameters Dialog

To modify the Configurator default status view:

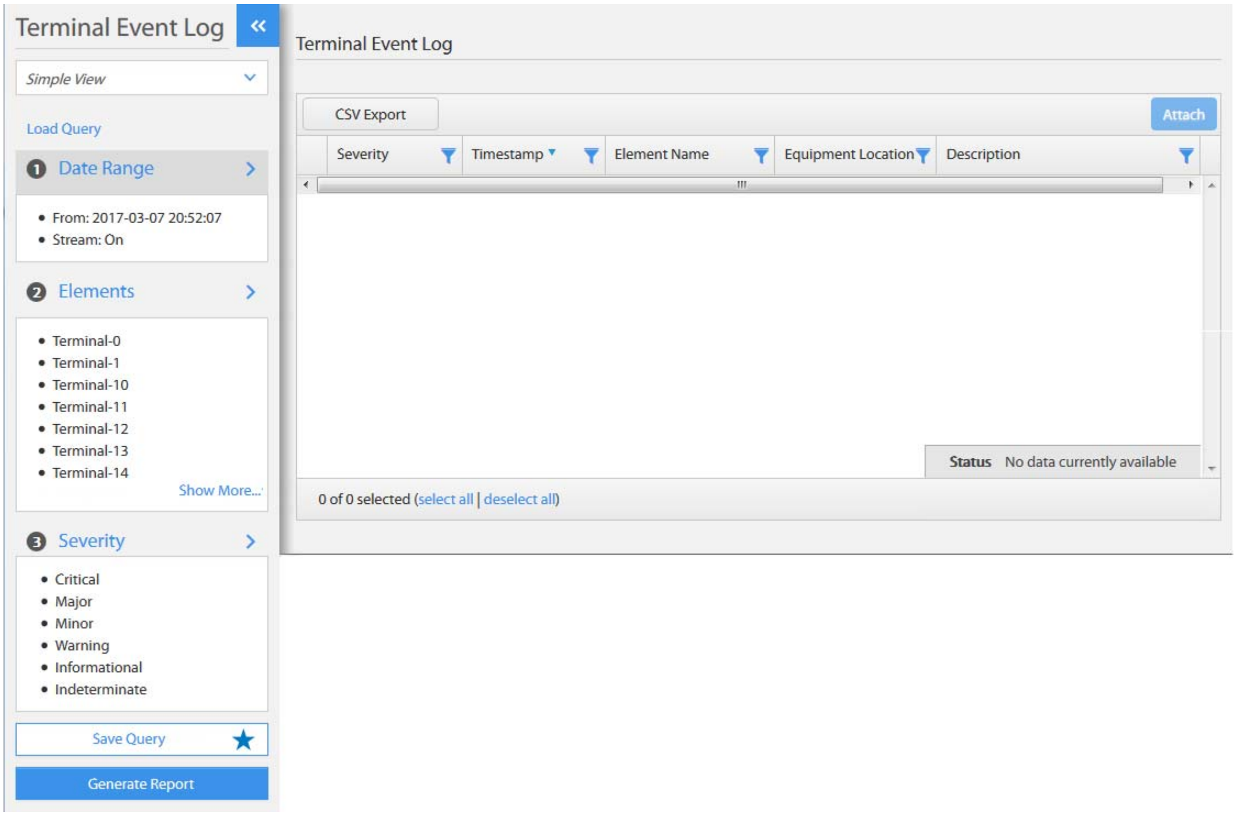
1. Open the Configurator to an Alarms operation.
2. Select **Advanced View** to enable the advanced Configurator options. By default, the **Simple View** is set, the **Status View** dialog is collapsed, and has default settings.
3. With **Advanced View** selected click the **Status View** options bar.
4. Modify the following parameters, as required, to change the **Status View** display options:
    a. **Alarm State:** choose **Raised**, to only show alarms that are still raised; choose **Cleared**, to only show alarms that have been automatically or manually cleared; and choose **Select All**, to show alarms that are still **Raised** and that have been **Cleared**.
    b. **Object Type:** choose **Alarm**, to only list alarms; choose **Incident** to only list incidents; and choose **Select All**, to show both **Alarms** and **Incidents**.
    c. **Incident/Alarm Type:** use the **Incident/Alarm Type Filter**, to limit the Incident/Alarm types that are displayed. Multiple incident/alarm types may be selected for the report.
    d. **Latch Type:** choose **Latched**, to show only alarms that are currently latched; choose **Unlatched**, to only list alarms that are currently unlatched; and choose **Non-latching**, to show alarms that have been configured as “non-latching alarms.”
    e. **Acknowledgment:** choose **Acknowledged**, to only show alarms that have been manually or automatically acknowledged; choose **Unacknowledged**, to only show alarms that have not been acknowledged; and choose **Select All**, to show both **Acknowledged** and **Unacknowledged** alarms.
    f. **Columns:** use this selection box to choose which columns to display. Multiple columns are individually selected by clicking the column while holding the **CTRL** key.
    g. **Suppress Child Incident/Alarm:** select this check box to suppress and not display any child incident/alarms associated with an incident or alarm.
5. The default Status view for alarms is also affected by the Configurator **Severity** settings. If required, click the **Severity** selector, to open and enable/disable any of the default severity levels settings. See *Severity Selector* on page 61.
6. Click **Done** to accept the modified **Status View** parameters. The modified parameters will take effect in the next report.
7. Click **Save Query** to store the configured parameters as a saved query with a name.

5.5 Log View Selector

The **Log View** is the default on-screen display used for rendering a **Monitoring** or **Reporting** operation that involves network Events.

When an **Event** operation is invoked, the report rendering is based on the default **Log View** preset parameters, and the Log View selector is not shown on the Configurator. The **Condition Type** parameter is set to **Select All**. This option causes events of all types to be reported; the **Columns** parameter is also preset to display a default set of columns that include Severity, Timestamp, Element Name, Equipment Location, and Description.

When the Configurator is in the Advanced View, all default Log View settings for Events reports can be viewed and modified. See *Modifying the Default Log View* on page 59.



Date Range
- From: 2017-03-07 20:52:07
- Stream: On

Elements
- Terminal-0
- Terminal-1
- Terminal-10
- Terminal-11
- Terminal-12
- Terminal-13
- Terminal-14

Severity
- Critical
- Major
- Minor
- Warning
- Informational
- Indeterminate

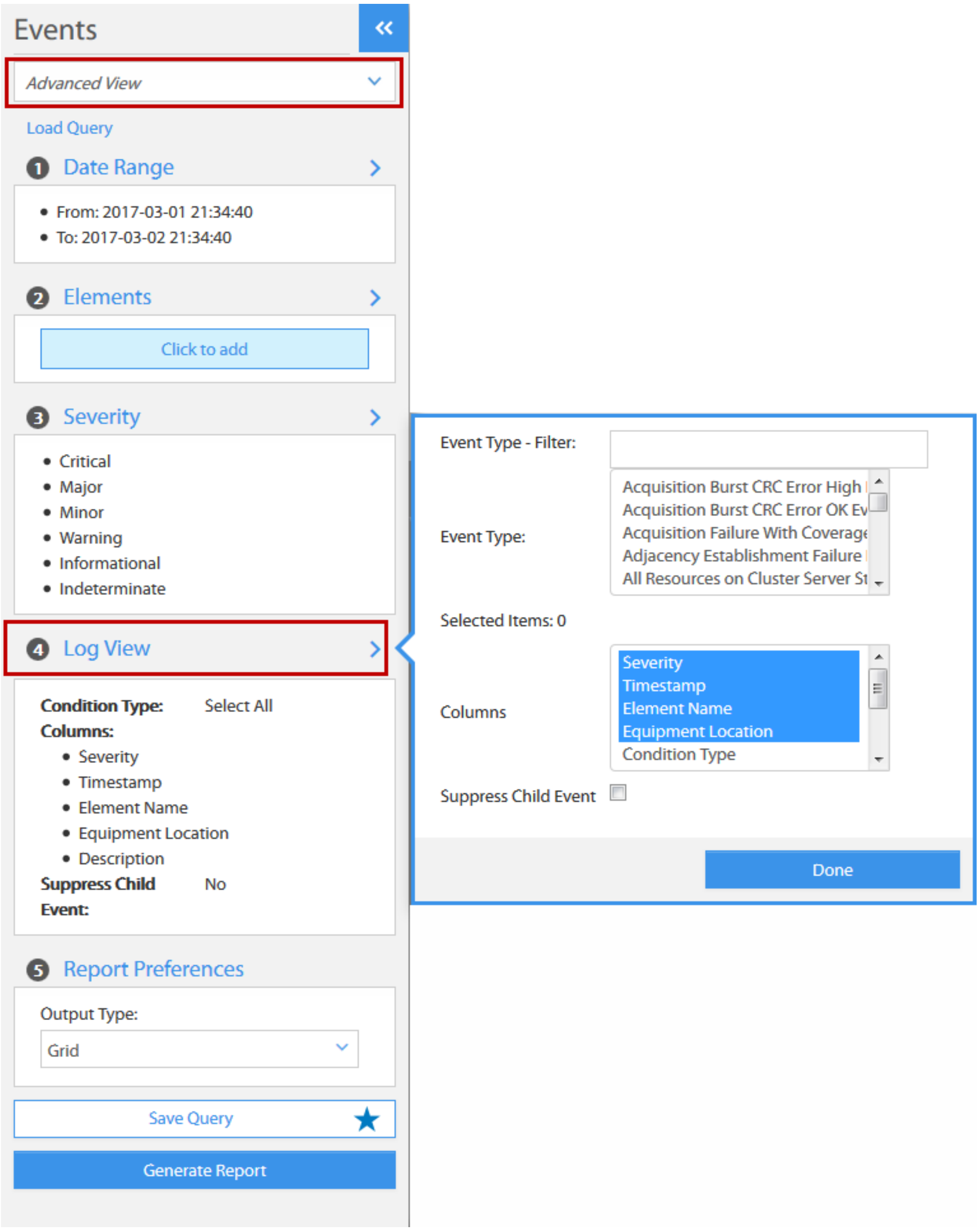
Status No data currently available

0 of 0 selected (select all | deselect all)

Figure 5-9. Configurator Log View Default

5.5.1 Modifying the Default Log View

The initial on-screen display of any Events report is based on the default **Log View** dialog settings of the Configurator. Users with permissions may modify the default settings, by first switching to the Configurator **Advanced View**, and then by modifying the Log View options for **Event Type**, **Columns**, and **Suppress Child Event** parameter fields. Columns, for example, may be added or removed, or even dragged to a new location when the report is open.



Events

Advanced View

Load Query

1 Date Range

- From: 2017-03-01 21:34:40
- To: 2017-03-02 21:34:40

2 Elements

Click to add

3 Severity

- Critical
- Major
- Minor
- Warning
- Informational
- Indeterminate

4 Log View

Condition Type: Select All
Columns:
- Severity
- Timestamp
- Element Name
- Equipment Location
- Description

Suppress Child Event: No

5 Report Preferences

Output Type: Grid

Save Query

Generate Report

Event Type - Filter:

Event Type:
Acquisition Burst CRC Error High
Acquisition Burst CRC Error OK Ev
Acquisition Failure With Coverage
Adjacency Establishment Failure
All Resources on Cluster Server St

Selected Items: 0

Columns
Severity
Timestamp
Element Name
Equipment Location
Condition Type

Suppress Child Event ☐

Done

Figure 5-10. Configurator Advanced View — Log View Parameters Dialog

To modify the Configurator default log view:

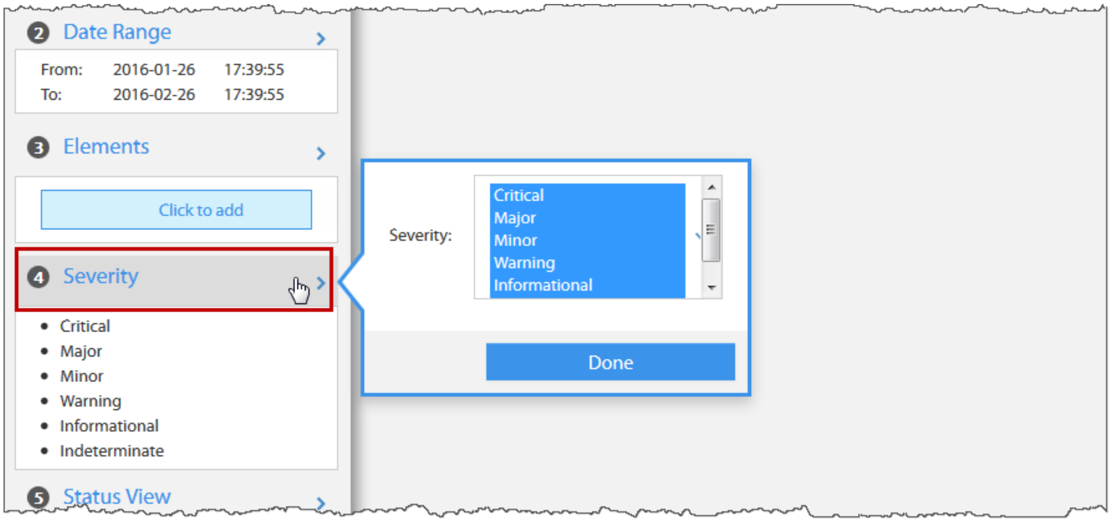
1. Open the Configurator to an Events operation.
2. Select **Advanced View** to enable the advanced Configurator options. By default, the **Simple View** is selected, the **Log View** dialog is collapsed, and has default settings.
3. With **Advanced View** selected click the **Log View** options bar.
4. Modify the following parameters as required to change the **Log View** monitoring display:
    a. **Event Type Filter:** use to filter the objects listed in the **Event Type** box.
    b. **Event Type:** select one or more event types to display in the report. Multiple event types may be selected.
    c. **Columns:** use this selection box to choose which columns to display in the report. Multiple columns may be selected.
    d. **Suppress Child Event:** select this check box to suppress and not display any child events associated with an event.
5. The default Log view for events reports is also affected by the Configurator **Severity** settings. If required, click the **Severity** selector, to open and enable/disable any of the default severity levels settings. See *Severity Selector* on page 61.
6. Click **Done** to accept the modified **Log View** parameters. The modified parameters will take effect in the next events report.
7. Click **Save Query** to store the configured parameters as a saved query with a name.

5.6 Severity Selector

Using the **Severity** selector, users may specify which network Alarms or Events should be reported on a **Monitoring** or **Reporting** report, based on severity.

The NMS classifies network and system related Alarms and Events in terms of **Severity** levels. In order of significance these levels include **Critical**, **Major**, **Minor**, **Warning**, **Informational**, and **Indeterminate.**

By default, the Configurator is preset with the Severity set to **Select All**, to include all severity levels in any report. This setting may be changed. A single level or any number or all of the severity levels may be selected.



From: 2016-01-26 17:39:55
To: 2016-02-26 17:39:55

- Critical
- Major
- Minor
- Warning
- Informational
- Indeterminate

Severity: Critical, Major, Minor, Warning, Informational

Figure 5-11. Configurator — Severity Selector

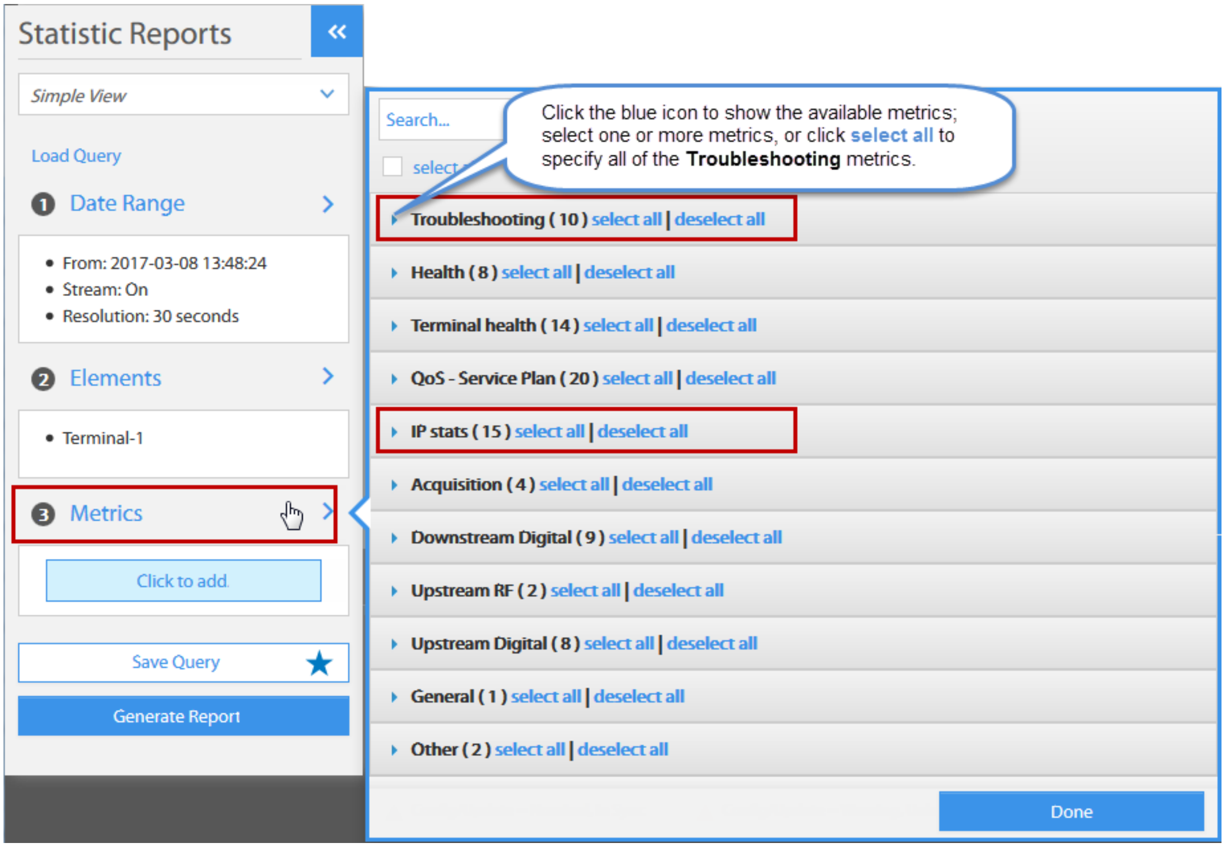
To select severity levels to display:

1. Click the **Severity** selector to open the **Severity** selection pane.
2. Select a single severity level or select multiple severity levels from the **Severity** pane.
3. Click **Done** to specify and add the selected **Severity** levels to the Configurator.

5.7 Metrics Settings

Using the *metrics* selector, you can select specific metrics when configuring a Status or Statistics report for selected elements. When configuring a Status report for line cards — for example, the selected metrics are based on state change and might include **board temperature** or **buffer overflow**. When the basic search dialog is opened, a context-sensitive list of metrics is listed, based on the currently selected element type.

If different elements types are selected for the report, the context-sensitive list of metrics will only include those metrics that the elements have in common.



- From: 2017-03-08 13:48:24
- Stream: On
- Resolution: 30 seconds

- Terminal-1

Click the blue icon to show the available metrics; select one or more metrics, or click **select all** to specify all of the **Troubleshooting** metrics.

- Troubleshooting (10) select all | deselect all
- Health (8) select all | deselect all
- Terminal health (14) select all | deselect all
- QoS - Service Plan (20) select all | deselect all
- IP stats (15) select all | deselect all
- Acquisition (4) select all | deselect all
- Downstream Digital (9) select all | deselect all
- Upstream RF (2) select all | deselect all
- Upstream Digital (8) select all | deselect all
- General (1) select all | deselect all
- Other (2) select all | deselect all

Figure 5-12. Configurator — Metrics Selector

To select the level of severity upon which to base the report:

1. Click **Metrics** to open the Basic Search window to a list of metrics based on the selected elements — for example terminal metrics. The listed metrics are grouped, by type, based on the metrics name.
2. Click the blue icon adjacent to a metric group to show the metrics within that group. Select one or metrics from the group, or click **Select All** to specify the metrics to be used in the report. The total number of selected metrics may be limited in some cases.
3. Click **Done** to add the selected metrics to the Configurator.

5.8 Saving a Query

A set of Configurator parameters, once set, can be saved under a specific name using the **Save Query** button. The query is saved to the current user profile. Saving Configurator settings that have been used successfully avoids trial and error attempts at a specific configuration. Later, recalling and loading a query is a convenience that saves considerable time, avoids tedious re-entry of parameters, and ensures the desired results. See *Loading a Saved Query*.

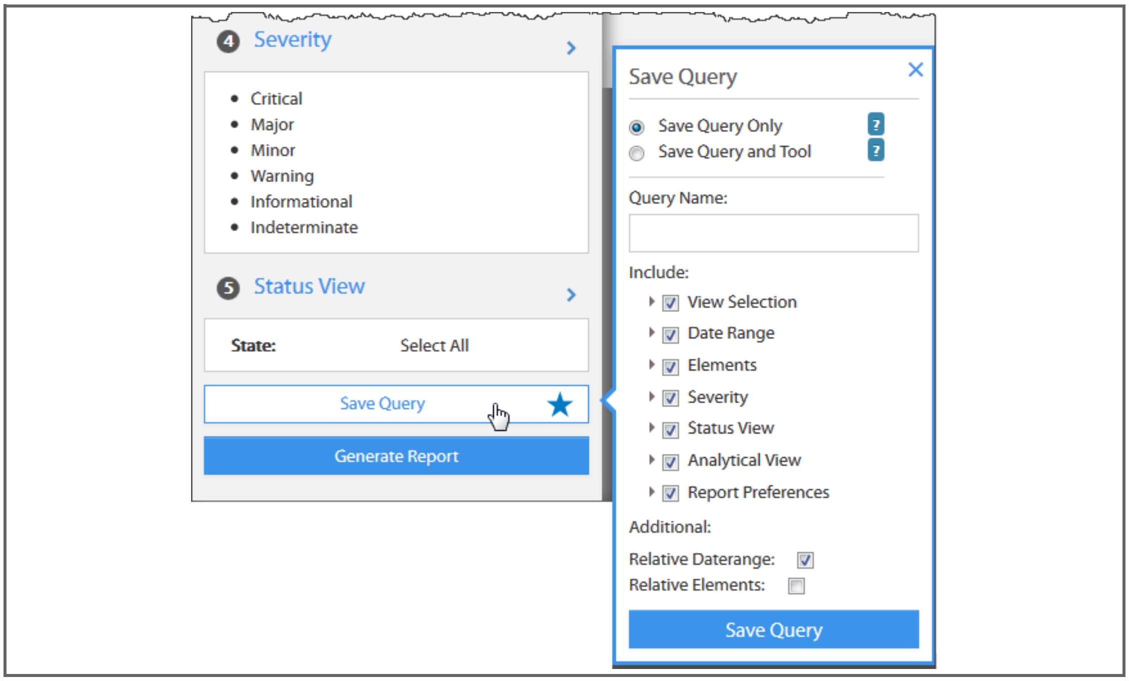


Figure 5-13. Configurator — Save Query

To save a query:

1. Click **Save Query** after entering the desired parameters in the Configurator panel. A **Save Query** dialog opens. The dialog and parameters are based on the operation.
2. Select **Save Query Only**, dialog option, in order to reuse a query with a different tool or from anywhere within Pulse; or select the **Save Query and Tool** option, if the query will be used to recreate the exact report, and will be used from the Configurator.
3. Type a **Query Name** to assign to the query.
4. Under **Include**, click and check or uncheck each check box in order to include or exclude the associated query field and attributes in the saved query. Note that each query field can be expanded to show additional associated attributes that may be included or excluded from the report.
5. Uncheck any check box for which the query field and/or attributes should be excluded.
6. Click **Save Query**.

5.9 Loading a Saved Query

The **Load Query** link is displayed at the top of every Configurator operation. Clicking the link displays a list of previously saved queries that are available to the user. Each query is listed by name and will contain a list of parameters that can be loaded to the Configurator panel.

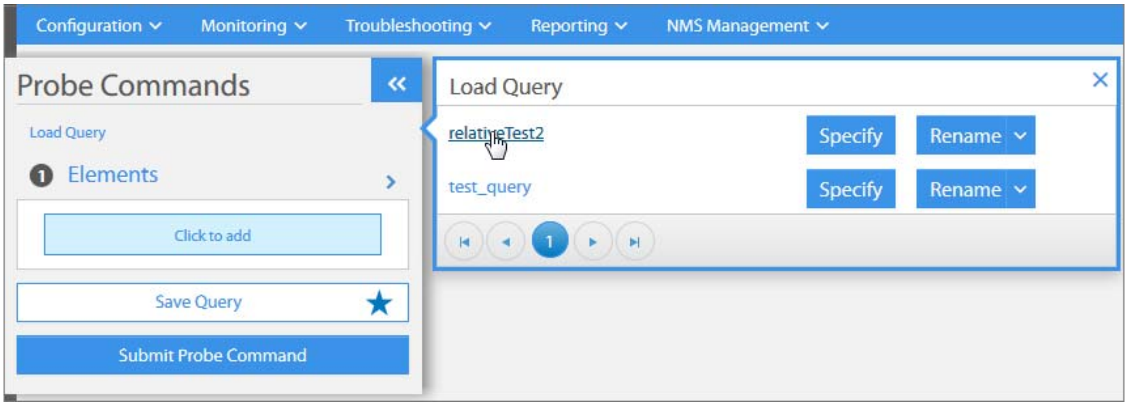


Figure 5-14. Configurator — Load Query Dialog

To load a saved query without any changes to the presets:

1. Click the **Load Query** button on the current Configurator tool dialog.
2. If necessary, use the next and previous navigator buttons to traverse through a list of queries to find a specific query to load.
3. Click on the query name to select the query, as it is, without making any changes to the presets. The Configurator presets are loaded in their entirety just as they were saved.
4. Once the query is loaded click the button to trigger the operation.

To load a saved query after first making some changes to the presets:

1. Click the **Load Query** button on the current Configurator tool dialog.
2. If necessary, use the next and previous navigator buttons to traverse through a list of queries; then with the desired query in view, click the **Specify** button to open the **Specify Presets** dialog.
3. With the **Specify Presets** dialog open click the **Expand** icon, to the left of a Configurator presets section, to view all of the presets.
4. Use the preset check boxes to enable/disable presets as desired.
5. Click the **Load Presets as Specified** button after making the required changes. The presets, with changes, are loaded to the Configurator.
6. Click the button to trigger the operation based on the modified presets.

To rename or delete a saved query:

1. Click the **Load Query** icon to display the **Load Query** dialog.
2. If necessary, use the next and previous buttons to traverse through the list of queries.

3. Click the **Rename** drop-down on the desired query. The **Rename** and **Delete** options are displayed. Use one of the following procedures:
    a. Click **Rename** to enable renaming of the query. Rename the query as desired, and press the **Enter** key to save the renamed query.
    b. Click **Delete** and when prompted respond with '**Yes'** to remove the saved query from the user profile.

6 Configuring & Managing User Settings

Before access to the NMS is granted to an individual using the Pulse Web interface or to an external system using the Web Service API, appropriate user credentials must be established.

The Pulse User Administration Domain supports a rich set of tools for defining, configuring, and managing user access and operations permissions in iDirect networks. These tools are accessed from the **NMS Management** tab, under the **User Management** and **User Credentials** sub-menus. Using these tools and operations authorized administrators can exercise precise control over the elements and operations to which a user has visual or functional access.

Configuring and managing user settings are covered in the following topics:

- *About User Groups, Roles, and Users* on page 68
- *Creating User Groups* on page 69
- *Creating User Roles* on page 70
- *Creating User Accounts* on page 72
- *Creating a New Customer Record* on page 75
- *User Account Management* on page 76
- *Creating and Managing Tokens* on page 80
- *User Administration Browse Actions* on page 83

6.1 About User Groups, Roles, and Users

What a user can see in Pulse and specifically what a user can do, with respect to network elements, is determined in conjunction, by the assignment of user groups and user roles to individual user accounts. In other words, groups and roles determine a user's level of access to network elements — access defines what a user can see and what actions are possible.

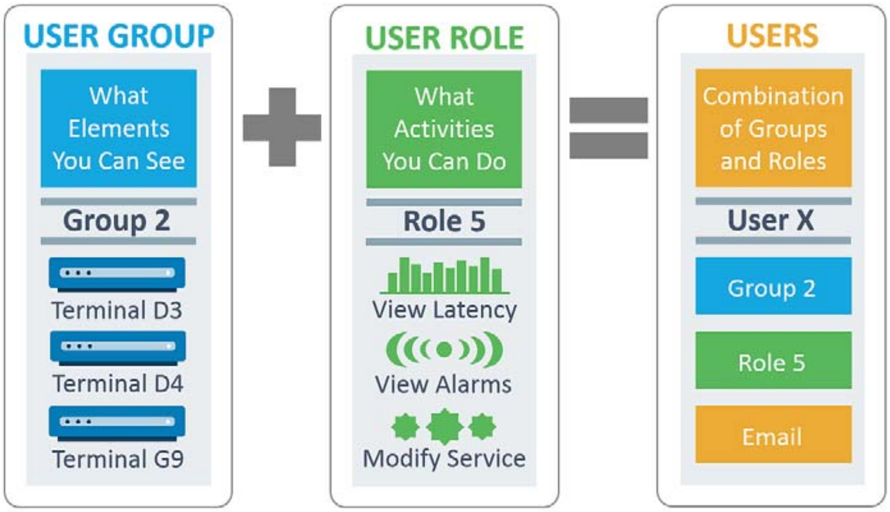


Figure 6-1. User Groups - Roles - Users

Each user group, when created, will contain a group of elements to which *Own Access*, *Read Access*, or *Write Access* is assigned to each element of the group. The access level assigned to the element is eventually inherited by the user when the user group is assigned to the user. Since access begins with the elements of the group, this access can be from including terminals only, to including all other network elements. And the access could be limited to viewing only or owning the element, which allows viewing, modifying, and deleting.

Similarly, user roles defined in the NMS specify a particular set of activities or functions that can be performed in the NMS. Later, by assigning a specific role to a user account, the user then inherits the ability to perform the activities defined by the user role, including adding new network elements. Once user groups and user roles are assigned to a user, it is determined exactly the elements to which a user has access (visibility) and what activities or functions the user can perform.

Table 6-1. Token Parameters

Element Access Permission	Brief Description
Read	Grants view access only; view access to child element is inherited.
Write	Grants view, create, and modify access to element; access to element child items is inherited.
Own	Grants full access to element (view, create, modify, and delete) and child elements.

6.2 Creating User Groups

A *user group* defines a group of logical or physical elements, whereby each element of the group is assigned level of access. Later, by assigning the group to a user, the user inherits permission to access the elements of the group at the defined access level.

As user accounts are defined, any one or more user groups can be assigned to the user. Group membership, as such, manages user access to the NMS, and prevents users from gaining access or visibility outside of what has been assigned by the group element permissions.

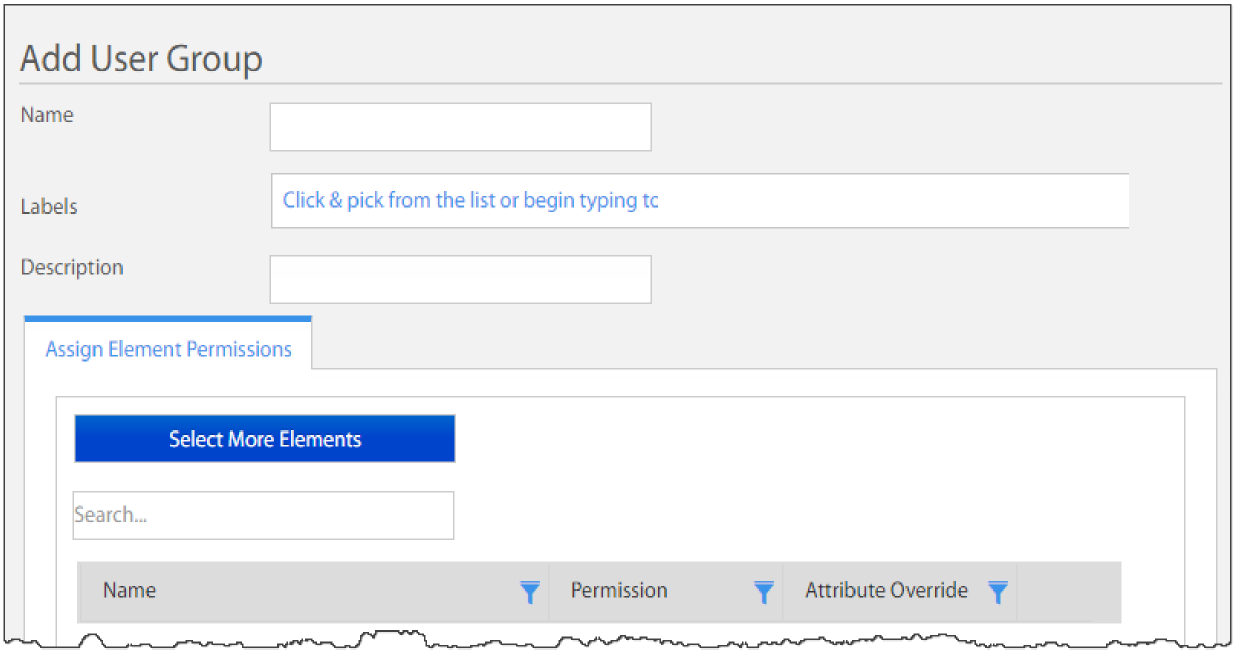
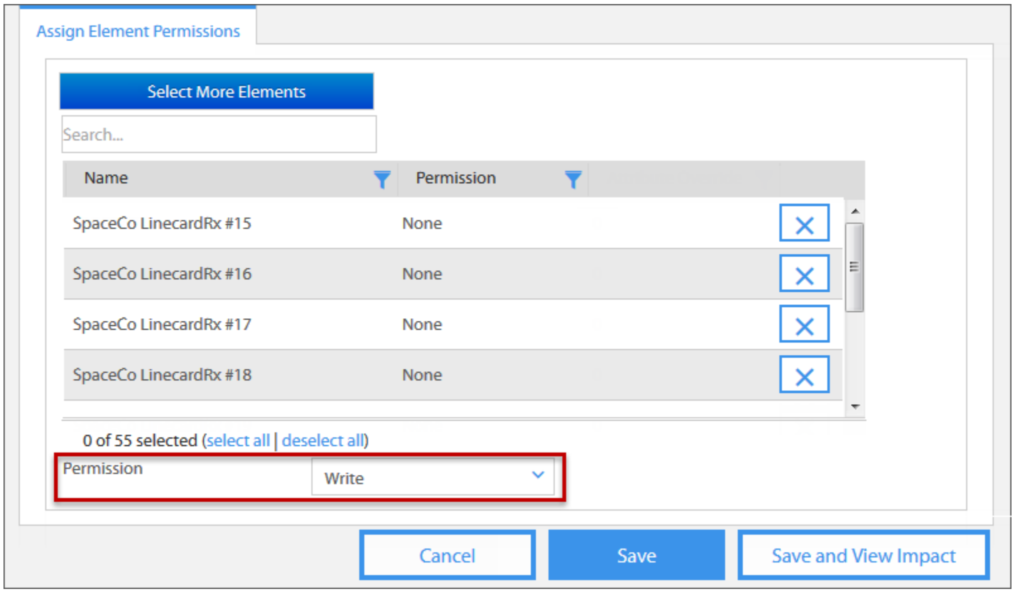


Figure 6-2. Add User Group Dialog

To create a new user group:

1. Click the **NMS Management** tab > **User Management** > **Add** > **User Group.**
2. Enter a **Name** and **Description** of the new user group.
3. Use the **Labels** multi-select field to assign one or more labels to this element, from the list of pre-configured labels.
4. Click **Select More Elements**, under **Assign Element Permissions**, to open the Search dialog to specify elements for which permissions will be assigned to this group.
5. If desired, use the **Element Type** filter drop-down, to list a selected type of element.
6. With the elements listed, use one of the following methods to select elements to which the user group will have either Read, Write, or Own access.
   a. Select one or more of the listed elements.
   b. Click the **Select All** link to select all of the listed elements.

7. With the elements selected, click the **Select Elements** button to add the elements to the **Add User Group** dialog. The elements are listed by **Name** and **Permission**.
8. With selected elements listed use one of the following methods to assign permissions:
   a. Click the **Permission** drop-down field on each listed element and choose **None**, **Read**, **Write** or **Own** as the Permission to assign to this group for the specified element.
   b. Select multiple elements or click the **Select-All** link to select all of the displayed elements, then use the **Permission** drop-down field, at the page bottom, to choose **None**, **Read**, **Write** or **Own** as the Permission to assign for the selected elements.
9. Repeat the previous steps, from Step 4, to assign additional elements to the group.
10. Click **Save** to save the configuration and continue or click **Save and View Impact**.



Name	Permission
SpaceCo LinecardRx #15	None
SpaceCo LinecardRx #16	None
SpaceCo LinecardRx #17	None
SpaceCo LinecardRx #18	None

0 of 55 selected (select all | deselect all)

Permission: Write

Figure 6-3. Add New User Group - Assign Element Permissions Dialog

6.3 Creating User Roles

In Pulse, a *user role* defines a set of NMS activities that can be performed by a user to which the role has been assigned. A role must exist in the NMS before it can be assigned to a user.

When a new role is created, the idea is to specify a set of permissions that align with specific responsibilities of different real-life roles, in terms of working with the iDirect Network. By creating multiple roles, each with specific permissions, roles can be assigned to allow access and functionality to specific users based on work responsibilities.

In the **Add User Role** dialog, there are seven permissions categories from which as many permissions as required may be selected and assigned to the new role. A role can allow user access to everything or can limit access to **Latency Stats only.**

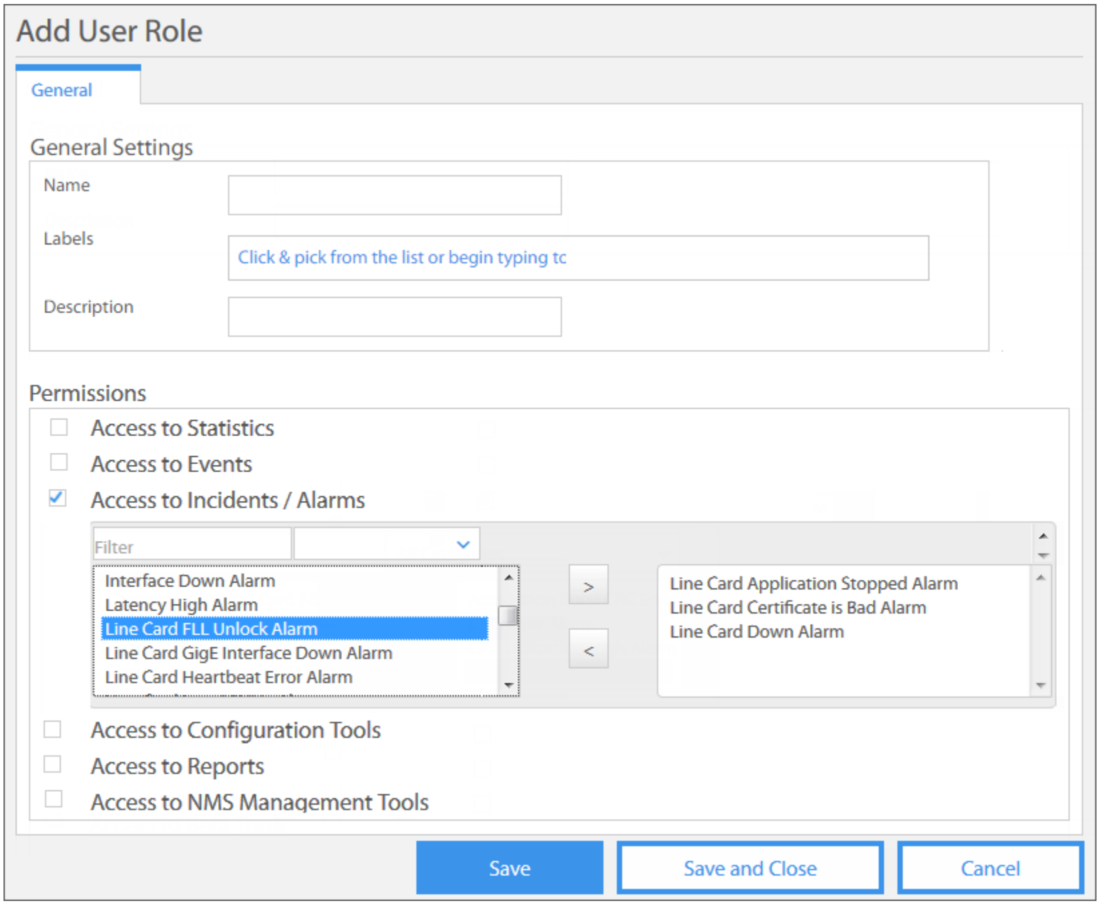

Add User Role
General
General Settings
Name
Labels
Click & pick from the list or begin typing tc
Description
Permissions
☐ Access to Statistics
☐ Access to Events
☑ Access to Incidents / Alarms
Filter
Interface Down Alarm
Latency High Alarm
Line Card FLL Unlock Alarm
Line Card GigE Interface Down Alarm
Line Card Heartbeat Error Alarm
>
<
Line Card Application Stopped Alarm
Line Card Certificate is Bad Alarm
Line Card Down Alarm
☐ Access to Configuration Tools
☐ Access to Reports
☐ Access to NMS Management Tools
Save
Save and Close
Cancel

Figure 6-4. Add User Role Dialog

To add a new user role:

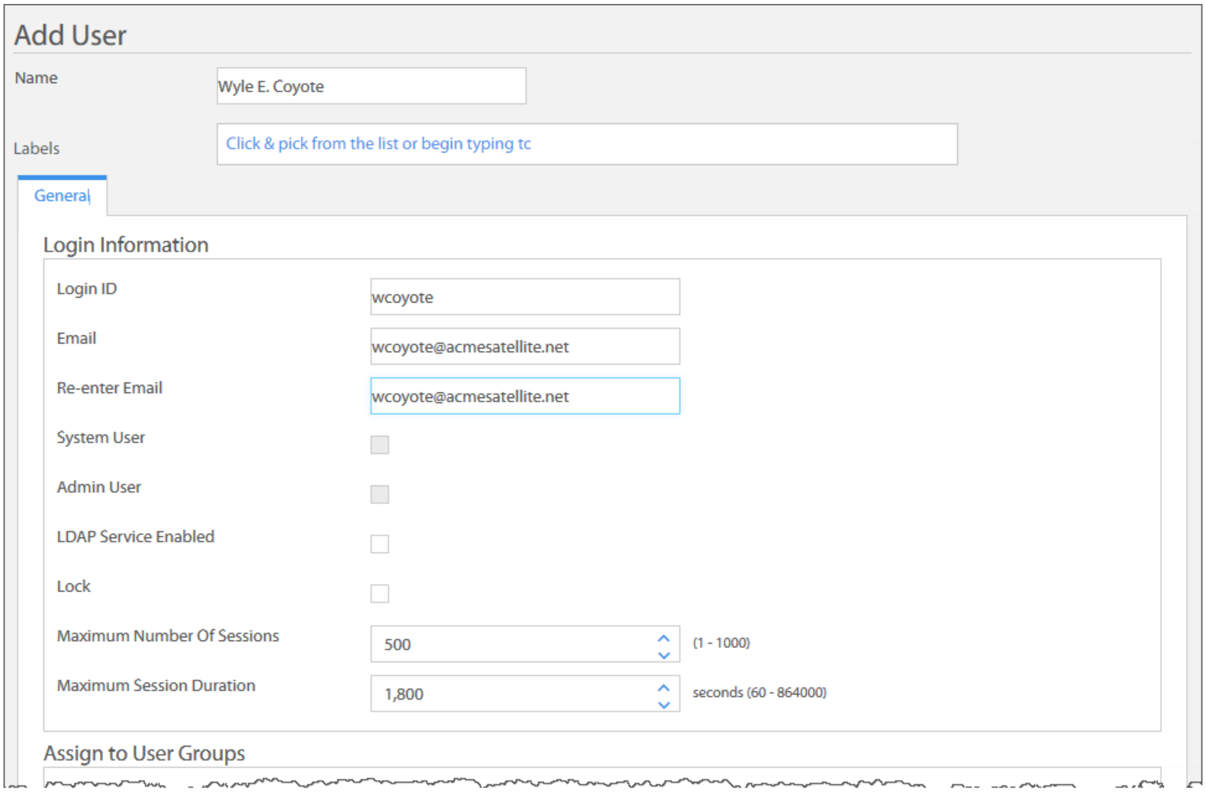
1. Click the **NMS Management** tab > **User Management** > **Add** > **User Role.**
2. Enter a **Name** and a **Description** for the new user role.
3. Use the **Labels** multi-select field to assign one or more labels to this element, from the list of pre-configured labels.
4. Click the check box adjacent to the permissions category, from which permissions are to be selected — for example, **Access to Statistics**, **Access to Events**, or **Access to NMS.** The permissions for the category are then displayed.
5. Click and select one or more permissions in the left pane of the permissions category.
6. Click the *add to list* arrow “**>**” to add the selected permissions to the new role. Repeat the previous two steps to add permissions from other permissions categories.
7. Use the *remove from list* arrow “**<**” to remove permissions from the role.
8. Click **Save** to save and continue working or click **Save and Close**.

6.4 Creating User Accounts

A *user* is an individual or an internal process or external system that has authorized access to the NMS, but only as a member of one or more user groups and with assigned user roles.

For each individual or entity that must gain NMS access, a new user account must be established. An individual or system not having established and active credentials in the NMS system is not considered an NMS user and is denied access.

When a user account is created, each user is assigned to group memberships and user roles. These assignments, which may be done during account creation or at a later date, determine the access level that each user is granted. Depending on the user’s responsibilities, group memberships and roles may be assigned. Memberships and roles may be changed at any time.



Add User

Name	Wyle E. Coyote
Labels	Click & pick from the list or begin typing tc

General

Login Information

Login ID	wcoyote	
Email	wcoyote@acmesatellite.net	
Re-enter Email	wcoyote@acmesatellite.net	
System User	☐	
Admin User	☐	
LDAP Service Enabled	☐	
Lock	☐	
Maximum Number Of Sessions	500	(1 - 1000)
Maximum Session Duration	1,800	seconds (60 - 864000)

Assign to User Groups

Figure 6-5. Add User Account - User Name and Credentials Dialog

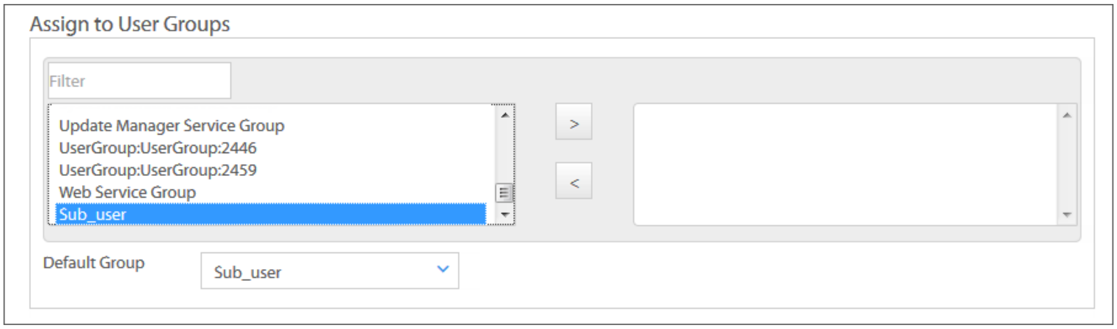
To create a new user account:

1. Click the **NMS Management** tab > **User Management** > **Add** > **User.** The **Add User** dialog opens. The dialog contains a **General** settings, **Login Information, Assign User Groups**, and an **Assign User Roles** section.
2. Type the full **Name** for the owner of the new user account.
3. Use the **Labels** multi-select field to assign one or more labels to this element, from the list of pre-configured labels.
4. Enter the NMS authentication credentials using **Login ID**

5. Enter the user **Email** address; and **Re-enter E-mail** address as confirmation.
6. Select **Enable LDAP Service** (*Light Weight Directory Access Protocol*) to enable the LDAP service to this user account.
7. Select **Lock** to lock down access to an existing user account.
8. Specify the **Maximum Number of Sessions** to allow this user account to establish.
9. Enter the **Maximum Session Duration**, in seconds.
10. See *Assigning User to Group Memberships*.

6.4.1 Assigning User to Group Memberships

Users may participate in multiple user groups, depending on their specific responsibilities and access permissions. Membership in various groups may change at any time, as required, by simply adding to or removing from the list of memberships.



Default Group: Sub_user

Figure 6-6. Dialog - Assign New User to Group Memberships

To assign user to one or more groups:

1. In the left pane of the **Assign to User Groups** section, use the **CTRL** key to select one or more groups to assign to this user account.
2. Click the *add to list* arrow "**>**" to assign the selected user groups to the new user.
3. Use the *remove from list* arrow "**<**" to remove a user group from the new account.
4. Select a **Default Group**, if two or more group memberships are assigned to the user.
5. See *Assigning Roles to New User*.

6.4.2 Assigning Roles to New User

Not only is a new user assigned specific group memberships, but also specific roles. By assigning roles to a user, the user is given access to specific NMS pages and allowed to perform certain functions. Multiple user roles may be assigned to a user, depending on his or her specific duties. When each user role is created, specific functional elements are added from the NMS operational categories.

Roles assigned to a user may change at any time as required, by adding to or removing specific items from the list of assigned roles.

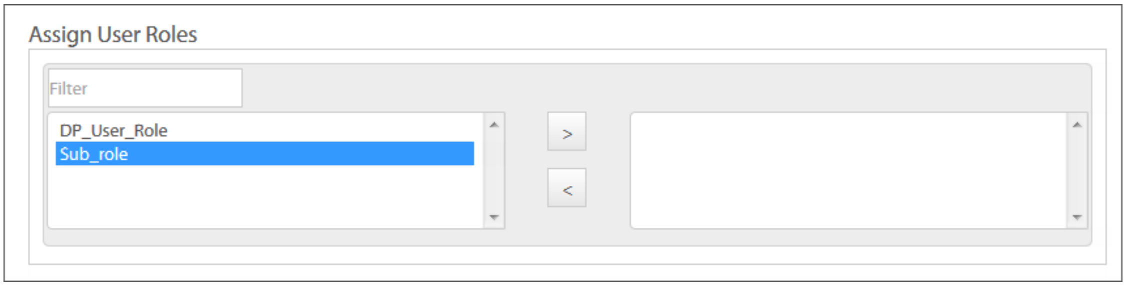


Figure 6-7. Dialog - Assign Roles to New user Account

To assign one or more roles to a new user:

1. Click a single role in the left pane of the **Assign User Roles** section, or use the **CTRL** key and select multiple roles targeted for this user account.
2. Click the *add to list* arrow "**>**" to add the selected user roles to the new user.
3. Use the *remove from list* arrow "**<**" to remove a user role from the new account.
4. Click **Save** to save the configuration and continue or click **Save and View Impact**.

6.5 Creating a New Customer Record

A *customer* is an NMS data record of a individual or business entity, and not necessarily an NMS user. The record contains contact information, including name, phone number, and e-mail address. Unless a customer has an authorized user account, it has no NMS access.

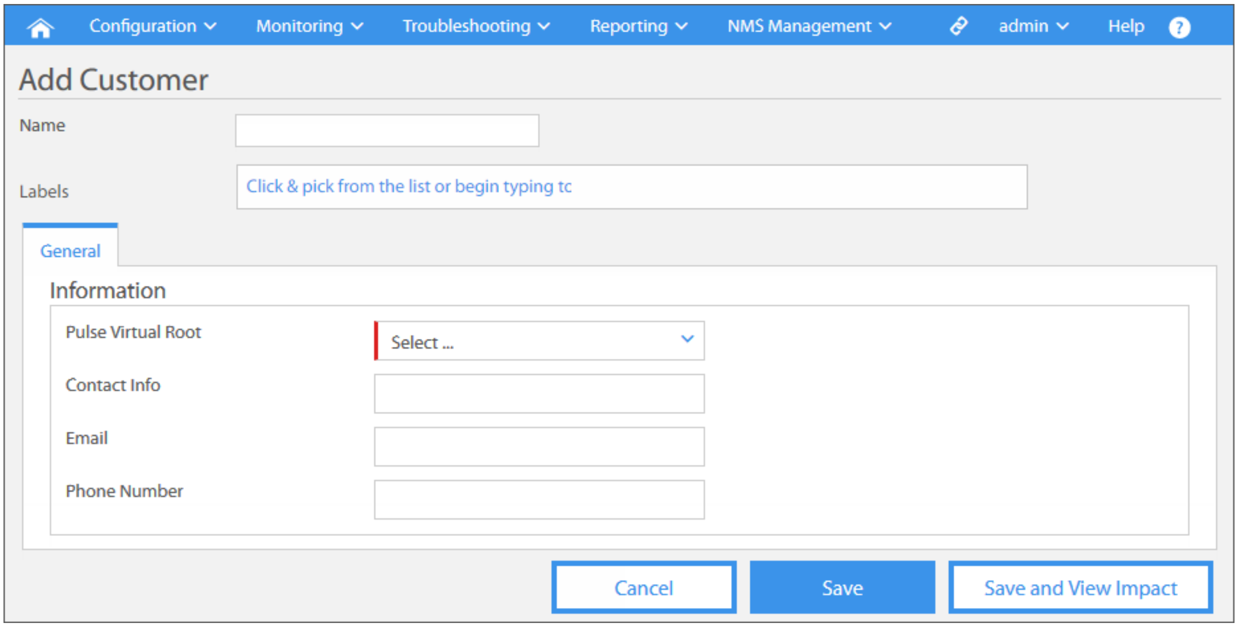


Figure 6-8. Add Customer Dialog

To create a new customer account:

1. Click the **NMS Management** tab > **User Management** > **Add** > **Customer.** The **Add Customer** dialog opens.
2. In the **Name** field, enter a customer name.
3. Use the **Labels** multi-select field to assign one or more labels to this element, from the list of pre-configured labels.
4. Use the **Pulse Virtual Root** drop-down to select the correct root node for this customer.
5. Use **Contact Info** to enter customer contact information.
6. Enter an **E-mail** address and **Phone Number** for the customer contact.
7. Click **Save** to save the configuration and continue or click **Save and View Impact**.

6.6 User Account Management

Pulse user account management operations are available depending on the permission level of the account holder. Many of these operations are indirectly accessed using the **Browse** commands for user groups, user roles, user accounts, or customers. By accessing these commands, it is possible to perform the following actions:

- Modify/Delete User Role, User Group, User Account, or Customer
- Modify/Delete System Tool
- Lock/Unlock User Account
- Create Tokens, Modify Token Number

6.6.1 User Account Lockout

If incorrect credentials are entered on several login attempts, then the account may be deactivated. If an account is deactivated as a result of too many failed attempts, the account will be set to inactive and no further login attempts will be accepted until an authorized system administrator resets that account.

This feature can be turned off by a system administrator, and the number of failed attempts that causes lockout can be adjusted by a system administrator.

6.6.2 Session Handling

By default, the NMS automatically terminates a user session and logs the user out of the system if there is no activity for 30 minutes. Authorized administrators may modify this default “no activity time-out” on a user or user group basis. It may become necessary, for example, to allow NOC operators and other support personnel to remain logged in for extended periods of time, even for those periods when there is no activity.

Overriding this feature may also be useful, for example, when operators need to bring up certain monitor displays and leave the display up for regular or extended observations.

6.6.3 Enabling/Disabling Session Inactivity Default Time-out

Caution should be exercised in choosing to enable this option. If a user, rather than clicking the ‘Logout’ link, disconnects by closing the browser, or the browser crashes, the user would then have to wait the requisite number of minutes of inactivity for the session to be regarded as ‘inactive’ and expire before re-connection is possible.

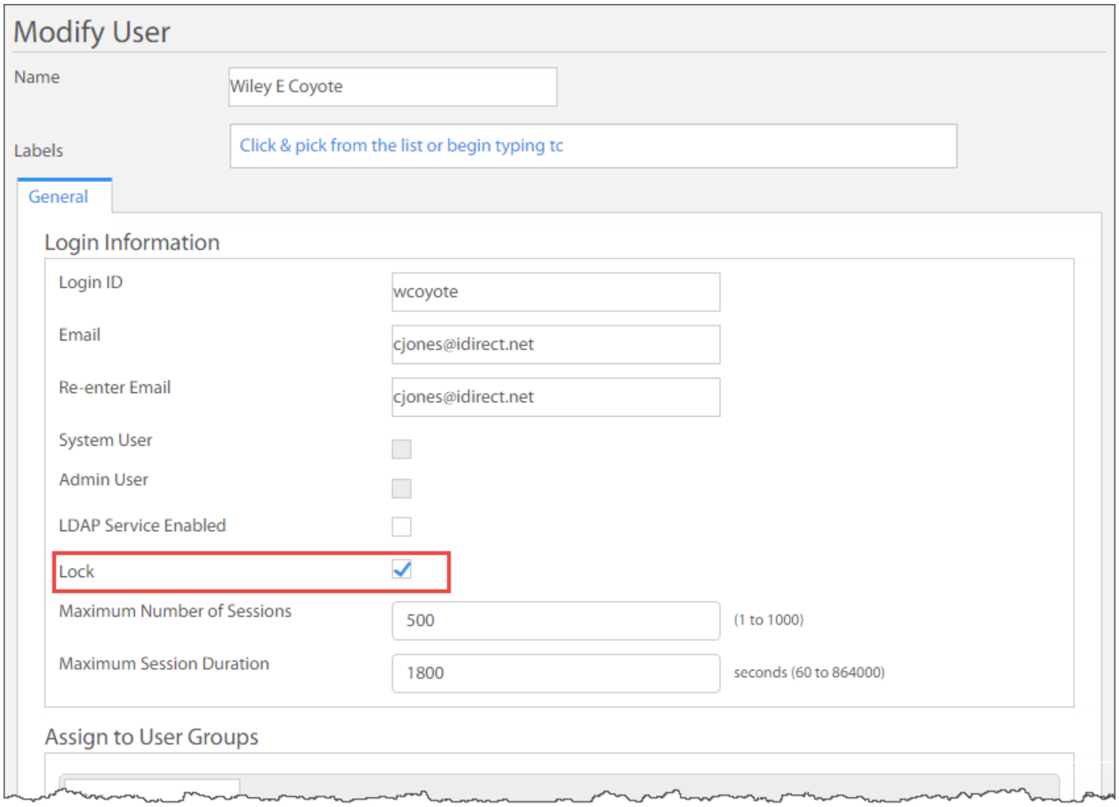
During any login, if login credentials are incorrectly entered on several login attempts, then the account may be deactivated. If the account is deactivated, as a result of too many failed login attempts, the account is set to inactive and no further login attempts are accepted until an authorized system administrator resets the account.

This feature can be turned off by a system administrator, and the number of failed attempts that causes lockout can also be adjusted.

6.6.4 Locking a User Account

Locking a user account is a second method by which the NMS removes a user account from active status. When a user is locked, all of the attributes of the account remain in the system, but no one can use the account to log in to the NMS.

A locked account can be reinstated by unlocking the account and thereby restoring all of its previously assigned functionality.



Modify User

Name: Wiley E Coyote

Labels: Click & pick from the list or begin typing tc

Login Information

Login ID: wcoyote

Email: cjones@idirect.net

Re-enter Email: cjones@idirect.net

System User ☐

Admin User ☐

LDAP Service Enabled ☐

Lock ☑

Maximum Number of Sessions: 500 (1 to 1000)

Maximum Session Duration: 1800 seconds (60 to 864000)

Assign to User Groups

Figure 6-9. User Credentials Dialog - Revoking User Credentials

To lock a user account:

1. Click the **NMS Management** tab, and under **User Management**, click **Browse** > **Users**.
2. Start typing the user name in the **Search** field to narrow the results list.
3. Select the desired user name when it appears.
4. Click the **Actions** button and select **Modify User**. The **Modify User** dialog opens, and is populated with all of the attributes configured for the user account.
5. Under **User Credentials**, select the **Lock** check box, to deactivate the user account.
6. De-select the **Lock** check box to reactivate a deactivated account.
7. Click **Save** to save the configuration and continue or click **Save and View Impact**.

6.6.5 Changing a User Account Password

When a new NMS user account is created, a limited time token is sent to the user that allows the user to login to the NMS and create a new password. After login users can change their own password. To increase security, NMS users should occasionally change their password.

Administrators or users that have the **Manage Users** permission may access and change all user passwords.

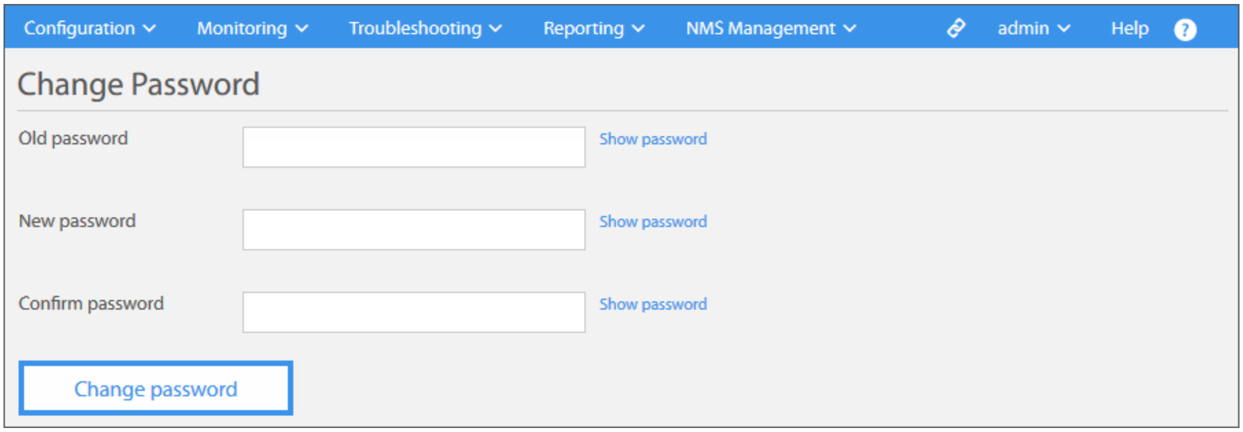


Figure 6-10. Change User Account Password Dialog

To change your user account password:

1. Click **NMS Management** from the main navigation tabs, and then under **User Credentials** select **Change User Password** to display the **Change Password** dialog.
2. Select **Show Password** on any of the password fields to reveal the entry.
3. Enter the current password in the **Old Password** field.
4. Enter the **New Password**; then re-enter using **Confirm New Password**.
5. Click **Change Password**.

Changes to a user account take place immediately. However, the new password does not take effect until the next login under the changed account. If changes are made during the current NMS session, the old settings remain in effect for the duration of that session.

The following guidelines should be observed when changing a user account password:

- Common dictionary words are not allowed
- Passwords must contain at least eight characters
- Passwords must contain at least one numeral (0-9) and one special character (~!@#$%^&*+<>?=)
- Passwords expire after 30 days and must be reset by the account owner
- The last three passwords used to access an account may not be reused

6.6.6 Resetting a User Account Password

The Reset Password command allows an NMS user to change his or her own user password. Upon initiating the command, an e-mail that contains a reset token is forwarded to the e-mail address of the account holder. Password reset is accessed from the **NMS Management** tab, under **User Credentials**.

This feature, which assists users in recovering their own passwords or user names, is only possible if the feature is enabled. If the feature is not enabled it will be necessary to contact an authorized system administrator or an individual with appropriate system-level access.

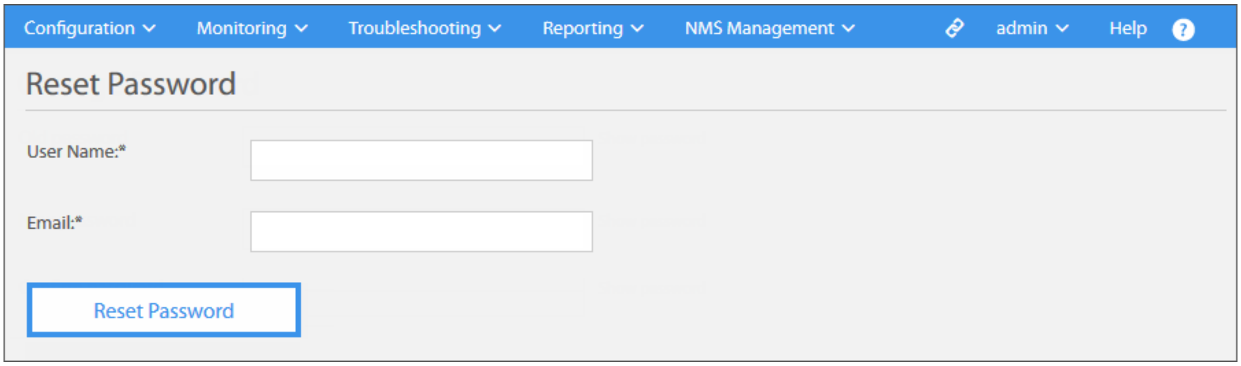


Figure 6-11. Reset Account Password Dialog

To reset a user account password:

1. Click **NMS Management** from the main navigation tabs, and then under **User Credentials** select **Reset Password** to display the **Reset Password** dialog.
2. Type the **User Name** and **E-mail** address configured for the NMS user account.
3. Click **Reset Password.** Upon submitting the request, an e-mail with instructions and reset token is sent to the e-mail address associated with the user account.
4. Click the token link that the e-mail contains and a new password reset dialog is opened.
5. Type a **New Password** and re-type to **Confirm New Password**.
6. Click **Reset Password.** The normal NMS login dialog is presented.
7. Enter a **User Name** and newly created **Password**, and click **Login**.

6.7 Creating and Managing Tokens

In an iDirect Network system a *token* is a way of managing certain operations — or, more precisely, a way of managing the number of times a certain operation can be performed or an element type may be created. For example, a user group may be assigned tokens that allow users in that group to create 1,000 terminals. Each time a new terminal is created, the token number is reduced by one. When the token number reaches zero, the user group cannot create additional terminals.

This section introduces token use and how tokens are managed in an iDirect network.

6.7.1 About Tokens

By assigning tokens to a specific user group, that user group becomes the owner of the tokens and is thereby able to perform the token-required operation, up to a predetermined number of times. Tokens may only be created to manage the operations by a User Group.

The following token types may be created:

- Terminals — to manage the number of Terminals created.
- SSPCs — to manage the number of Subscriber Service Plan Profiles created.
- User Groups — to manage the number of User Groups created.
- Users — to manage the number of User Accounts created.

The NMS tracks the *token number* — which is the number of tokens owned by a user group for a specific operation; the *available tokens* — which is the number of tokens still open for use by a user group; and *used tokens* — the number of tokens that are already used or given away.

If a user group uses a token to create a new SSPC, the number of “available tokens” decreases by one and the number of “used tokens” increases by one. The “token number” is unchanged. On the other hand, giving a token to another user group, which is possible, results in a decrease of the “token number” and “available tokens”, but “used tokens” is unchanged.

Table 6-2. Token Parameters

Token Parameters	Brief Description
Token Type	Examples are SSPP, Terminal, User Group, User Account
Element ID	Link to network element instance - for example SSPP, terminal
Token Parent	Link to user group owner of token
Token Number	Total number of tokens owned by a user group
Available Token	Number of tokens still available to a user group
Used Tokens	Number of tokens already used by a user group

6.7.2 Token Validation

An illustration of token use is demonstrated in the following example of two user groups.

If User Group A has 100 tokens of SSPP-1, then it can own up to 100 Subscriber Service Plan Components (SSPCs) of SSPP-1. In order to enforce this token validation, each time a User Group A operator attempts to create a new SSPC for SSPP-1, the NMS checks the available token value of User Group A. If no tokens remain, creation of the element is rejected.

Table 6-3. Token Management Illustration

	USER GROUP A			USER GROUP B		
Token Activity	**Token No.**	**Avail. Tokens**	**Used Tokens**	**Token No.**	**Avail. Tokens**	**Used Tokens**
Initial state	100	100	0	0	0	0
User Group A uses a token to create an SSPC	100	99	1	0	0	0
User Group B attempts to use a token to create an SSPC, and fails — there are no Available Tokens	100	99	1	0	0	0
User Group A assigns 30 tokens to User Group B	70	69	1	30	30	0
User Group A uses a token to create an SSPC	70	68	2	30	29	1
User Group B uses a token to create an SSPC	70	68	2	30	29	1

6.7.3 Creating a Token

This section describes the steps associated with creating a token. Tokens are created that manage the number of operations performed by a specific User Group.

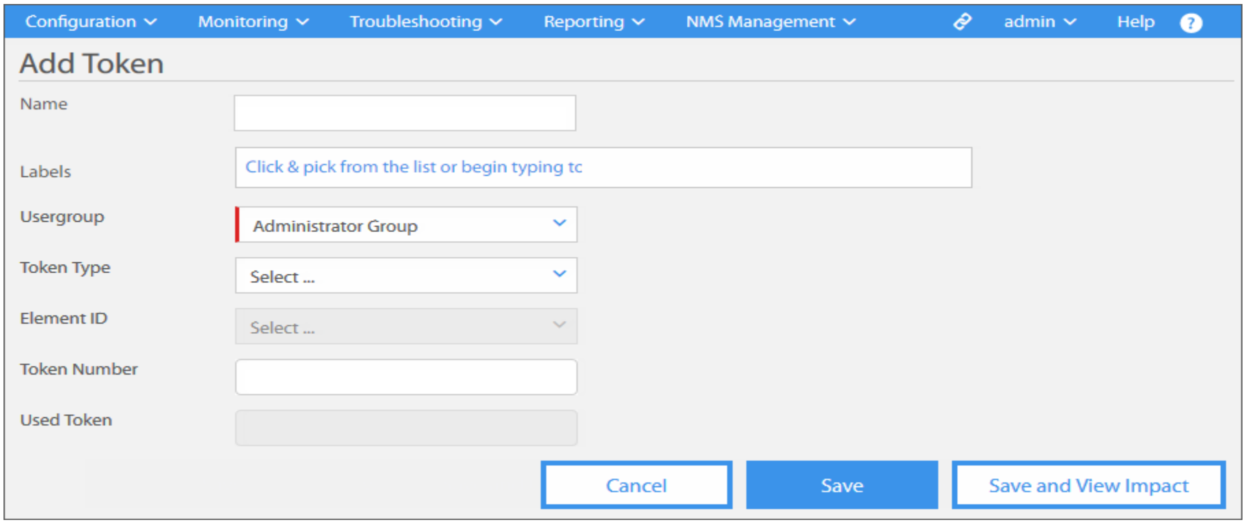


Figure 6-12. Add Token Dialog

To create tokens:

1. Click the **NMS Management** tab > **User Management > Browse** > **User Groups.**
2. With the browse results listed, choose the desired **User Group** to which ownership of the new token is to be assigned.
3. Click the **Actions** button and select **Create Token**. **The Add Token** dialog is presented**.**
4. Enter a **Name** for the token.
5. Use the **Labels** multi-select field to assign one or more labels to this element, from the list of pre-configured labels.
6. Use the **User Group** drop-down list and select the user group to which the token will be assigned.
7. Use the **Token Type** drop-down list and select **SSPP**, **Terminal**, **User**, or **User Group** as the type of token to create. When **SSPP** is selected, the **Element ID** field is enabled.
8. If **Element ID** is enabled, choose the SSPP (Subscriber Service Plan Profile) for which the token is being created.
9. Enter the **Token Number** value to assign to this new token.This value represents the maximum number of times the token can be used.
10. In the **Used Token** field, enter the initial value at which the token count should start. After initiation of the token, the **Available Tokens** is set to *Token Number – Used Token*.
11. Click **Save** to save the configuration and continue or click **Save and View Impact**.

6.8 User Administration Browse Actions

Using the appropriate **Browse** command, users can interact with configured User Administration Domain elements in the Browse Results list. From the browse results, a set of specific operations can be performed. These operations are called "*actions*." An action can be performed on a single selected element or simultaneously on several selected elements.

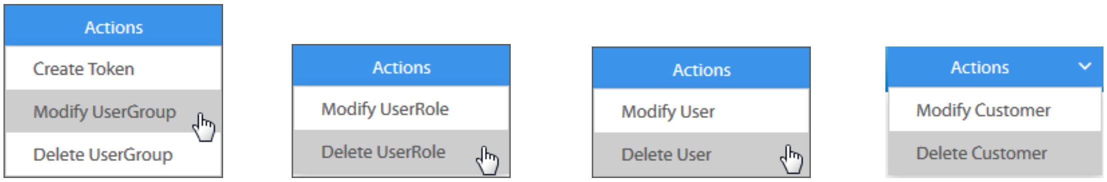


Figure 6-13. User Domain Elements Action Menus

The operations that are possible from an **Actions** menu, is based on the selected element, and only those actions are displayed when that element is selected.

The User Administration Domain element Actions are listed and briefly described in Table 6-4.

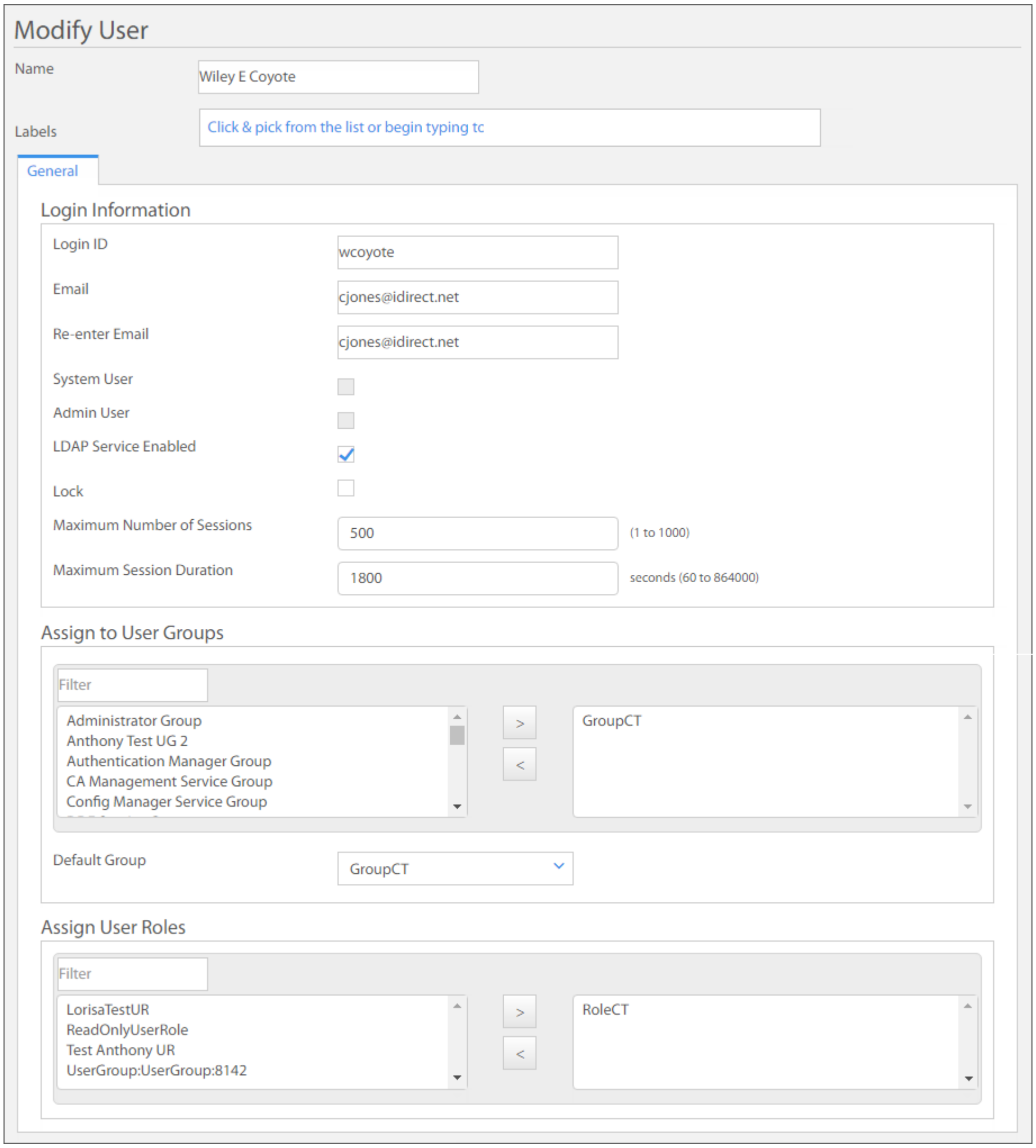
Table 6-4. User Groups, User Roles, User Accounts — Browse Actions

Action	Brief Description
Modify Element	View or Modify the configured information for the selected element. Modify as required and re-save with changes.
Delete Element	Remove the selected domain element from the NMS.
Create Token	Create token to manage the number of times a specific operation can be performed by a user group. The Create Token command applies only to user groups.

6.8.1 Modifying a User Group, User Role, User, or Customer

When a user group, user role, user account, or customer record is opened using the *modify element* action, all of the current attributes of the element are write-enabled and may be modified. In the case of a user account, for example, the user name and credentials may be changed; and group memberships and assigned roles may be added or removed.

The steps to modify a user account user group, user role, or customer record is essentially the same after listing the elements using the appropriate **Browse** command.



Modify User

Name: Wiley E Coyote

Labels: Click & pick from the list or begin typing tc

Login Information

Login ID: wcoyote

Email: cjones@idirect.net

Re-enter Email: cjones@idirect.net

System User ☐

Admin User ☐

LDAP Service Enabled ☑

Lock ☐

Maximum Number of Sessions: 500 (1 to 1000)

Maximum Session Duration: 1800 seconds (60 to 864000)

Assign to User Groups

Filter
Administrator Group
Anthony Test UG 2
Authentication Manager Group
CA Management Service Group
Config Manager Service Group
>
<
GroupCT

Default Group: GroupCT

Assign User Roles

Figure 6-14. Modify User Account Properties

To modify a user account:

1. With the **Browse** window open to a list of users found in the NMS, start typing the name of the user in the **Search** field to narrow the results list.
2. Select the desired user name when it appears.
3. Click the **Actions** drop-down list and select the **Modify** action. The **Modify User** dialog opens and is populated with all of the configured attributes.
4. Modify entries to the element as required.
5. Click **Save** to save the configuration and continue or click **Save and View Impact**.

6.8.2 Deleting a User Group, User Role, User, or Customer

The *delete element* action is invoked for a specific user group, user role, user account, or customer when the intent is to remove the element from the NMS. The implication of deleting each of these elements is described below:

- **Delete User Group** — This action results in the deletion of all memberships related to the user group. To delete a user group requires the “**Own”** permission of the element.
- **Delete User Role** — This action results in the removal of the role from the NMS. The user role is removed from all user accounts to which it was previously assigned.
- **Delete User** — This action removes, from the NMS, all of the user account attributes except for any activity log entries that pertain to the user. After the user is deleted, post-deletion queries of the activity log for the account are still possible, since the user name is written to every activity and is maintained in the activity log.
- **Delete Customer** — This action removes, from the NMS, all of the customer attributes, except for activity log entries that pertain to the customer. After the customer is deleted, post-deletion queries of the customer activity log are still possible, since the customer name is written to every activity and is maintained in the activity log.

.

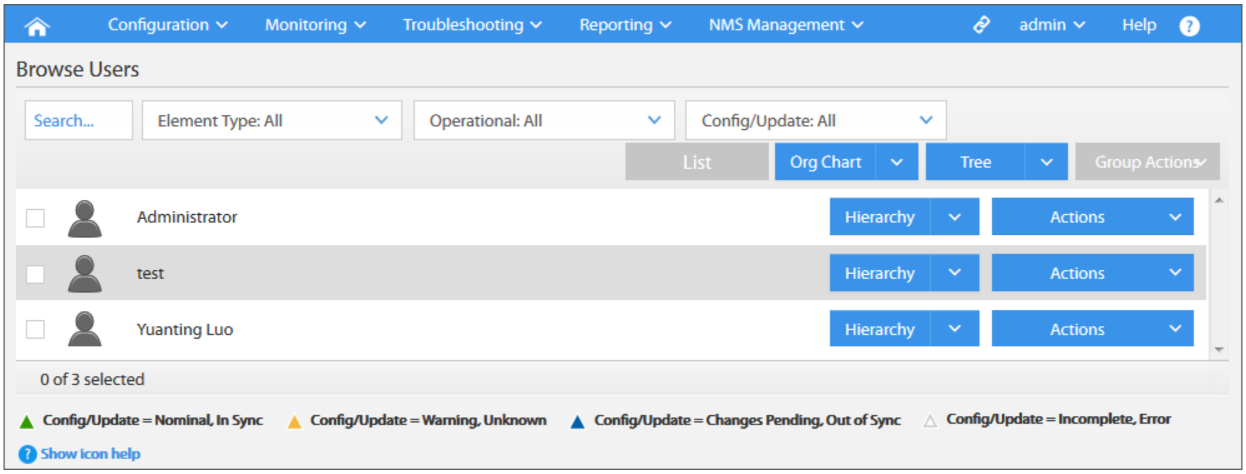


Figure 6-15. Example - Deleting a User Account

The **Delete Element** action is performed in much the same way for all User Admin elements.

To delete a user:

1. With the browse result open to a list of users found in the NMS, start typing the name of the user in the **Search** field to narrow the results list.
2. Select the desired user when it appears.
3. Click the **Actions** drop-down list and select **Delete User**. A delete confirmation prompt is presented.
4. Click **OK** to confirm that the user account should be removed from the NMS database; click **Cancel** to abort the operation.

7 Configuring Pulse NMS Physical Domain Elements

In an iDirect Network, physical infrastructure elements include physical sites at which network subsystems are located, as well as the equipment located at those sites.

Site types in an iDirect network include Satellite Access Stations (SAS), Network Operations Center (NOC), and the Extended Access Portal (EAP). The NMS physical domain represents only the equipment in those sites that form the Pulse Network Management System (NMS).

Configuring Pulse NMS Physical Domain Elements is covered in the following topics:

7.1 About NMS Sites (SAS, NOC, EAP)

A *Site,* in an iDirect network, is a collection of processes and machines at a given location. A *Satellite Access Station* (SAS) site, for example, contains hub equipment such as Protocol Processor servers, line cards and chassis, NMS servers, as well as the associated SVNs.

The operational mode of a site can be configured as a SAS, NOC (*network operations center*), or an EAP (*external access portal*) site. Each site type supports full redundancy that consist of a primary and, in some cases, an optional backup or secondary site.

NMS sites include the following:

- *Satellite Access Station (SAS) Site* — the SAS site contains a Pulse NMS cluster, which is responsible for system configuration, control, monitoring, alarming, and reporting; as well as control of local network upgrades, real-time events and statistics reporting.

  Each SAS site supports a single satellite within a satellite network. In addition to the NMS physical domain elements, the SAS includes hub chassis, line cards, protocol processors, switches and routers, all of which provide an interface between the IP network of the backbone network and the radio frequency (RF) links to a satellite. Multiple SAS sites are possible at a given location. See **Note**.

- *Network Operations Center (NOC) Site* — the NOC site contains a Pulse NMS cluster that is responsible for system configuration, control, monitoring and reporting of events and alarms, control of all network upgrades, as well as long-term storage of statistics, alarms, and historical data.

  The NOC site also contains a Global Bandwidth Management (GBWM) cluster that is responsible for global QoS enforcement, by adjusting bandwidth allocation to reflect the configured committed and maximum information rates on Group Service Plans as well as the aggregate demand of all SAS sites.
- *Extended Access Portal (EAP) Site* — an EAP site is a Pulse instance that is responsible for providing secure portals to allow NMS access to the Velocity system by service providers and subscribers. If desired, an EAP may be installed in the same physical location as the NOC.

NOTE: Since the hub-related SAS components are considered part of the Velocity Physical Domain, and therefore, are configured from the **Configuration** tab under **Physical Domain**. Refer to the document *iDirect Velocity Network Operations Using Pulse* for configuring these elements.

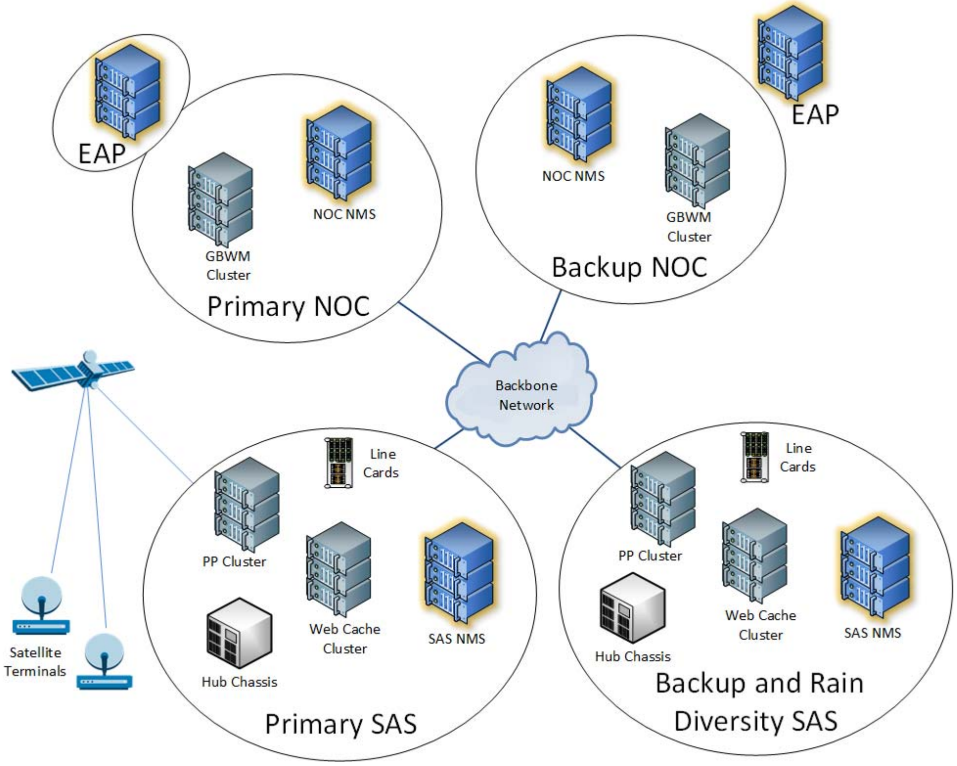


Figure 7-1. NMS Site — Distributed Components (SAS, NOC, EAP)

See the *iDirect Velocity™ Technical Reference Guide* for additional details on Velocity sites.

7.2 Creating an NMS Site (SAS, NOC, EAP)

Each applicable NMS site, which can be designated as the primary site or as the backup site, must be configured in Pulse.

The Add Site dialog is used to create NMS sites or sites at which the NMS is located. A Pulse Network Management System can be installed at a SAS, NOC, or EAP site, or at all three sites.

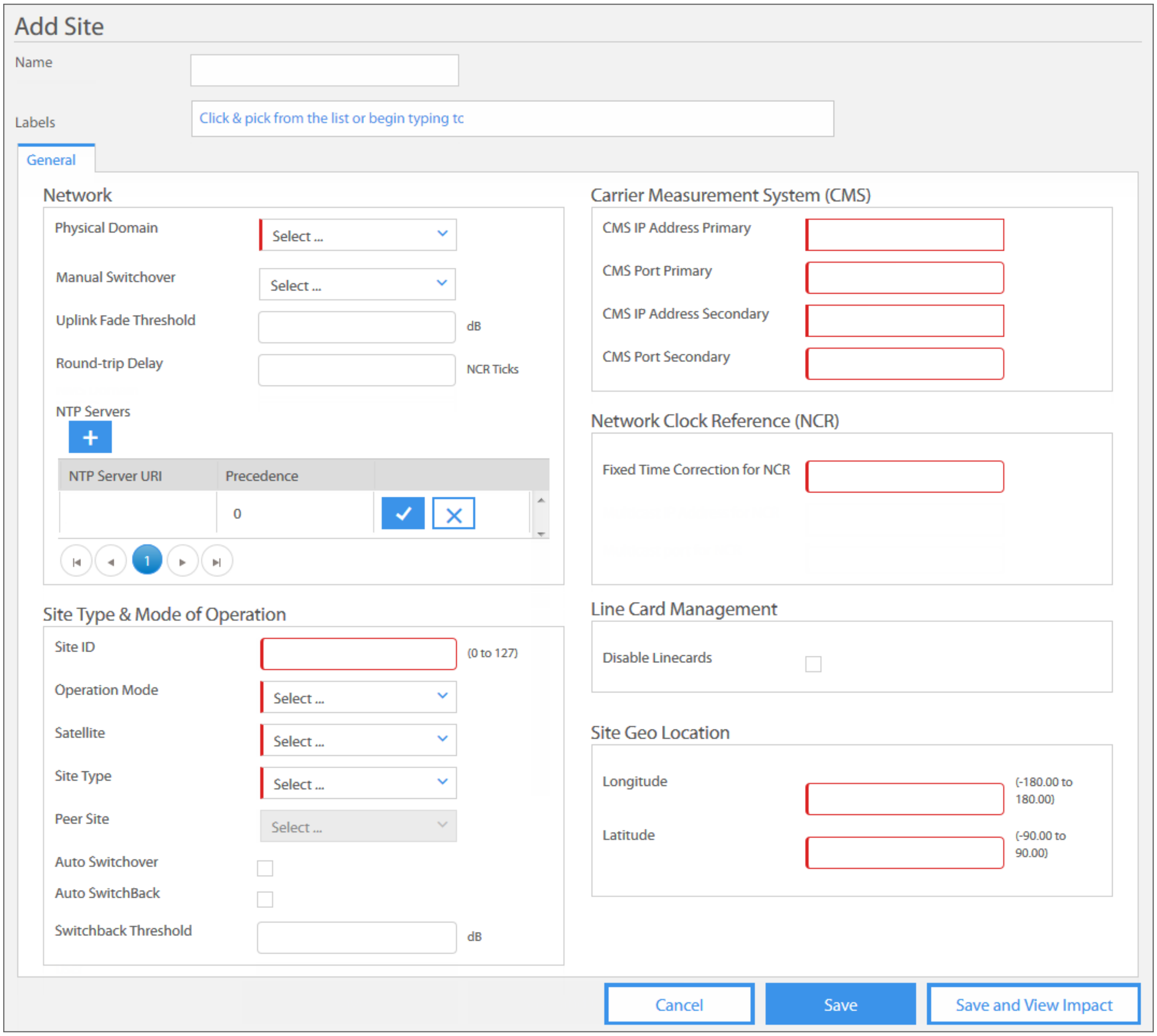


Figure 7-2. Add NMS Site Dialog (SAS, NOC, EAP)

To add a Site:

1. Click the **NMS Management** tab > **NMS Physical Domain** > **Add** > **NMS Site**.
2. Type the **Name** of the new Velocity site in the **Add Site** dialog.
3. Use the **Labels** multi-select field to assign one or more labels to this element.

4. Under the **Network** section, select the **Physical Domain** to which the Site is associated — this association refers to the Network to which this Site belongs.
5. Use the **Manual Switchover** drop-down and select whether the site should become a **Forced Primary** site or **Forced Diversity** site during a manual site switchover.
6. Enter the **Uplink Fade Threshold**. This value, measured in dB, represents the fade value at which a primary site will automatically switchover to the backup.
7. Enter the **Round-Trip Delay** time, in NCR ticks, between the satellite and this site.
8. Under the **NTP Server** section define one or more NTP Servers for use by this site to maintain clock synchronization among sites and servers. See *Configure Site NTP Servers*.
9. Under the **Site Type and Mode of Operation** section, enter the **Site ID**, as a value of 0-127. This value uniquely identifies this site.
10. Enter the **Operation Mode** of this site as a **NOC**, **SAS**, or **EAP**.
11. In the case of a SAS site only, use the **Satellite** drop-down to select the appropriate satellite.
12. Use the **Site Type** drop-down and designate this site as a **Primary_Site** or **Backup_Site**.
13. If applicable, use the **Peer Site** drop-down to select, from a list of configured sites, the peer site (primary/backup) that is associated with the site being configured.
14. Select **Auto Switchover** to enable an automatic switchover to the backup site in fade conditions; and select **Auto Switchback** to enable automatic switchback to the primary upon reaching the defined **Switchback Threshold**.
15. Enter the **Switchback Threshold** value. This value, measured in dB, represents the fade value at which a primary site will automatically switch back to the primary.
16. Under **Carrier Measurement System (CMS)**, use **CMS IP Address Primary** and **CMS Port Primary** to enter an IP address and port for the primary *CMS System* server for this site.
17. Use **CMS IP Address Secondary** and **CMS Port Secondary** to enter an IP address and port number for the secondary *CMS System* server for this site.
18. Under the **Network Clock Reference (NCR)** section, use **Fixed Time Correction For NCR**, to enter a value by which the NCR time is adjusted.
19. Under **Line Card Management**, select **Disable Line Cards** if the active line cards should disable their transmit carriers at the Tx line cards for channels that are to be switched.
20. Under **Site Geo Location**, use **Longitude** (-180 to +180) and **Latitude** (-90 to +90) to enter the site geographic location in degrees.

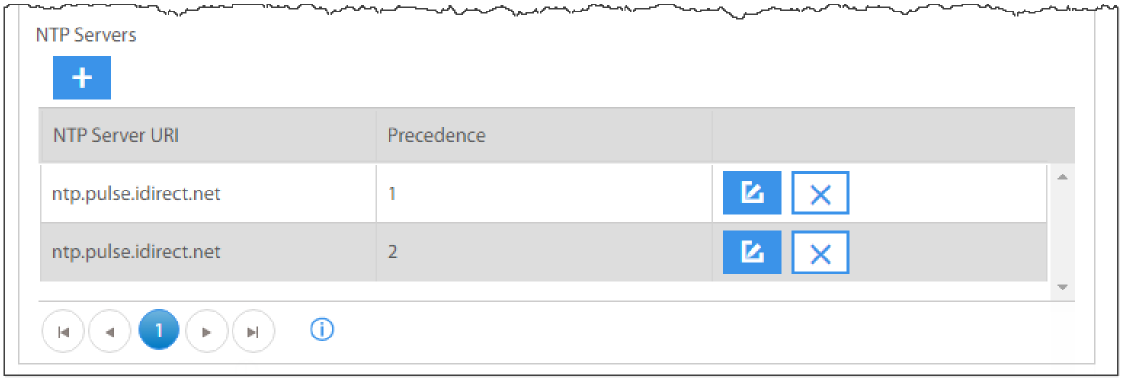
7.2.1 Configure Site NTP Servers

Using the **NTP Servers** dialog, multiple NTP servers can be entered as individual records for use by the site.

To configure an NTP Server for the Site configuration:

1. From the **Add Site** page, under the **NTP Server** section, click the **Add Record** icon to enable the configuration fields for entering a new NTP server record.
2. In **NTP Server URL,** enter the appropriate IP Address/URL for accessing the NTP server.

3. Click the **Update** icon to accept the **NTP Server** record entry.
4. Repeat the steps, from Step (2), to insert additional NTP Server records.
5. Click the **Edit** icon, on an **NTP Server** record, to modify the record; click the **Delete** icon, to remove the record.
6. Click **Save** to save the Site to the NMS database.



NTP Server URI	Precedence	
ntp.pulse.idirect.net	1	
ntp.pulse.idirect.net	2	

Figure 7-3. Add Site NTP Server Dialog

7.3 About Pulse NMS Servers

In an iDirect network, a cluster is a rack-mounted group of servers acting as a single system to provide related system resources. As network requirements grow, additional servers are added to a cluster. Currently, only one cluster, of a given type, may be configured at a site, and this cluster must be configured prior to adding servers to the cluster.

The NMS is composed of a comprehensive Web client and required servers that collectively provide control and visibility of all network components. NMS servers provide support for managing network configuration and control, software version management and updates, as well as for monitoring and reporting on network events and alarms.

Although NMS operations are generally centralized at the NOC, both centralized and distributed operations are supported. In particular, the NMS supports SAS-level operations if the NOC is not accessible.

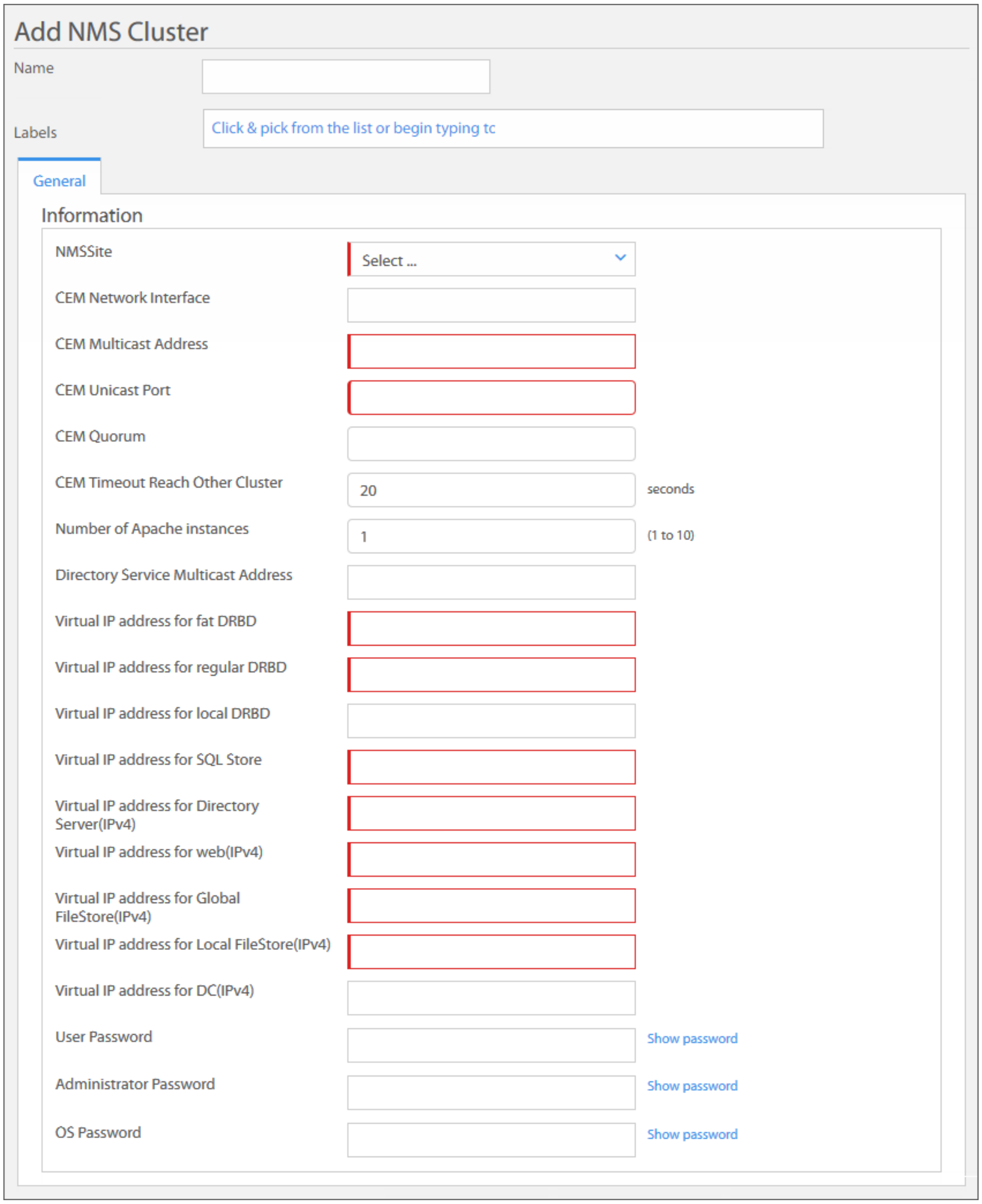
The NMS cluster supports the following functionalities:

- *NMS Storage and Compute* — are responsible for processing and computational work as opposed to persistent data storage. The emphasis is on maximizing execution threads, processing speed, memory usage and overall network throughput.
- *NMS Stats* — receive data from PP servers and provide data to the NMS when requested. The main emphasis of these services is on maximizing local storage throughput and in providing Network File System (NFS) exports to other cluster nodes.

7.4 Adding an NMS Cluster

An NMS *cluster* must be implemented at each primary SAS (SAS NMS) and primary NOC (NOC NMS) sites, and where applicable, at each optional backup SAS, and backup NOC site. The NMS cluster may also be located at an EAP site.

A new NMS cluster is added to the NMS using the Add NMS Cluster dialog. The NMS cluster must be configured before any servers are added to the cluster.



Add NMS Cluster

Name	
Labels	Click & pick from the list or begin typing tc

Information

NMSSite	Select ...	
CEM Network Interface		
CEM Multicast Address		
CEM Unicast Port		
CEM Quorum		
CEM Timeout Reach Other Cluster	20	seconds
Number of Apache instances	1	(1 to 10)
Directory Service Multicast Address		
Virtual IP address for fat DRBD		
Virtual IP address for regular DRBD		
Virtual IP address for local DRBD		
Virtual IP address for SQL Store		
Virtual IP address for Directory Server(IPv4)		
Virtual IP address for web(IPv4)		
Virtual IP address for Global FileStore(IPv4)		
Virtual IP address for Local FileStore(IPv4)		
Virtual IP address for DC(IPv4)		
User Password		Show password
Administrator Password		Show password
OS Password		Show password

Figure 7-4. Add NMS Cluster Dialog

To add an NMS cluster:

1. Click the **NMS Management** tab > **NMS Physical Domain** > **Add** > **NMS Cluster**.
2. Type the **Name** of the new NMS Cluster.
3. Use the **Labels** multi-select field to assign one or more labels to this element.
4. Use the **Site** drop-down and select the site at which the NMS cluster is located — for example, NOC, SAS, or EAP. The designated site can be either a primary site or optional backup site.
5. In **CEM Network Interface**, specify an interface name for the cluster election manager (CEM) LAN interface, for example – **ETH0**.
6. In **CEM Multicast Address**, specify a valid multicast address for the cluster election manager.
7. In **CEM Unicast Port**, specify a valid unicast port for use by the cluster election manager.
8. In **CEM Quorum**, specify the minimum number of NMS servers that must remain functional in order for the cluster to remain up and running. In the iDirect implementation, this integer value is calculated as (**N+1)/2**. The calculation ensures a non-zero value.
9. In **CEM Timeout Reach Other Cluster**, specify a communication time out duration for when communicating with other clusters.
10. Specify the **Number of Apache Instances** that can be used by this NMS cluster.
11. In **Directory Service Multicast Address**, specify a valid multicast address for the Directory Service process.
12. Use the following fields to enter virtual IP addresses for the NMS Cluster processes**:**
    a. **Virtual IP Address for FAT DRBD**
    b. **Virtual IP Address for Regular DRBD**
    c. **Virtual IP Address for Local DRBD**
    d. **Virtual IP Address for SQL Store**
    e. **Virtual IP Address for Directory Server**
    f. **Virtual IP Address for Web IPv4** (necessary for Web access)
    g. **Virtual IP address for Global File Store IPv4**
    h. **Virtual IP address for Local File Store IPv4**
    i. **Virtual IP Address for DCIPv4** (designated coordinator node for the cluster)
13. Enter a **User Password** for gaining access to the cluster at the application level.
14. Enter a **Administrator Password** for gaining administrative access to the cluster.
15. Enter an **OS Password** for gaining access to the cluster at the system level.
16. Click **Save** to save the NMS Cluster configuration.

7.5 Adding an NMS Server

The Add NMS Server dialog is used to add a new NMS server to an existing NMS cluster. The NMS includes configuration pages that support adding, modifying, and deleting NMS servers.

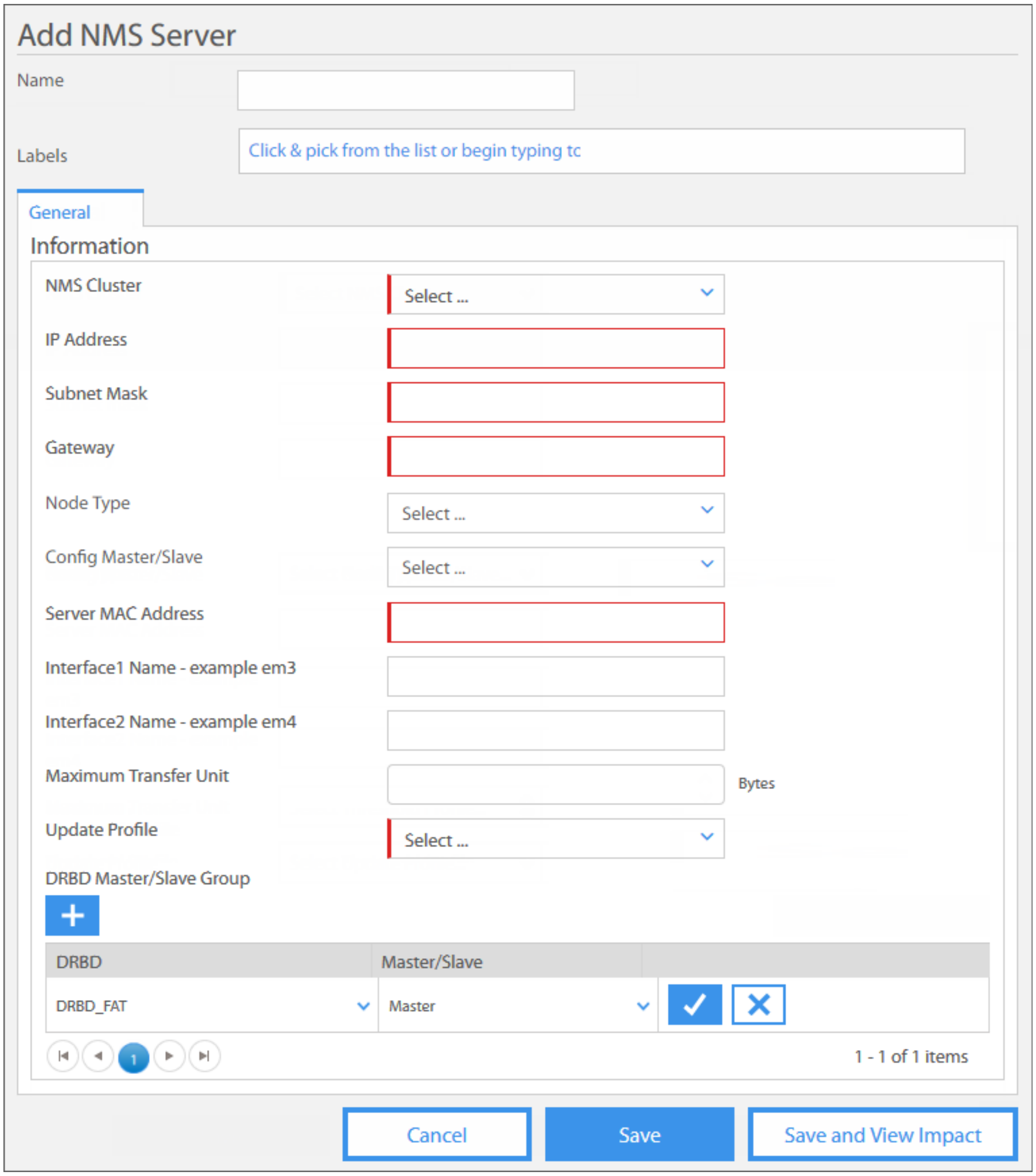


Figure 7-5. Add NMS Server Dialog

To add an NMS server:

1. Click the **NMS Management** tab > **NMS Physical Domain** > **Add** > **NMS Server**.
2. Type the **Name** of the new NMS server.
3. Use the **Labels** multi-select field to assign one or more labels to this element.

4. Under **Information**, use the **NMS Cluster** drop-down and select the cluster to which the new server is a member node.
5. Enter the following IPv4 address information for the upstream interface:
    a. Add the NMS Server **IP Address**.
    b. Add the **Subnet Mask** address.
    c. Add the **Gateway** address. This is the IP address of the upstream router interface connected to the to upstream LAN segment.
6. Select the appropriate **Node Type** — for example, “webserver”. Provides web acceleration features including web caching, and optional Domain Name Service (DNS) pre-fetch.
7. Use the **Config Master/Slave** drop-down to designate the server as a configuration **Master** or **Slave**.
8. Enter the NMS **Server MAC Address**.
9. Specify interface names using **Interface1 Name** and **Interface2 Name** respectively.
10. Use **Maximum Transfer Unit** to specify, in bytes, the maximum data transmission size.
11. Select a configured **Update Profile** that the Update Manager should apply to this NMS server.
12. Click **Save** to save the NMS Server configuration.

7.6 NMS Physical Domain Browse Actions

Using the **Browse NMS Physical Domain** command, users can interact with configured Pulse NMS Physical Domain elements, to perform a variety of operations. These operations are called “actions.” An action can be performed on a single selected element or simultaneously on several elements of the same type. NMS Physical Domain browse element actions are listed and briefly described as follows:

Table 7-1. NMS Physical Domain — Browse Actions

Action	Brief Description
View Element	View configured information for the selected network.
Copy Element	Create a cloned copy of the selected network, which can be modified as required, renamed, and saved as a new network system.
Modify Element	Modify the configuration of the selected network, and re-submit to NMS.
Delete Element	Remove the selected network from the NMS database.
Apply Configuration	Apply configured NMS changes to the selected network, using the pending option file configured for the network.
Progress Report	View a summary report of update manager progress since applying changes to the selected network.
Retrieve Pending Option File	Load from the NMS database, and display the pending copy of the options file for the selected network.
Retrieve Active Option File	Load and display the options file currently active for the selected network.
Compare Configuration	Compare the pending and the active options files for the selected network.
Modify Engineering Debug Keys	Modify custom key associated with a specific feature of the selected network, to enable, disable, add or modify functionality.

8 NMS Services & System Management

This chapter is the first of three chapters that cover Pulse System Administration domain operations. In large, this chapter is concerned with the various NMS services and operations that involve management of network element configuration and update. It is also concerned with the management of events and stats data collection in an iDirect Network.

Finally, this chapter includes those operations that support Pulse NMS job scheduling, and the monitoring of performance characteristics of the NMS itself.

NMS services and system management is covered in the following topics:

- *Adding a Network* on page 98
- *Network Browse Actions* on page 99
- *About Management Profiles* on page 100
- *Adding an Events Management Profile* on page 101
- *Adding a Stats Threshold Rule* on page 102
- *Adding a Stats Threshold Profile* on page 104
- *Adding an Update Rule* on page 104
- *Adding an Update Profile* on page 106
- *Adding a Scheduled Job* on page 107
- *Modifying an NMS Service Config File* on page 109
- *NMS Services Browse Actions* on page 110

8.1 Adding a Network

The **Add Network** operation is used to specify a new iDirect Network to be managed using Pulse. Each configured network will contain, under it, the components of each element domain — for example, Physical, Transport, Network, Service, and Terminal domain components. As you configure each element of the new network, you must associate the element with the appropriate network. Although a basic network will generally define a single network, complex network systems may have multiple networks defined in Pulse.

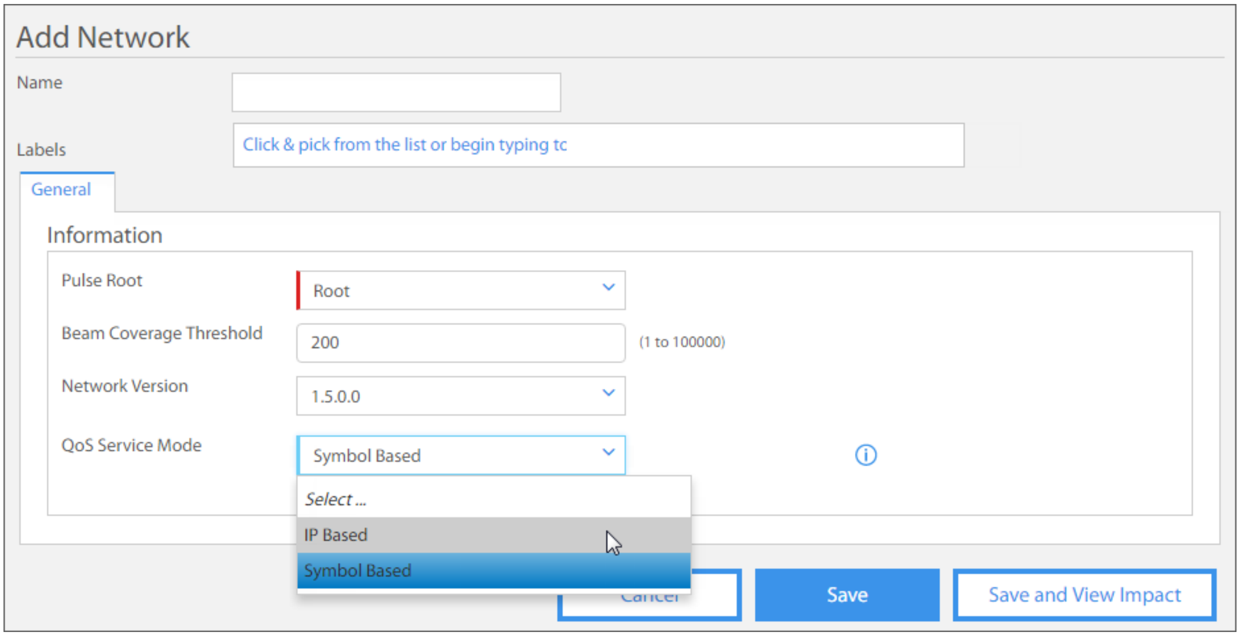
When adding or modifying a network, using the **Add Network** dialog, two parameters must be considered — the **Network Version** and the **QoS Service Mode**. Prior to Velocity Release 1.5, only one QoS Service mode option was available — the Symbol-based mode.

The *Network Version* parameter, specifies the iDirect network version for which the Pulse Web User Interface should be set — for example Velocity 1.5. If the Network Version is not set properly, certain features or configuration fields may not appear. A setting of Version 1.3, for example, would mean that Version 1.5 features and options would not appear in Pulse. An upgrade from Version 1.4 to 1.5 would require that the Network Version be set to 1.5.

The *QoS Service Mode*, determines the service type the network provides in the downstream direction (hubs to terminals). The network service mode options are briefly described below:

- *Symbol Based Mode* — is the original or default QoS service mode, which supports data rates in terms of Mb/s at a nominal MODCOD (equivalent to Symbols or MHz) and is the GBWM implementation for Velocity releases prior to Velocity 1.5.
- *IP Based Mode* — supports Layer-3/IP outbound (hub to remotes) services with CIR/MIR specified in Mbps rate, based on a service region with the existing GSP configuration based on beams. This mode also support QoS Stats reporting in Mbps.

See *iDirect Velocity Technical Reference Guide* for additional details on QoS Service modes.



Add Network

Name

Labels: Click & pick from the list or begin typing tc

General

Information

Pulse Root: Root

Beam Coverage Threshold: 200 (1 to 100000)

Network Version: 1.5.0.0

QoS Service Mode: Symbol Based

Figure 8-1. Add Network

To add a new network:

1. Click the **NMS Management** tab > **NMS Services** > **Add** > **Network.**
2. Type the **Name** of the new Network.
3. Use the **Labels** multi-select field to assign one or more labels to this element, from the list of pre-configured labels.
4. Use the Pulse Root drop-down to specify the root node of this network.
5. Select the appropriate iDirect **Network Version** of this new Network — for example 1.5.0.0, for Velocity Release 1.5. With this selection, the Pulse user interface will reflect the appropriate configuration pages and parameter fields that support the features available in the selected Network Version.
6. In **QoS Service Mode**, select **IP-based** or **Symbol-based**. The IP-based mode supports unicast GSP configuration with CIR/MIR specified in Mbits/second. Changing the QoS service mode will impact how the global bandwidth management is handled.
7. Click **Save** to save the configuration and continue or click **Save and View Impact**.

8.2 Network Browse Actions

Using the **Browse Network** command, users can interact with configured Pulse Networks, to perform a variety of specific operations. These operations are called “actions.” An action can be performed on a single selected Network or simultaneously on several Networks. Network element actions are listed and briefly described as follows:

Table 8-1. Network — Browse Actions

Action	Brief Description
View Network	View configured information for the selected network.
Copy Network	Create a cloned copy of the selected network, which can be modified as required, renamed, and saved as a new network system.
Modify Network	Modify the configuration of the selected network, and re-submit to NMS.
Delete Network	Remove the selected network from the NMS database.
Apply Configuration	Apply configured NMS changes to the selected network, using the pending option file configured for the network.
Progress Report	View a summary report of update manager progress since applying changes to the selected network.
Retrieve Pending Option File	Load from the NMS database, and display the pending copy of the options file for the selected network.
Retrieve Active Option File	Load and display the options file currently active for the selected network.
Compare Configuration	Compare the pending and the active options files for the selected network.
Modify Engineering Debug Keys	Modify custom key associated with a specific feature of the selected network, to enable, disable, add or modify functionality.

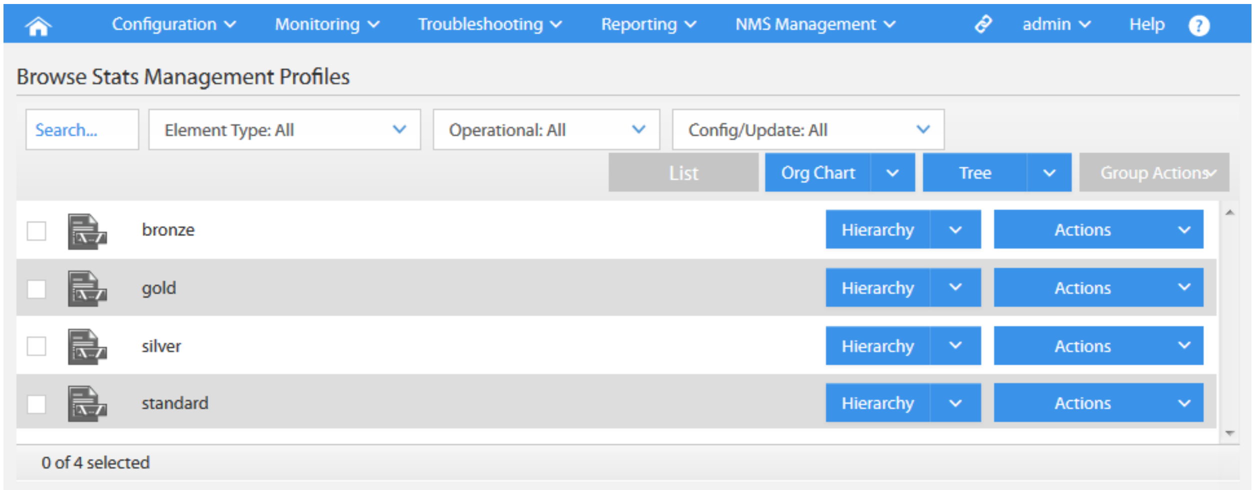
8.3 About Management Profiles

The scale of an iDirect Network, and stringent data storage requirements, warrant a method for managing the collection of real-time and historical network data as well as the queries associated with reporting the collected data. This method must anticipates and manage disk space usage to ensure that data storage and retrieval meets performance requirements and efficiently supports both small and large networks.

Management Profiles, the Pulse data management solution, represent a standardized method of defining how real-time and historical network data are collected and stored. A profile allows users to define, what data are collected and stored, the severity, and in days, the duration for maintaining *real-time data cache*, *real-time data storage*, *historical data cache*, and the *historical data storage* for the collected data. In Pulse there are two types of management profiles.

- *Events management profile* — defines requirements for discrete data including network events, alarms, and incidents.
- *Stats management profile* — defines requirements for the collection of various network element statistics.

On initial deployment, the NMS has four pre-defined Management Profiles — Gold, Silver, Bronze, and Standard. The Gold profile supports the most storage, while the Standard profile supports the least. An individual Management Profile, for example, Bronze, can be manually associated with one or more Terminals at the time the terminal is created or at a later time. Management profiles may be duplicated and modified to create new profiles as required.



Browse Stats Management Profiles

Element Type: All
Operational: All
Config/Update: All

☐ bronze
☐ gold
☐ silver
☐ standard

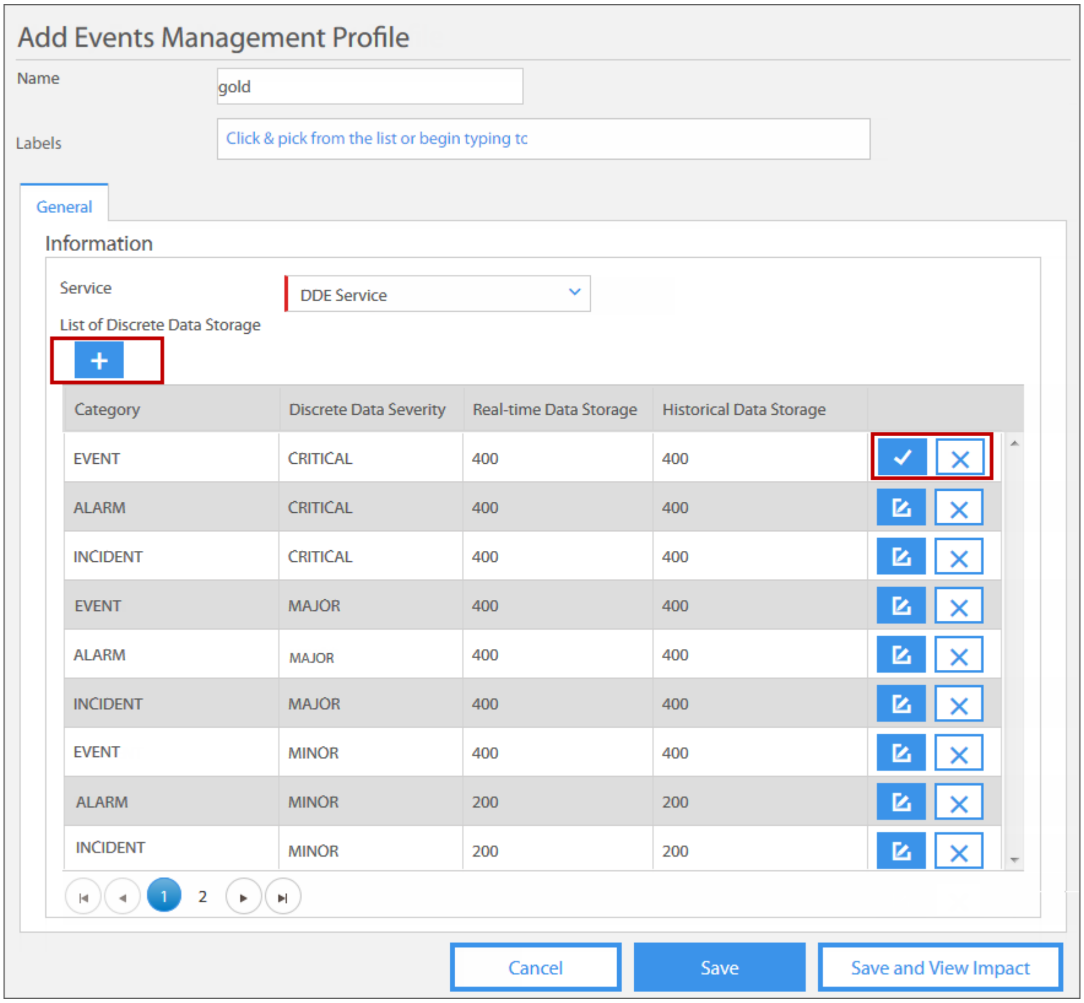
0 of 4 selected

Figure 8-2. Pulse Default Stats Management Profiles

8.4 Adding an Events Management Profile

An *Events Management Profile* is a profile definition of how Pulse discrete data, including events, alarms, and incidents are to be collected, and the duration for which the data is collected. Parameters that are defined include the DDE **Category**, for example, alarm, event, or incident; the **Discrete Data Severity** of the collected events, for example minor, major, or critical; and the duration, in days, for **Real-time Data Storage** and **Historical Data Storage**.

The **Add Events Management Profile** command is accessed directly from the **NMS Management** menu, under **NMS Services**, or from the **Actions** menu of the **DDE Service**, when the service is listed in the **Browse NMS Services** results.



Add Events Management Profile

Name: gold

Labels: Click & pick from the list or begin typing tc

General

Information

Service: DDE Service

List of Discrete Data Storage

Category	Discrete Data Severity	Real-time Data Storage	Historical Data Storage
EVENT	CRITICAL	400	400
ALARM	CRITICAL	400	400
INCIDENT	CRITICAL	400	400
EVENT	MAJOR	400	400
ALARM	MAJOR	400	400
INCIDENT	MAJOR	400	400
EVENT	MINOR	400	400
ALARM	MINOR	200	200
INCIDENT	MINOR	200	200

Figure 8-3. Add Events Management Profile Dialog

To add an Events Management profile:

1. Click the **NMS Management** tab > **NMS Services** >**Add** > **Events Management Profile.**
2. In the **Name** field, enter a name for the new profile - for example “**Platinum**.”

3. Use the **Labels** multi-select field to assign one or more labels to this element, from the list of pre-configured labels.
4. Use the **Service** drop-down list and select **DDE Service** as the type of service.
5. Click the **Add Record** icon to enable the fields of a new **Discrete Data Storage** record for the new profile.
6. Use the **Category** drop-down list and select **Alarm**, **Event**, or **Incident** as the category of the new profile record for how the data will be collected.
7. Use the **Discrete Data Severity** drop-down list and select the level of severity for which data is to be collected. For example, **Informational**, **Warning**, **Major**, or **Critical.**
8. Enter the **Discrete Data Type ID**.
9. Specify the number of days to store **Real-time Data Storag**e and **Historical Data Storag**e.
10. Click the **Update Record** icon to accept the **Discrete Data Storage** record entry.
11. For a given **Discrete Data Storage** record, click the **Edit** icon (pencil in box), to modify the record; click the **Delete** icon, to remove the record.
12. Repeat this procedure, from Step (4), to insert additional discrete data storage records.
13. Click **Save** to save the configuration and continue or click **Save and View Impact**.

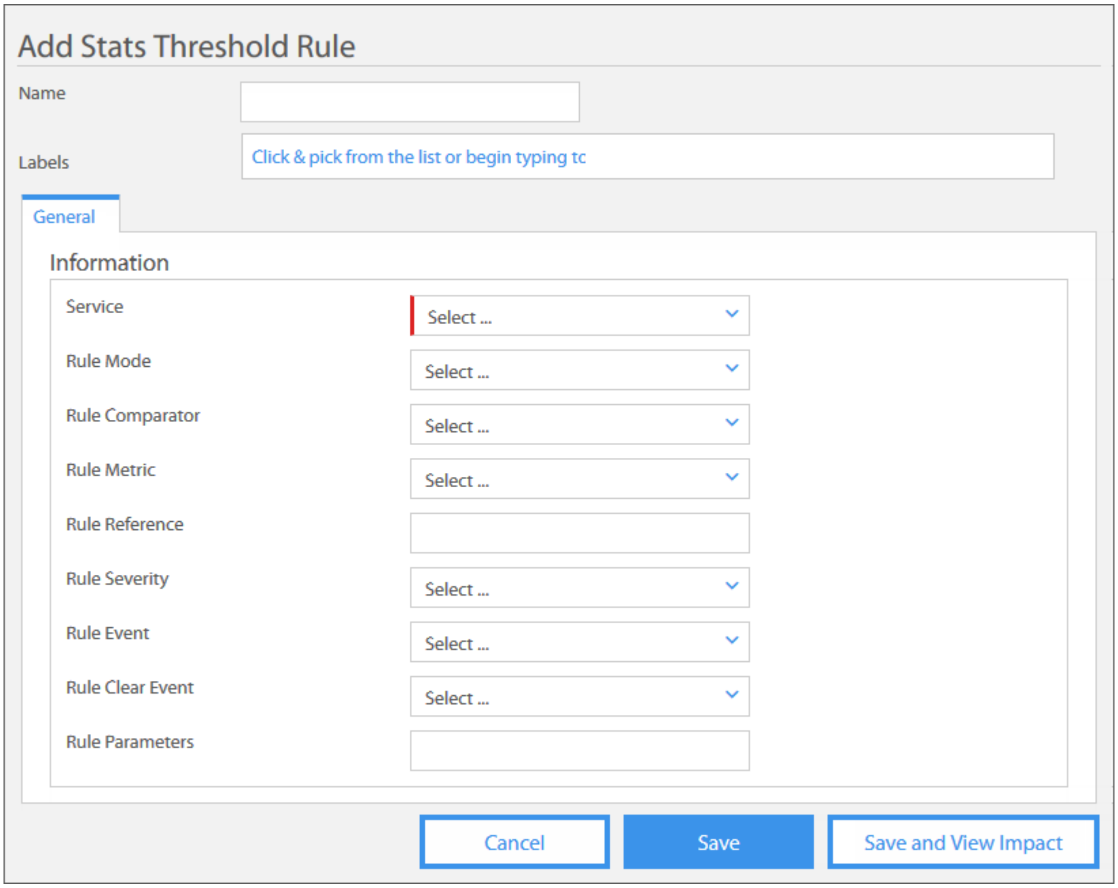
8.5 Adding a Stats Threshold Rule

A *stats threshold rule* is a user-defined rule that is based on a specific network metric, and that generates an event when the rule is met. For example, if latency is > 100 generate event. Several Stats threshold rules are already pre-defined in the NMS.

To add a new Stats Threshold Rule:

1. Click the **NMS Management** tab > **Browse** > **Services**.
2. Locate the **Stats Service**, click the **Actions** menu > **Add Stats Threshold Rule**.
3. Enter a **Name** for the new Stats Threshold Rule.
4. Use the **Labels** multi-select field to assign one or more labels to this element, from the list of pre-configured labels.
5. Select the **Stats Service** option from the **Service** drop-down list.
6. Use the **Rule Mode** drop-down list and select **STATEFUL** or **STATELESS** as the mode. With STATEFUL, the rule is applied and generates the event once when the threshold is crossed; with STATELESS, the rule is applied and generates the event each time the limit is exceeded.
7. Use the **Rule Comparator** drop-down list and select a compare operator to use when this Stats Threshold Rule is applied.
8. Use the **Rule Metric** drop-down list and select a pre-defined network metric to which this threshold rule is to be applied.
9. In **Rule Reference**, enter a threshold value to which the metric will be compared.

10. Use the **Rule Severity** drop-down list to choose a severity to assign to this threshold rule/event when triggered.
11. Use the **Rule Event** drop-down list to choose the event this threshold rule will trigger.
12. Use the **Rule Clear Event** menu to choose the event that clears the rule event.
13. Click **Save** to save the configuration and continue or click **Save and View Impact**.



Add Stats Threshold Rule

Name

Labels: Click & pick from the list or begin typing tc

General

Information

Service: Select ...
Rule Mode: Select ...
Rule Comparator: Select ...
Rule Metric: Select ...
Rule Reference
Rule Severity: Select ...
Rule Event: Select ...
Rule Clear Event: Select ...
Rule Parameters

Figure 8-4. Add Stats Threshold Rule Dialog

8.6 Adding a Stats Threshold Profile

A *stats threshold profile* is a grouping of Stats threshold rules. This profile, once configured, can be applied to a specific element at the time of creation — for example a Stats threshold profile might be defined for line cards or for Satellite Terminals. Several Stats Threshold Rule Profiles are already pre-configured in the NMS. See *Adding a Stats Threshold Rule*.

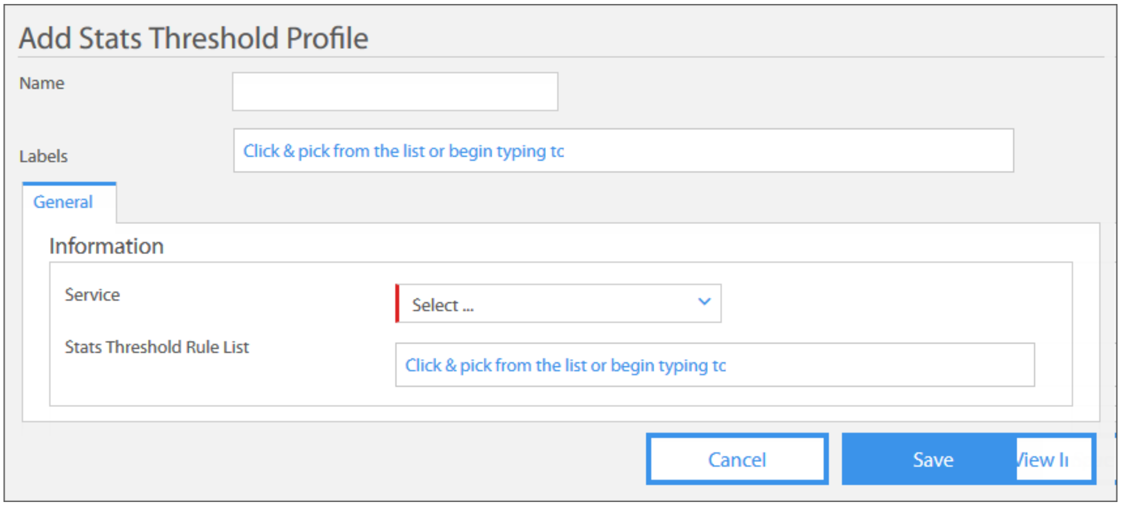

Add Stats Threshold Profile
Name
Labels
Click & pick from the list or begin typing tc
General
Information
Service
Select ...
Stats Threshold Rule List
Click & pick from the list or begin typing tc
Cancel
Save
/iew li

Figure 8-5. Add Stats Threshold Profile Dialog

To add a new Stats Threshold Profile:

1. Click the **NMS Management** tab > **Browse** > **Services**.
2. Locate the **Stats Service** from the list, click the **Actions** menu > **Add Stats Threshold Profile**. The **Add Stats Threshold Profile** dialog opens.
3. In the **Name** field, type a descriptive name for the new Stats threshold profile.
4. Use the **Labels** multi-select field to assign one or more labels to this element, from the list of pre-configured labels.
5. Select the **Stats Service** option from the **Service** drop-down list.
6. Click the **Stats Threshold Rule List** box, and select one or more threshold rules to add to the new Stats threshold profile.
7. Click **Save** to save the configuration and continue or click **Save and View Impact**.

8.7 Adding an Update Rule

Users with permission, can create an *update rule*, in the NMS, to affect how the Pulse Update Manager delivers specific manifest elements, such as blobs, option files, packages, or a license to a target element.

As seen in the **Add Update Rule** dialog, for a given **Manifest Type** (for example — BLOB or Option File), the update rule can specify the **Download Bandwidth**, a **Transaction Timer** that specifies a maximum time to allow for the transaction.

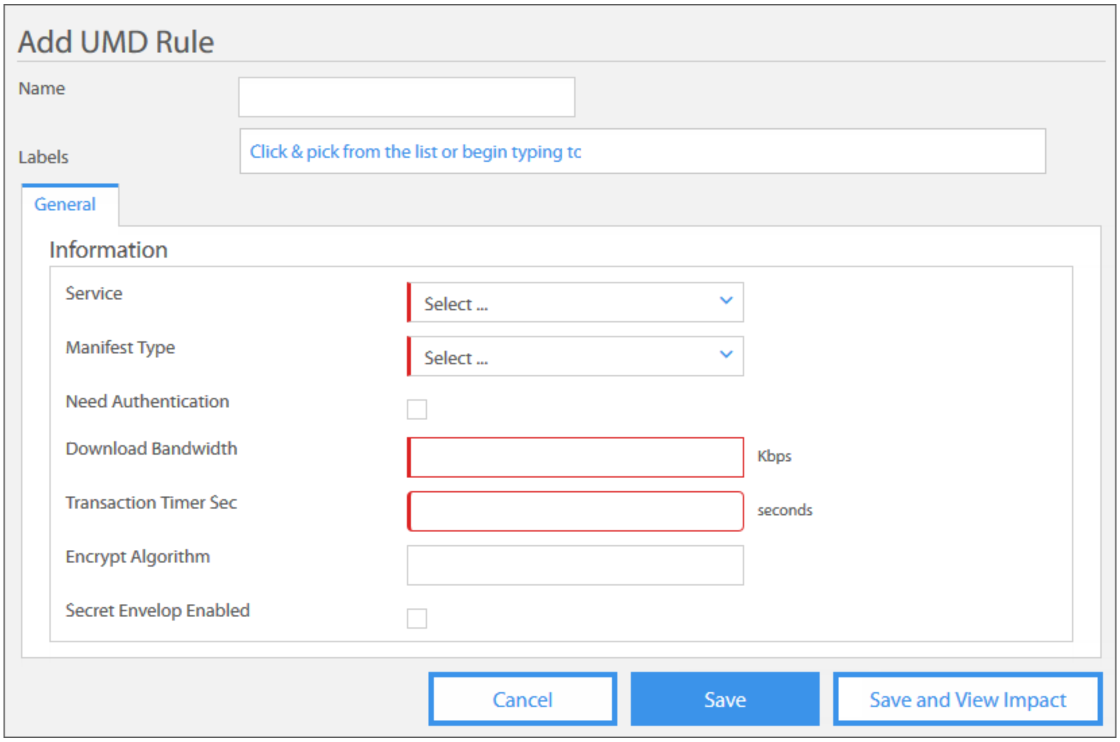


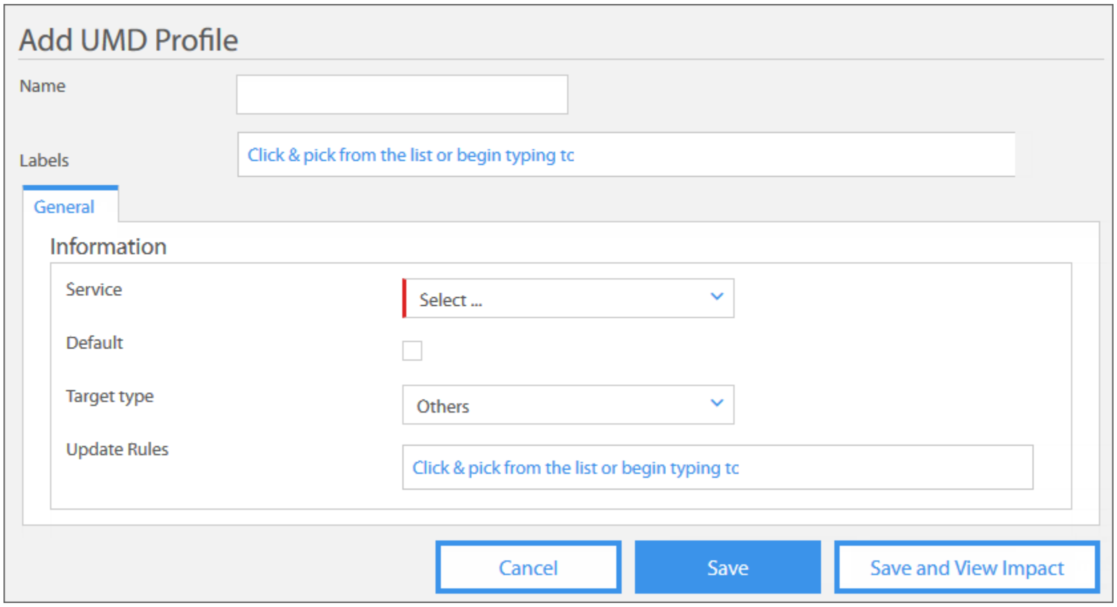
Figure 8-6. Add Update Rule Dialog

To add a new update manage rule:

1. Click the **NMS Management** tab > **Browse** > **Services**.
2. Locate the **Update Manager Service** from the list, click the **Actions** menu > **Add UMD Rule**. The **Add UMD Rule** dialog opens.
3. Enter a **Name** for the new update rule.
4. Use the **Labels** multi-select field to assign one or more labels to this element, from the list of pre-configured labels.
5. Select the **Update Manager** option from the **Service** drop-down list.
6. Select **Authentication** if this update rule requires authentication.
7. Enter **Download Bandwidth** to allocate to the Update Manager when applying this rule.
8. Use **Transaction Timer Sec**, to enter a value, in seconds, to allocate as a watchdog timer for when applying this rule.
9. **Click Save** to save the configuration to the NMS.

8.8 Adding an Update Profile

An *update profile* comprises a list of one or more update rules. Once defined, an update profile, can be applied to a new element as it is being created. In this way, the rules of the update profile are all applied during the delivery of files/packages for the elements to which the update rule is applied.


Add UMD Profile

Name

Labels: Click & pick from the list or begin typing tc

General

Information

Service: Select ...

Default: ☐

Target type: Others

Update Rules: Click & pick from the list or begin typing tc

Figure 8-7. Add Update Profile Dialog

To add a new Update Profile:

1. Click the **NMS Management** tab > **Browse** > **Services**.
2. Locate the **Update Manager** > click the **Actions** menu > **Add Update Profile**.
3. Enter a **Name** for the new update profile.
4. Use the **Labels** multi-select field to assign one or more labels to this element, from the list of pre-configured labels.
5. Select the **Update Manager** option from the **Service** drop-down list.
6. Select **Default** if this update profile should be applied as a default update profile.
7. Use the **Target Type** drop-down list to select the element type targeted by this profile.
8. From the **Update Rules** list box, select one or more of the listed rules to add to this update profile.
9. **Click Save** to save the configuration to the NMS.

8.9 Adding a Scheduled Job

Using the **Add Scheduled Job** command, a network administrator can add a scheduled job to the NMS, to operate on one or more designated servers to perform specific tasks.

The scheduling engine serves as a contact point for administering, performing, and monitoring system level tasks on all NMS servers. The scheduler actively awaits service subscriptions from any NMS server. After successful subscription, all pre-scheduled tasks are activated and transferred to a server’s **CronJob** list.

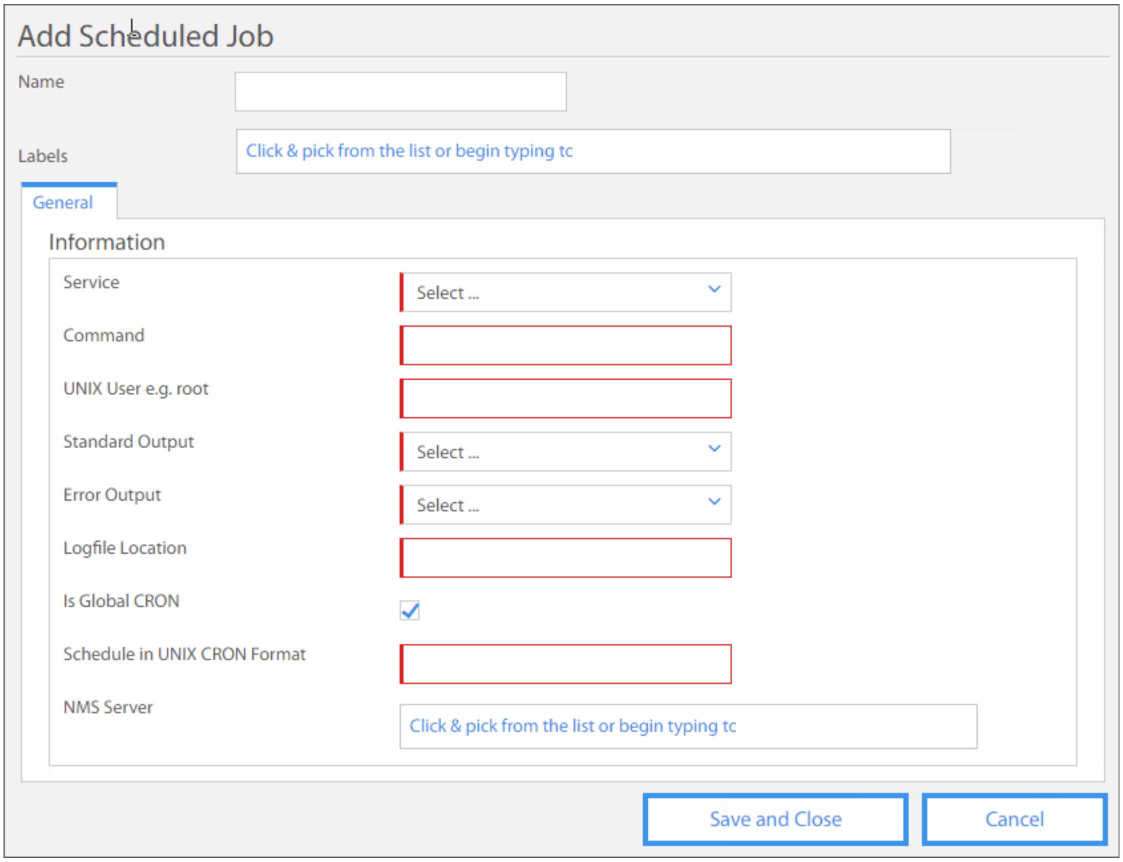


Figure 8-8. Add Scheduled Job Dialog

The **Add Scheduled Job** operation can be accessed directly from the **NMS Management** menu, or from the **Actions** menu of the **Scheduling Service**, using the **Add Cron Job** option.

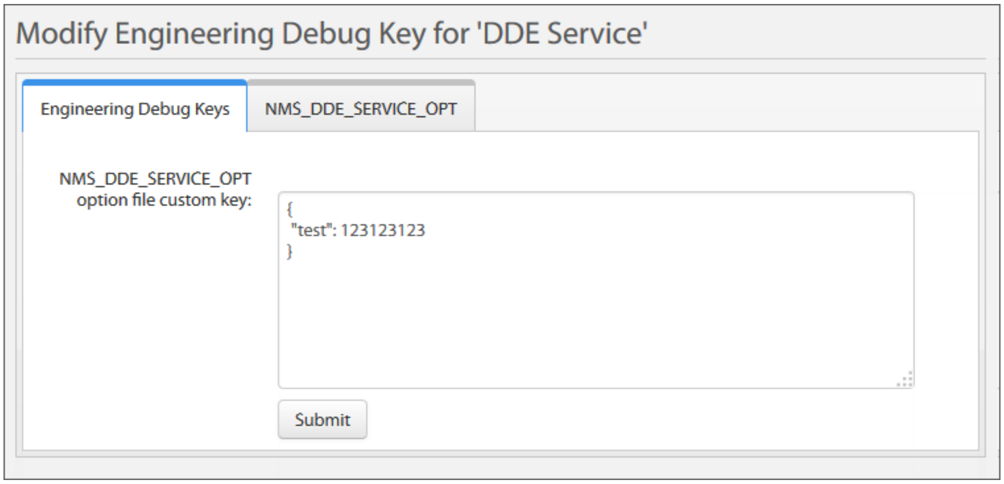
To add a new scheduled job:

1. Click **NMS Management** tab > **NMS Services** > **Add > Scheduled Job**. The **Add Scheduled Job** page is opened.
2. In the **Name** field, type a descriptive name for the new scheduled job.
3. Use the **Labels** multi-select field to assign one or more labels to this element, from the list of pre-configured labels.

4. Select the **Scheduling Service** option from the **Service** drop-down list.
5. In the **Command** field, type a complete command to be executed in the scheduled job.
6. In the **UNIX User** field, specify a valid user who has permission to perform the command.
7. Use the **Standard Output** drop-down list to select an appropriate output type for the scheduled job, to be triggered upon completion of the command.
8. From the **Error Output** drop-down list, select the appropriate output type — for example **Event, E-mail** or **Log** file, in case of an error in the job. The NMS only sends the error output in case of failures that may have resulted in incompletion of the job.
9. In the **LogFile Location** field, specify directory location where the log file is saved, if this output options was selected.
10. Check the **Is Global Cron** option only if this new scheduled job is configured for global operation, meaning that the job will be executed for all NMS servers in the network.
11. From the **NMS Server** selection pane, select one or more NMS servers to target the scheduled job for operation.
12. If E-Mail is specified for the Error Output type, use the **E-mail to Receive Status** field, to enter addresses for those that should be informed of the status of the scheduled job. Multiple comma delimited addresses may be entered.
13. **Click Save and Close** to save the configuration to the NMS database.

8.10 Modifying an NMS Service Config File

When an NMS service element is opened using the **Modify Service Config File** action, the options file for that service is opened. The page displays an **Engineering Debug Keys** tab and one or more associated **Options Files** tabs. The options files are displayed in a view-only mode, since it is an NMS generated file. Debug keys may be added to the **Engineering Debug Keys** tab, and changes are submitted by clicking the **Submit** button.



Modify Engineering Debug Key for 'DDE Service'
Engineering Debug Keys
NMS_DDE_SERVICE_OPT
NMS_DDE_SERVICE_OPT option file custom key:
Submit

```
{
 "test": 123123123
}
```

Figure 8-9. Modifying DDE Service Configuration File

The steps for modifying an NMS Service are shown in the following procedure. The steps are similar for modifying other NMS services where **Modify Service Config File** is an action. Service Config files apply to the DDE Service, Stats Service, and the Update Manager Service.

To modify an NMS service:

1. Click the **NMS Management** tab > **Browse** > **Services**.
2. Select the desired NMS Service. Not all services have **Config Files** that may be modified.
3. Click the **Actions** drop-down menu and select the **Modify Service Config File** action. The **Modify Service Config File** dialog opens, and displays the **Engineering Debug Keys** tab and one or more **Options File** tabs.
4. Click **Options File** to view the options file; click **Engineering Debug Keys** to view, modify, or add custom keys to the configuration for the selected service.
5. Modify entries to the element as required.
6. Click **Submit** to save the modifications to the NMS Service **Engineering Debug Keys** tab, and return to the Browse Results window.

8.11 NMS Services Browse Actions

This section provides an overview of the various actions that can be performed from the Browse window when Network elements or NMS services or security elements are listed.

8.11.1 Browse Actions — CA Foundry Service

The *CA foundry service* creates, renews and, when necessary, revokes X.509 certificates created for communication among hub network elements. The CA foundry also maintains intermediate certificates to sign certificates for each network element.

CA Foundry Service browse actions are listed and briefly described as follows:

Table 8-2. CA Foundry Service Browse Actions

Action	Brief Description
Add Vault	Create a vault to store CA objects that belong to a chain of trust branch. This action is also available from the **NMS Management** tab, under the **Security sub-menu**.
Add CA (Certificate Authority)	Create a certificate authority for a network element. This command is also accessed from the **NMS Management** tab, under the **Security sub-menu.**
Apply Configuration	Apply configured NMS changes to the selected service, using the pending option file for the element.
Impact Analysis	View impact on other elements, if changes are applied to the selected object.
Progress Report	View a summary report of update manager progress since applying changes to the selected object.
Issue Certificate	Issue certificate for a specific network element. This action is also available from the **NMS Management** tab, under the **Security sub-menu.**
Revoke Certificate	For details, see *Revoking a Certificate*.
Download Certificate	For details, see *Downloading a Certificate*.

8.11.2 Browse Actions — Stats Service and DDE Service

When the **Stats Service** or the **DDE Service** is selected in the **Browse NMS Services** list, network administrators can perform the **Actions** menu operations.

Stat service and DDE service actions are listed and briefly described as follows:

Table 8-3. DDE and Stats Services Browse Actions

Action	Brief Description
Add Stats Threshold Rule	Applies to Stats service only. See *Adding a Stats Threshold Rule*
Add Stats Threshold Profile	Applies to the Stats service only. See *Adding a Stats Threshold Profile*
Modify Service Config File	Modify the configuration file for the selected NMS service, by adding or modifying a Custom Key.
Apply Configuration	Apply configured NMS changes to the selected service, using the pending option file for the element.
Impact Analysis	View impact on other elements, if changes are applied to the selected object.
Progress Report	View a summary report of update manager progress since applying changes to the selected object.
Retrieve Pending Option File	Load from the NMS database, and display the pending copy of the options file for the selected element.
Retrieve Active Option File	Load and display the options file currently active in the selected element.
Compare Configurations	Compare the pending options file and the active options file for the selected element.
Add DDE Management Profile	Applies to the DDE service only. Add a new Events Management Profile to the NMS.

8.11.3 Browse Actions — Scheduling and System Monitor

The *scheduling service* is implemented in an iDirect Network system to support the carrying out of various server tasks that must be performed on a routine or other basis. These tasks, which may range from disk cleanup and system status, to file replication, may involve regular maintenance operations as well as performance of system-critical functions.

The *system monitor service* supports NMS functionality that allows administrators to monitor the physical health and status of the NMS and Data Path servers, routers, and switches. System Monitoring provides a number of output forms, including numerical monitoring via charts, high level views of the overall status of network elements, and the ability to run various system tools.

Scheduling and System Monitor service actions are listed and briefly described as follows:

Table 8-4. Scheduling and System Monitor Services Browse Actions

Action	Brief Description
Modify Service Config File	Modify the configuration file for the selected NMS service, by adding or modifying a Custom Key.
Impact Analysis	View impact on other elements, if changes are applied to the selected object.
Progress Report	View a summary report of update manager progress since applying changes to the selected object.
Retrieve Pending Option File	Load from the NMS database, and display the pending copy of the options file for the selected element.
Retrieve Active Option File	Load and display the options file currently active in the selected element.
Compare Configurations	Compare the pending options file and the active options file for the selected element.
Add Scheduled Job	Add a new scheduled job to the NMS. This action only applies to the scheduling service. Also accessed on the **NMS Management** tab, under the **NMS Services.**
Add System Monitor Instance	Configure a monitor instance on a target server. This action only applies to the system monitor service.This action is also accessed on the NMS Management tab, under NMS Services menu.

8.11.4 Browse Actions — Update Manager Service

The *update manager service* delivers configuration information to network elements — for example, option files, software and firmware packages, OS images, and licenses. It queries those elements about configuration status and sends commands to those elements to apply delivered configurations as required.

When the **Update Manager Service** is selected in the **Browse NMS Services** list, network administrators can perform the **Actions** menu operations. Additional **Action** commands, which are also available from the **Actions** menu of the **Update Manager Service**, are described under *Configuration Options Files*.

Update Manager Service actions are listed and briefly described as follows:

Table 8-5. NMS Services — Browse Actions

Action	Brief Description
Add Package	Invoke Import Package command to upload software to the NMS.
Add Update Rule	Configure a new update rule in the NMS. See *Adding an Update Rule*
Add Update Profile	Configure new update profile in the NMS. See *Adding an Update Profile*.
Modify Service Config File	Modify the configuration file for the selected NMS service, by adding or modifying a Custom Key.
Apply Configuration	Apply configured NMS changes to the selected service, using the pending option file for the element.
Impact Analysis	View impact on other elements, if changes are applied to the selected object.
Progress Report	View a summary report of update manager progress since applying changes to the selected object.
Retrieve Pending Option File	Load from the NMS database, and display the pending copy of the options file for the selected element.
Retrieve Active Option File	Load and display the options file currently active in the selected element.
Compare Configurations	Compare the pending options file and the active options file for the selected element.

9 NMS Element Security Management

This chapter is the second of three chapters that cover Pulse System Administration operations. Whereas the previous User Administration chapter introduced operations that manage user access to the iDirect Network, this chapter describes those operations concerned with the security and operations management of the physical and logical infrastructure elements that make up the iDirect Network system.

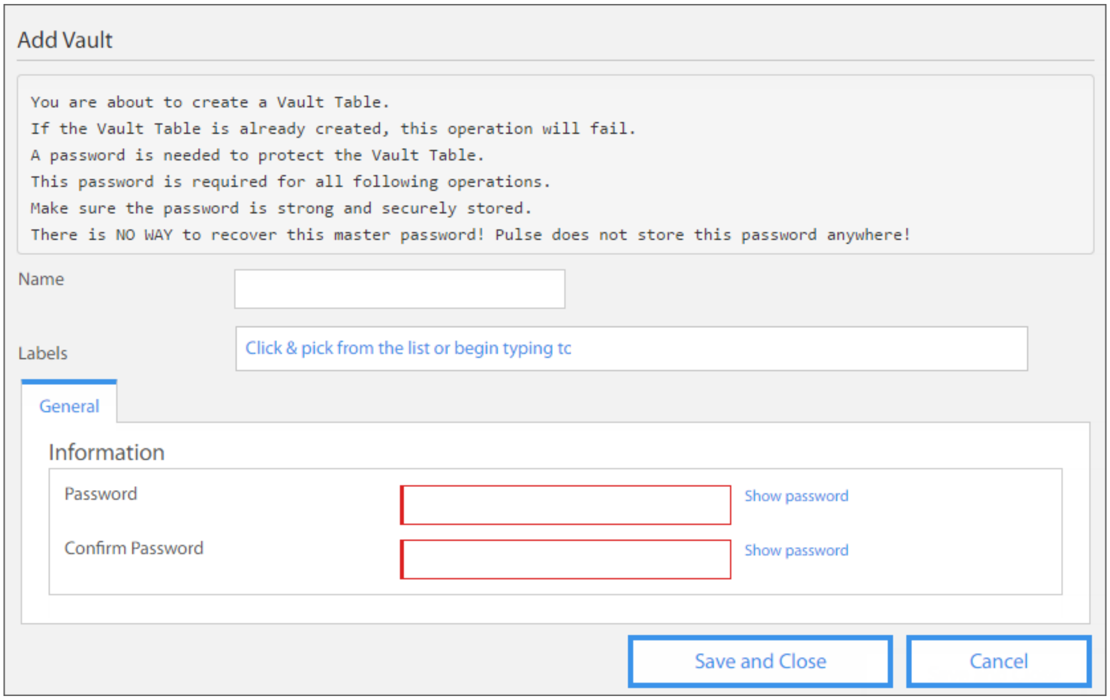
Pulse NMS management associated with element security is covered in the following topics:

- *Adding a Vault Table* on page 116
- *Adding a Certificate Authority* on page 122
- *Issuing a Certificate* on page 124
- *Downloading Global PKI Data* on page 126
- *Locking a Vault Table* on page 118
- *Unlocking a Vault Table* on page 119
- *Setting a Vault as Default* on page 117
- *Rolling a Vault Table* on page 120
- *Migrating a Vault Table* on page 121
- *Deleting a Vault Table* on page 122
- *Revoking a Certificate* on page 127
- *Downloading a Certificate* on page 128
- *Managing Terminal Authentication* on page 129
- *Security Elements Browse Actions* on page 131

9.1 Adding a Vault Table

Using the **Add Vault Table** command, administrators can create a new security vault in the NMS. A *vault table* stores a set of AES keys, used to encrypt all certificate authority (CA) private keys that are associated with the same chain of trust branch. This table allows better CA management and control in an iDirect Network.

The **Add Vault Table** command can be accessed directly from the **NMS Management** menu, under **Security**, or from the **Actions** menu of the **CA Foundry** service when listed in the **Browse NMS Services** results.



Add Vault

```
You are about to create a Vault Table.
If the Vault Table is already created, this operation will fail.
A password is needed to protect the Vault Table.
This password is required for all following operations.
Make sure the password is strong and securely stored.
There is NO WAY to recover this master password! Pulse does not store this password anywhere!
```

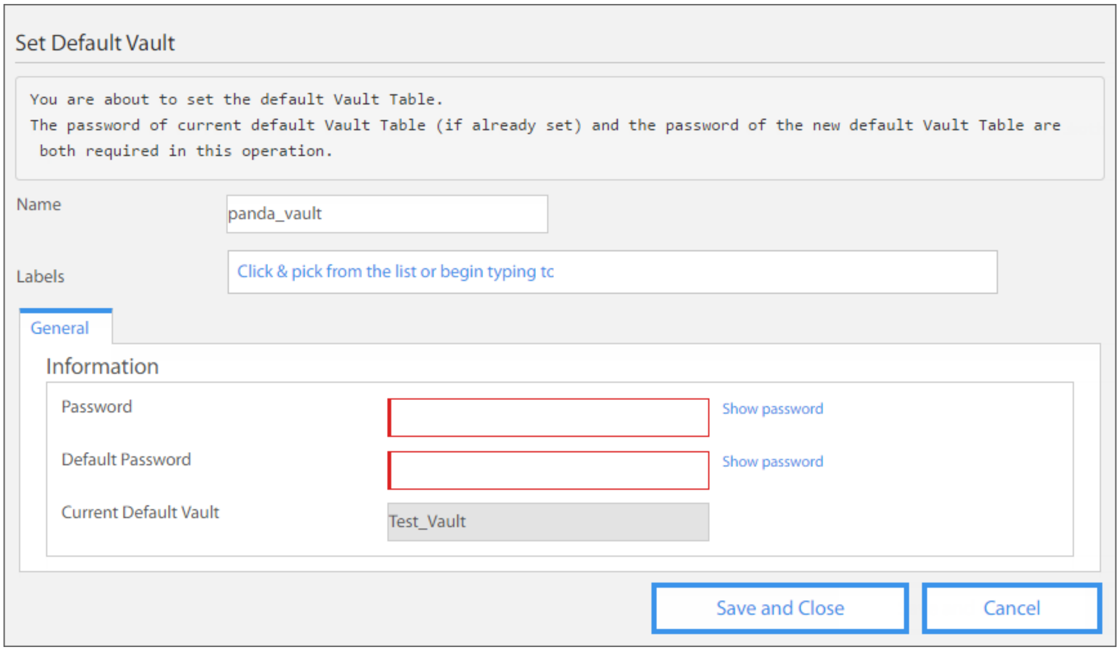
Figure 9-1. Add Vault Table Dialog

To create a vault table:

1. Click **NMS Management** tab > **Security** > **Add > Vault Table**. The **Add Vault** dialog opens.
2. Enter a name for the new vault in the **Name** field.
3. Use the **Labels** multi-select field to assign one or more labels to this element, from the list of pre-configured labels.
4. Enter a password using a minimum of 14 characters in the **Password** field.
5. Re-enter the encrypted password in the **Confirm Password** field. Be sure to save the password in a secure location. Since the password is not stored anywhere in the iDirect system, it is NOT recoverable if lost.
6. **Click Save and Close** to save the vault to the NMS and open the **Browse Security Elements** window. The new vault is unlocked and ready for use. See *Setting a Vault as Default* on page 117.

9.2 Setting a Vault as Default

The **Set Default** command, is accessed from the **Actions** command options of a selected vault, and is used to make the vault table the new default vault to which all new certificates are assigned. Only one vault table can be set as the default vault. To complete this operation, the password of the current default vault (if already set) and the password of the new default vault table are both required.



You are about to set the default Vault Table.
The password of current default Vault Table (if already set) and the password of the new default Vault Table are both required in this operation.

Name: panda_vault

Labels: Click & pick from the list or begin typing tc

Password:

Default Password:

Current Default Vault: Test_Vault

Figure 9-2. Set Vault Table Default Dialog

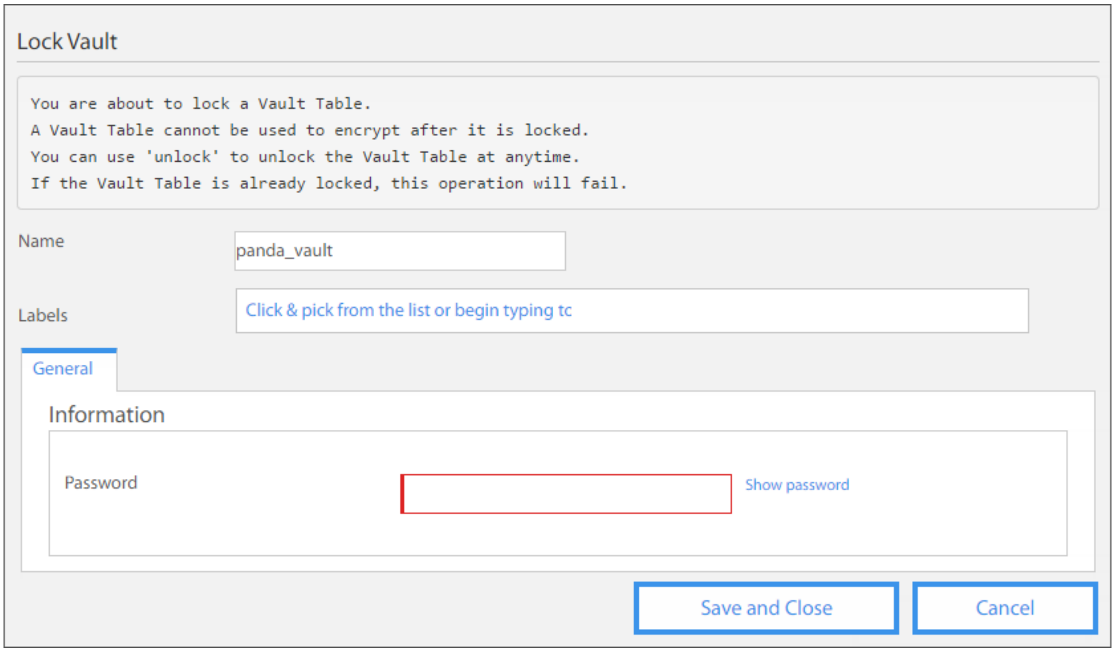
To set a vault table to default:

1. Click the **NMS Management** tab > **Security** > **Browse Security Elements**.
2. Use the **Element Type** drop-down list and select **Vault**, to show vault tables only.
3. Find and select the vault table element to set as the new default vault.
4. Click the **Actions** button and select **Set Default**. The **Set Default Vault** dialog opens.
5. Use **Password**, to enter the password of the current default vault.
6. Use the **Default Password** field, enter a password for the new default vault.
7. Click **Save and Close**. This operation will fail if the current **Default Password** is incorrect.

NOTE: The default vault must be unlocked prior to issuing certificates.

9.3 Locking a Vault Table

Applying the **Lock** command to a vault table, prevents access to the vault by any user. Until a locked vault is unlocked a certificate stored in that vault cannot be issued to a network element. Use the following steps to lock a vault.



```
You are about to lock a Vault Table.
A Vault Table cannot be used to encrypt after it is locked.
You can use 'unlock' to unlock the Vault Table at anytime.
If the Vault Table is already locked, this operation will fail.
```

Name: panda_vault

Labels: Click & pick from the list or begin typing tc

Password:

Figure 9-3. Lock Vault Table Dialog

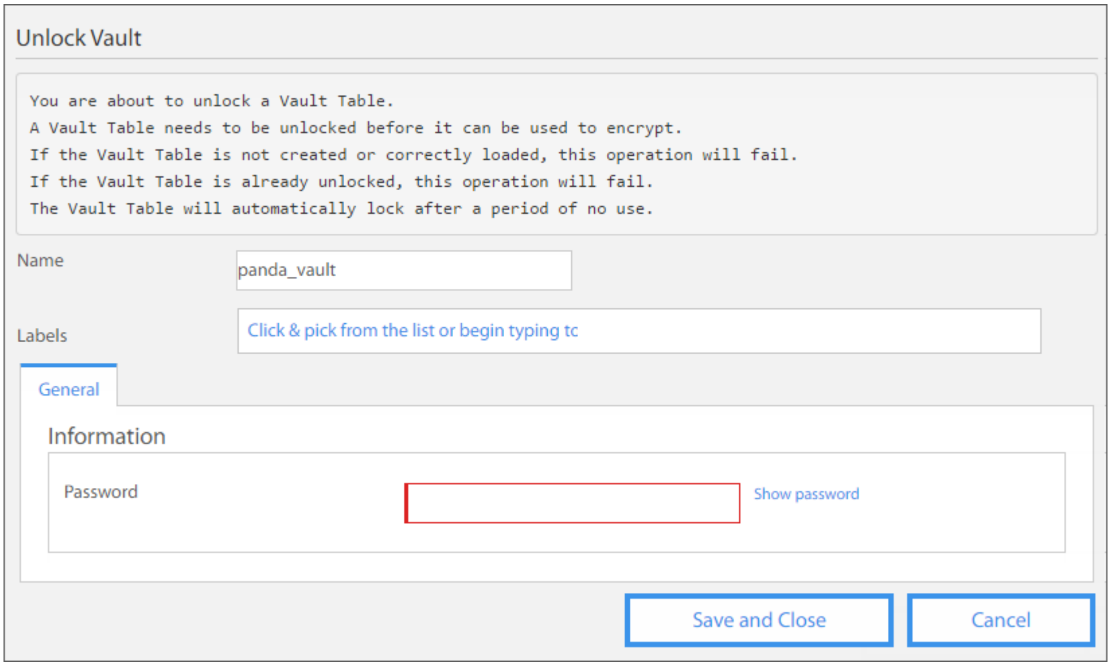
To lock a vault table:

1. Click the **NMS Management** tab > **Security** > **Browse Security Elements**.
2. Use the **Element Type** drop-down list and select **Vault**, to show vault tables only.
3. Find and select the desired vault table element.
4. Click the **Actions** button and select **Lock**. The **Lock Vault Table** dialog is opened.
5. In the **Password** field, enter the password using a minimum of 14 characters.
6. **Click Save and Close** to complete the lock vault process in the NMS, and open the **Browse Security Elements** window. This operation fails if the vault is already locked. See *Unlocking a Vault Table* on page 119.

NOTE: The vault must be unlocked prior to issuing certificates to any elements.

9.4 Unlocking a Vault Table

The **Unlock** command is used to gain access to a previously locked vault. Prior to issuing a certificate to any network elements, the vault where certificate are stored must be unlocked.



Unlock Vault

```
You are about to unlock a Vault Table.
A Vault Table needs to be unlocked before it can be used to encrypt.
If the Vault Table is not created or correctly loaded, this operation will fail.
If the Vault Table is already unlocked, this operation will fail.
The Vault Table will automatically lock after a period of no use.
```

Name: panda_vault

Labels: Click & pick from the list or begin typing tc

Figure 9-4. Unlock Vault Table Dialog

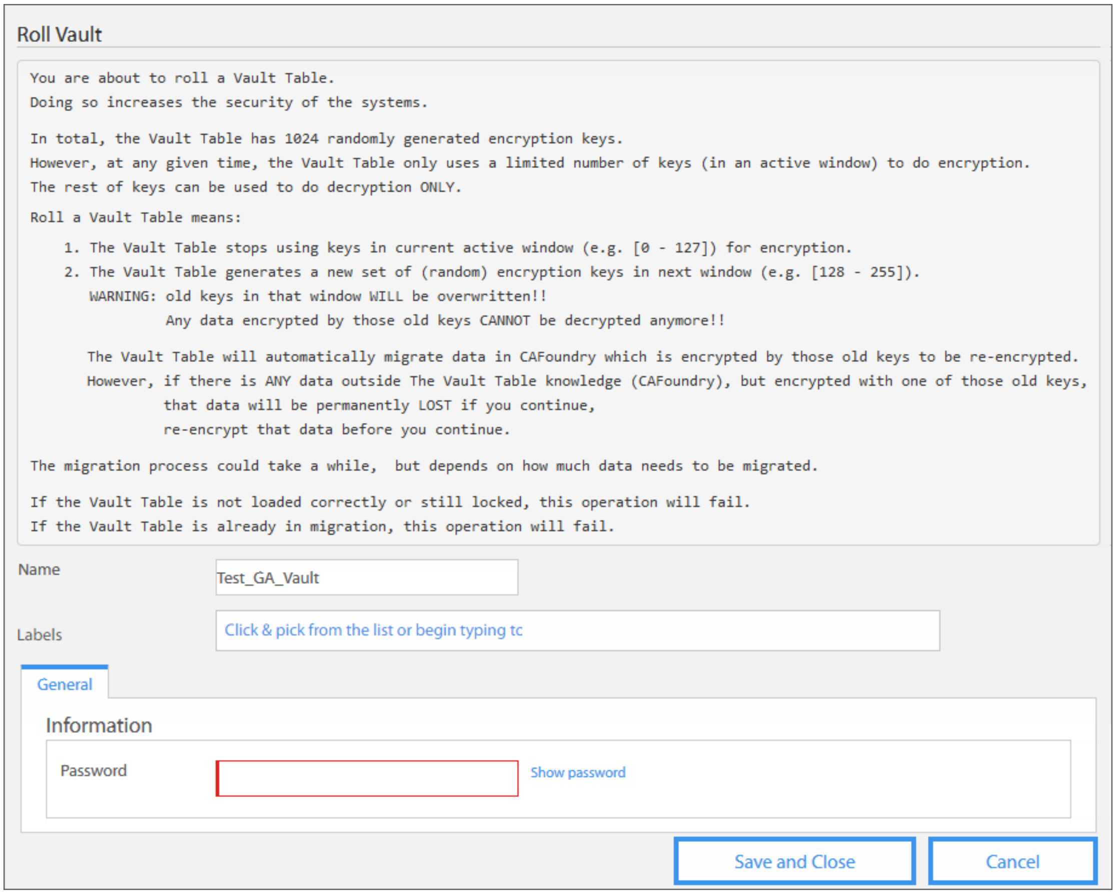
To unlock a vault table:

1. Click the **NMS Management** tab > **Security** > **Browse Security Elements**.
2. Use the **Element Type** drop-down list and select **Vault**, to show vault tables only.
3. Find and select the desired vault table element.
4. Click the **Actions** button and select **Unlock**. The **Unlock Vault Table** dialog is opened.
5. In the **Password** field, enter the required 14 character password.
6. **Click Save and Close** to complete the unlock vault process in the NMS, and open the **Browse Security Elements** window. The operation fails if the vault is already unlocked.

9.5 Rolling a Vault Table

The **Roll Vault** command is accessed from the **Actions** command options of a selected vault. The *roll vault* action is mainly used to increase security of the network by requesting that the vault table cease using the existing keys and generate a new set of keys for data encryption.

In normal operations, the vault table is designed to store 1024 randomly generated encryption keys. At any given time, the vault uses a limited set of keys (in active window) for encryption, and the remainder of the randomly generated keys may be used for data decryption. Rolling a vault is to stop the vault table from using existing keys in the active window.



```
You are about to roll a Vault Table.
Doing so increases the security of the systems.

In total, the Vault Table has 1024 randomly generated encryption keys.
However, at any given time, the Vault Table only uses a limited number of keys (in an active window) to do encryption.
The rest of keys can be used to do decryption ONLY.

Roll a Vault Table means:

    1. The Vault Table stops using keys in current active window (e.g. [0 - 127]) for encryption.
    2. The Vault Table generates a new set of (random) encryption keys in next window (e.g. [128 - 255]).
       WARNING: old keys in that window WILL be overwritten!!
                Any data encrypted by those old keys CANNOT be decrypted anymore!!

       The Vault Table will automatically migrate data in CAFoundry which is encrypted by those old keys to be re-encrypted.
       However, if there is ANY data outside The Vault Table knowledge (CAFoundry), but encrypted with one of those old keys,
                that data will be permanently LOST if you continue,
                re-encrypt that data before you continue.

The migration process could take a while,  but depends on how much data needs to be migrated.

If the Vault Table is not loaded correctly or still locked, this operation will fail.
If the Vault Table is already in migration, this operation will fail.
```

Name: Test_GA_Vault

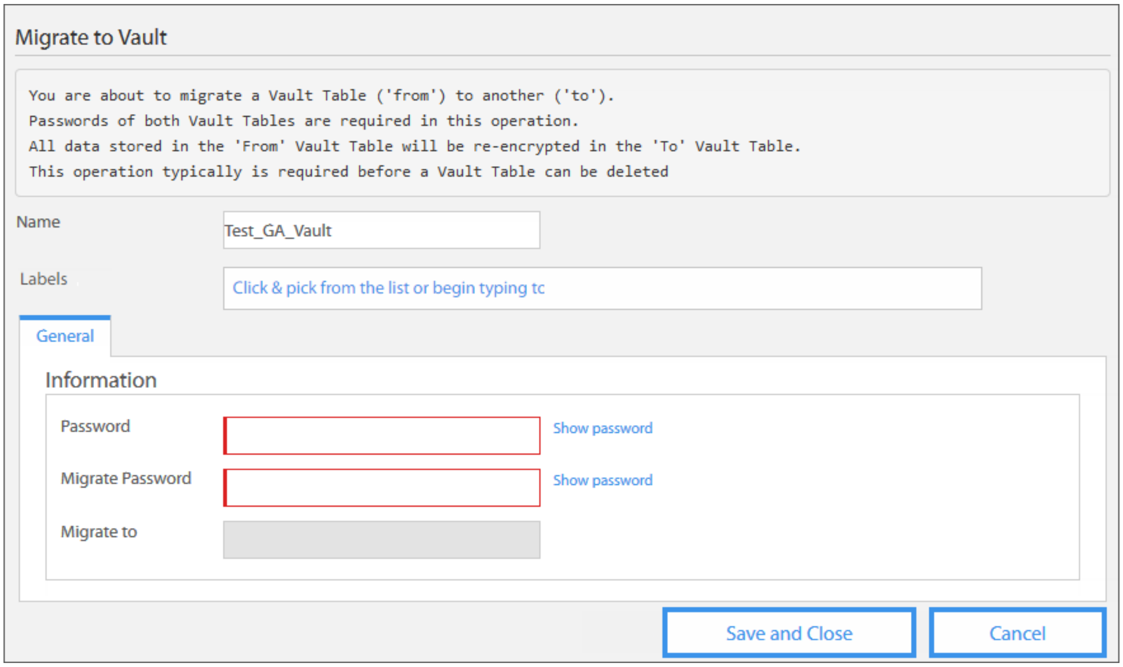
Figure 9-5. Roll Vault Table Dialog

To roll a vault table:

1. Click the **NMS Management** tab > **Security** > **Browse Security Elements**.
2. Use the **Element Type** drop-down list and select **Vault** to show vault tables only.
3. Locate the desired vault table, click **Actions** and choose the **Roll** option. The **Roll Vault Table** dialog is opened.
4. Enter the vault table **Password**.
5. Click **Save and Close** to complete the **Roll Vault** action.

9.6 Migrating a Vault Table

The **Migrate To Vault** command, is accessed from the **Actions** command options of the selected vault table. The *migrate* action results in all data of the selected vault being moved to another vault table. This function is useful in protecting the encrypted data prior to deleting a vault table.



```
You are about to migrate a Vault Table ('from') to another ('to').
Passwords of both Vault Tables are required in this operation.
All data stored in the 'From' Vault Table will be re-encrypted in the 'To' Vault Table.
This operation typically is required before a Vault Table can be deleted
```

Name: Test_GA_Vault

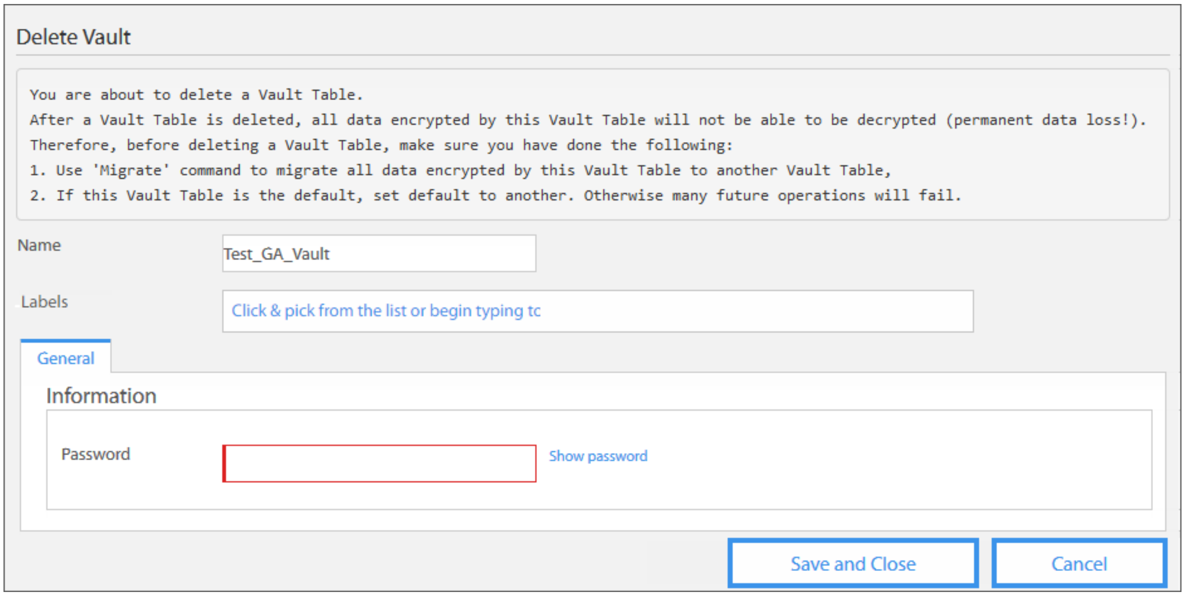
Figure 9-6. Migrate to Vault Dialog

To migrate a vault table:

1. Click the **NMS Management** tab > **Security** > **Browse Security Elements**.
2. Use the **Element Type** drop-down list and select **Vault** to show vault tables only.
3. Locate the vault table to be migrated, click the **Actions** command, and choose the **Migrate To** option to open the **Migrate to Vault** dialog.
4. Enter the **Password** for the vault table from which the encrypted data will be migrated.
5. Enter the **Migrate Password** for the vault table to which the encrypted data will migrate.
6. Click **Save and Close** to complete the **Migrate To Vault** action.

9.7 Deleting a Vault Table

The **Delete Vault** command, is accessed from the **Actions** command options of a selected vault table. The *delete* action results in the removal of the vault from the NMS.



```
You are about to delete a Vault Table.
After a Vault Table is deleted, all data encrypted by this Vault Table will not be able to be decrypted (permanent data loss!).
Therefore, before deleting a Vault Table, make sure you have done the following:
1. Use 'Migrate' command to migrate all data encrypted by this Vault Table to another Vault Table,
2. If this Vault Table is the default, set default to another. Otherwise many future operations will fail.
```

Name: Test_GA_Vault

Figure 9-7. Delete Vault Dialog

CAUTION: Deleting a vault table results in the permanent loss of all encrypted data belonging to the vault. Migration of the existing encrypted data of a vault to a new vault is recommended prior to deleting the vault.

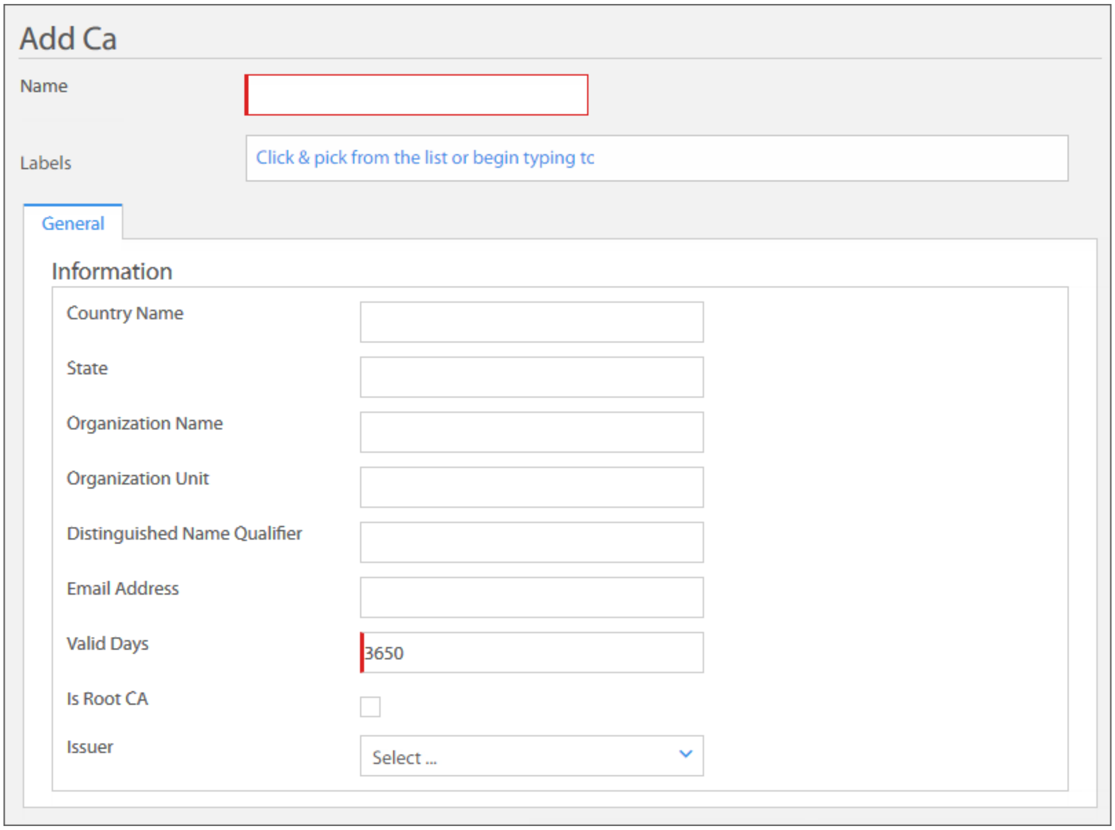
To delete a vault table:

1. Click the **NMS Management** tab > **Security** > **Browse Security Elements**.
2. Use the **Element Type** drop-down list and select **Vault** to show vault tables only.
3. Locate the vault table to be deleted, click the **Actions** command, and choose **Delete** to open the **Delete Vault** dialog.
4. Enter the **Password** of the vault table to be deleted.
5. Click **Save and Close** to confirm the **Delete Vault** action.

9.8 Adding a Certificate Authority

A *Certificate Authority (CA)* is the certificate issuing authority for any applications or network elements that require a certificate in the iDirect Network. There are two types of CA — a *Root CA* and a *registration authority (RA)*. The Root CA is used specifically to create RAs, and an RA is used to create certificates. Using the **Add Certificate Authority** command, administrators can create a new certificate authority in the NMS.

The **Add Certificate Authority** command is accessed directly from the **NMS Management** menu, under **Security**; or from the **Actions** menu of the **CA Foundry** service, using **Add CA**, when listed in the **Browse NMS Services** results.



Add Ca

Name

Labels: Click & pick from the list or begin typing tc

General

Information

Country Name

State

Organization Name

Organization Unit

Distinguished Name Qualifier

Email Address

Valid Days: 3650

Is Root CA ☐

Issuer: Select ...

Figure 9-8. Add Certificate Authority Dialog

To create a certificate authority:

1. First, ensure that the vault is unlocked, before attempting to add a new CA.
2. Click **NMS Management** > **Security** > **Add > Certificate Authority** to open **Add CA** dialog.
3. In the **Name** field, enter a descriptive name for the new certificate authority.
4. Enter a **Country Name**, a **State or Province Name**, an **Organization Name**, an **Organization Unit Name,** a **Distinguished Name Qualifier,** and an **E-mail Address**. These fields are optional and may be blank if no information is available or required.
5. Use the default entry for **Valid Days** or enter a duration for the new certificate authority.
6. Enable the **ROOT Certificate Authority** check box only if the new CA entry is to be classified as a Root CA. This option is not be enabled when creating an RA.
7. If not a root CA, use the **Issuer** drop-down to select the CA issuer of the new CA.
8. **Click Save and Close** to save the new **Certificate Authority** (CA) to the NMS database.

9.9 Issuing a Certificate

A *certificate*, created by the CA Foundry, is required by all iDirect Network elements in the PKI system, in order to communicate with one another. It is important to note that only those network elements with certificates originated from the same Root CA can trust and communicate with one another. Using the **Issue Certificate** command, administrators can provide a specific network element with the required certificate.

The **Issue Certificate** command is accessed directly from the **NMS Management** menu, under the **Security** sub-menu; or from the **Actions** menu of an appropriate network element selected from the Browse Elements list. For example, the **Issue Certificate** operation can be accessed from the **Actions** menu of a Line Card, PP Server, or NMS Server.

In some cases, depending on the target type, there is an option to select “All” elements of the target type and simultaneously issue certificates to all of the associated elements. In such cases, this is the preferred option as opposed to issuing individual certificates.

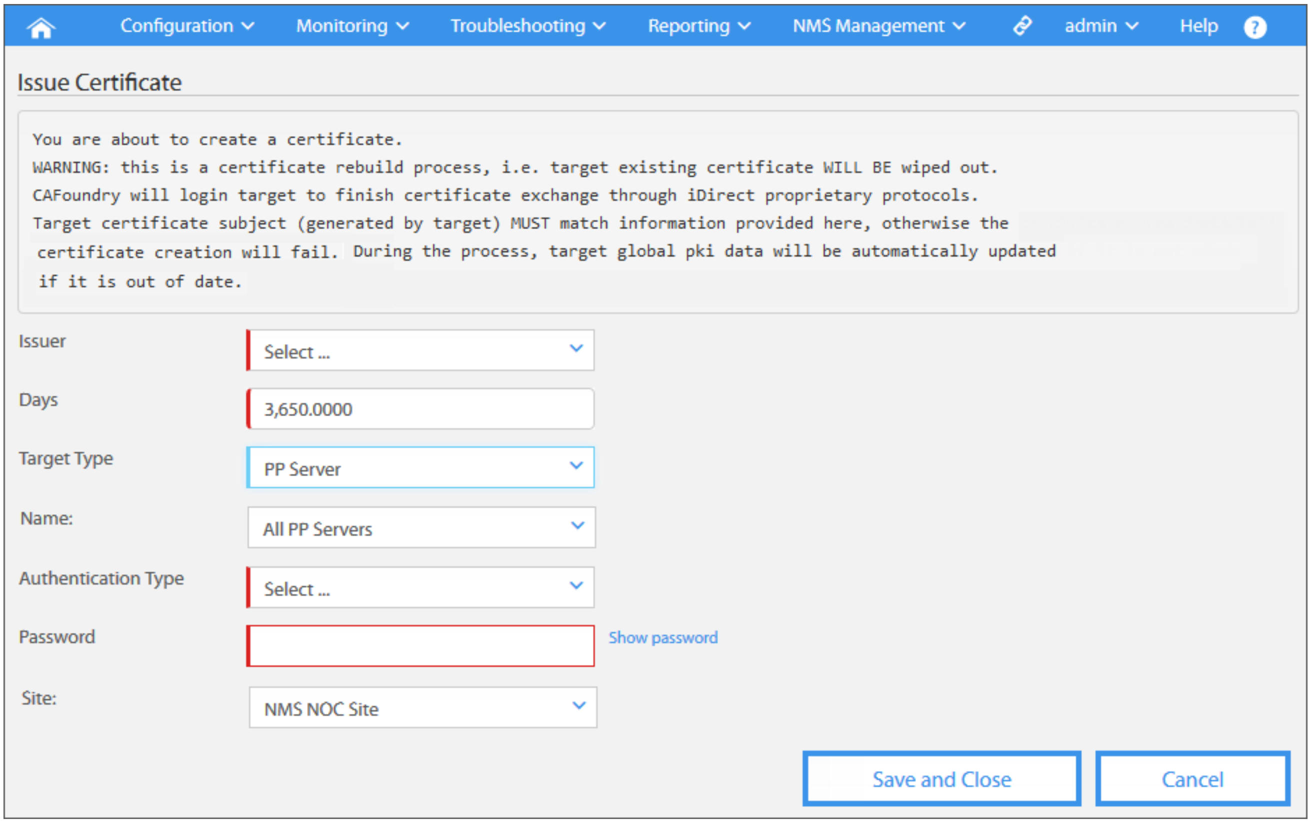
NOTE: Prior to issuing a certificate, first the appropriate certificate vault must be unlocked; and then the certificate authority (CA) must be unlocked. See *Unlocking a Vault Table*.

The following are some important guidelines for consideration when issuing certificates:

1. The objects listed in the **Name** dropdown field are not filtered based on the selection in the Site dropdown field.
2. When “**All** …” is selected from the **Name** drop down field:
   a. **NMS Server** and **PP Server** Target Types should successfully issue certificates to all objects listed in the **Name** field, regardless of the selected Site. For example, for Target Type PP Server, all PP servers are issued certificates, regardless of of the Site.
   b. All other **Target Types**, for example Line Cards, should successfully issue certificates only to the objects listed in the **Name** field which belong to the selected Site.

      For example, if “All Services” is selected for the SAS site, then certificates will be sucessfully issued to all services that run on the SAS - a failure to issue certificate message is presented for each service that does not run on the SAS.
3. After issuing certificates, review the success and failure messages to ensure that all intended objects for a selected Site successfully received certificates.
   a. If objects that belong to the selected Site failed, investigate what is happening with the failed object(s) and/or the selected Site.
   b. If objects that belong to a Site other than the selected Site failed, re-issue certificates with the correct Site selected.

NOTE: Where it is applicable, for example with NMS Service as the Target Type, certificates must be issued to “All” elements of each Site (SAS, NOC, EAP).



Issue Certificate

```
You are about to create a certificate.
WARNING: this is a certificate rebuild process, i.e. target existing certificate WILL BE wiped out.
CAFoundry will login target to finish certificate exchange through iDirect proprietary protocols.
Target certificate subject (generated by target) MUST match information provided here, otherwise the
certificate creation will fail. During the process, target global pki data will be automatically updated
if it is out of date.
```

Issuer: Select ...

Days: 3,650.0000

Target Type: PP Server

Name: All PP Servers

Authentication Type: Select ...

Password:

Site: NMS NOC Site

Figure 9-9. Issue Certificate Dialog

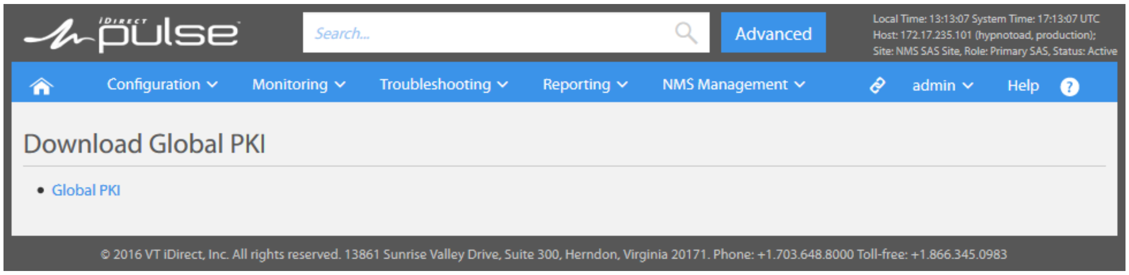
To issue a certificate:

1. Click the **NMS Management** tab > and under **Security > More Options > Issue Certificate**. The **Issue Certificate** dialog is opened.
2. Use the **Issuer** drop-down list, and select the issuing Certificate Authority.
3. In the **Days** field, enter a duration for the certificate or use the default value.
4. Use the **Target Type** drop-down list to select a target element type for which a certificate will be issued. For example, **Line Card, NMS Server, NMS Service**, **PP Server**.
5. Use the **Name** field drop-down list, and select a specific element for which the certificate is being issued; or select "All..." elements to issue certificates to all of the elements of the Target Type. **Note**: If applicable, ensure that the correct **Site**,is selected.
6. Use the **Authentication Type** drop-down list and select **Password** as the method of authentication for the certificate to be issued.
7. Enter a **Password** in the associated field.
8. Select the **Site** of the element for which this certificate is being issued.
9. **Click Save and Close** to save the new **Certificate Authority** (CA) to the NMS database and open the **Browse Security Elements** window.

9.10 Downloading Global PKI Data

The *Public Key Infrastructure (PKI) data file*, of the hub network elements, represents the chain of trust required by network elements to facilitate inter-communication. This PKI data file, which is maintained by the CA Foundry, is integrated with the configuration system. The Global PKI data includes the root x509 certificate and all other signing node certificates, as well as those certificates that have been revoked.

In the case of adding or replacing a line card, a server (PP, NMS, or Squid), and when commissioning a new Satellite Terminal, the Global PKI data file must be manually downloaded and transferred to these elements before they can acquire into the network.



Local Time: 13:13:07 System Time: 17:13:07 UTC
Host: 172.17.235.101 (hypnotoad, production);
Site: NMS SAS Site, Role: Primary SAS, Status: Active

Download Global PKI

- Global PKI

© 2016 VT iDirect, Inc. All rights reserved. 13861 Sunrise Valley Drive, Suite 300, Herndon, Virginia 20171. Phone: +1.703.648.8000 Toll-free: +1.866.345.0983

To download Global PKI data:

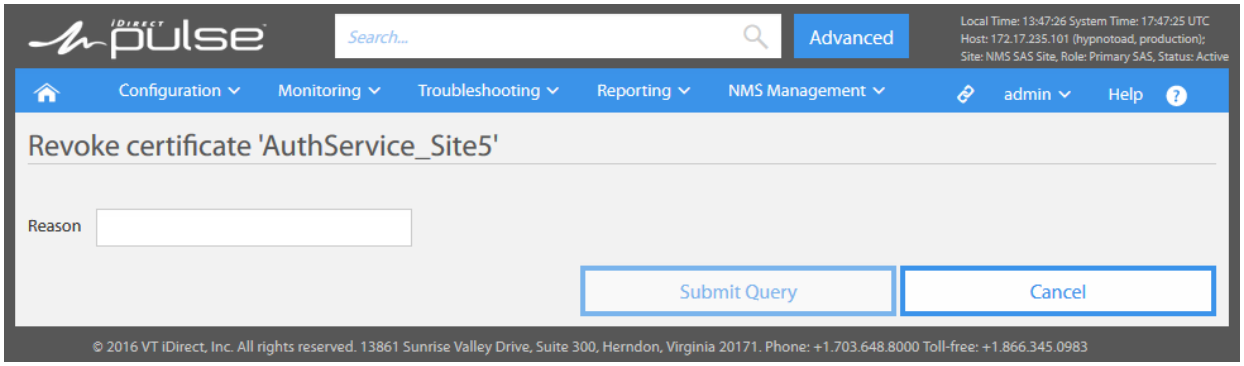
1. Click the **NMS Management** tab > **Security > More Options > Download Global PKI Data**.
2. Click the **Global PKI** link. A dialog is opened to allow the Global PKI Data file to be downloaded and saved.
3. Choose the **Save** option, and click **OK**. The file is saved to the local PC **Download** folder.

Once the Global PKI data file is downloaded to the local PC/laptop, it can be used to transfer to either a Line Card, a PP, NMS or Squid Server, or to a Satellite Router.

9.11 Revoking a Certificate

The **Revoke Certificate** operation, is accessed from the **Actions** menu of a selected certificate in the **Browse Security Elements** list, or from the **Actions** menu of a physical or logical infrastructure element when the element is displayed in a **Browse** window.

The *revoke certificate* action results in the retraction of a security certificate that was previously assigned to a network element.


iDIRECT pulse
Search...
Advanced
Local Time: 13:47:26 System Time: 17:47:25 UTC
Host: 172.17.235.101 (hypnotoad, production);
Site: NMS SAS Site, Role: Primary SAS, Status: Active
Configuration
Monitoring
Troubleshooting
Reporting
NMS Management
admin
Help
Submit Query
Cancel
© 2016 VT iDirect, Inc. All rights reserved. 13861 Sunrise Valley Drive, Suite 300, Herndon, Virginia 20171. Phone: +1.703.648.8000 Toll-free: +1.866.345.0983

Revoke certificate 'AuthService_Site5'

Reason

Figure 9-10. Revoke Certificate Dialog

To revoke a certificate:

1. Use the **Browse Security Elements** command to list the configured security elements.
2. Use the **Element Type** drop-down list to filter the list to show **Certificates** only.
3. Locate the certificate to be revoked, click the **Actions** command, and choose **Revoke Certificate** to open the **Revoke Certificate** page.
4. Optionally, enter a brief reason for revoking the certificate.
5. Click **Revoke** to complete the **Revoke Certificate** action.

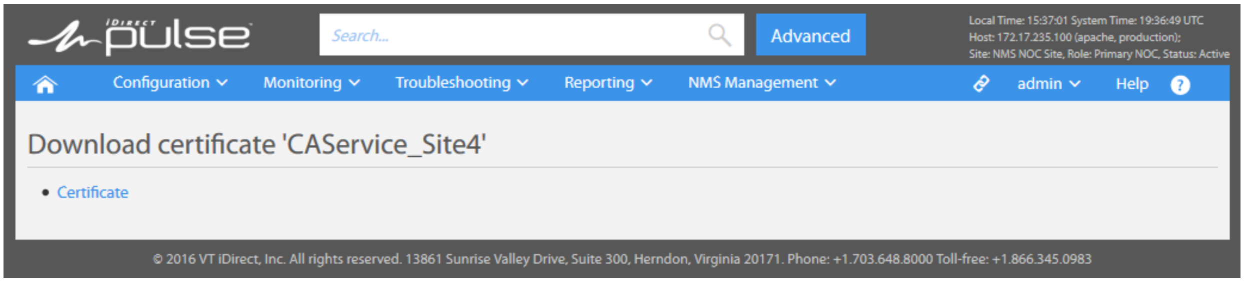
9.12 Downloading a Certificate

The **Download Certificate** operation is accessed directly from the **Actions** menu of a selected certificate; from the **Actions** menu of an NMS Service; or from the **Actions** menu of a physical network element — for example, **Line Card**, **PP Server**, or **SQUID Server** from which the certificate is to be downloaded.

The *download certificate* action results in the actual transfer of a certificate from the NMS element to a local PC or laptop device. The file can then be saved for later convenience or for manual copying to a specific element.

To download a certificate:

1. Use the appropriate **Browse** command to list the elements from which a certificate will be downloaded:
    a. **Browse Security Elements** — to return a list of security elements, from which to display the configured certificates.
    b. **Browse Physical Elements** — to return a list of elements, from which Line Cards, NMS Servers or PP Servers can be listed.
2. Use the **Element Type** drop-down list to filter the list as required.
3. Locate the security element (certificate) or the Physical element (Line Card, PP Server, or NMS Server) from which the certificate will be downloaded.
4. Click the **Actions** button and choose **Download Certificate**. The Download Certificate page is opened for a specific logical element, such as a certificate, or for a specific physical element.
5. Click the **Certificate** link to download and save the certificate file.



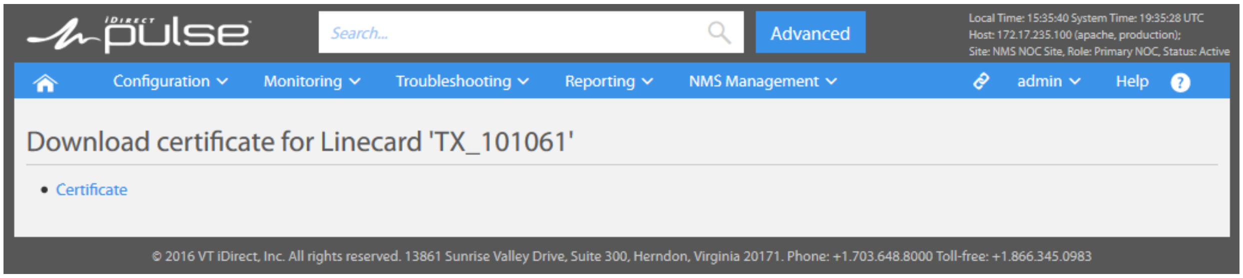
Local Time: 15:37:01 System Time: 19:36:49 UTC
Host: 172.17.235.100 (apache, production);
Site: NMS NOC Site, Role: Primary NOC, Status: Active

Download certificate 'CAService_Site4'

- Certificate

© 2016 VT iDirect, Inc. All rights reserved. 13861 Sunrise Valley Drive, Suite 300, Herndon, Virginia 20171. Phone: +1.703.648.8000 Toll-free: +1.866.345.0983

Figure 9-11. Download Certificate



Local Time: 15:35:40 System Time: 19:35:28 UTC
Host: 172.17.235.100 (apache, production);
Site: NMS NOC Site, Role: Primary NOC, Status: Active

Download certificate for Linecard 'TX_101061'

- Certificate

© 2016 VT iDirect, Inc. All rights reserved. 13861 Sunrise Valley Drive, Suite 300, Herndon, Virginia 20171. Phone: +1.703.648.8000 Toll-free: +1.866.345.0983

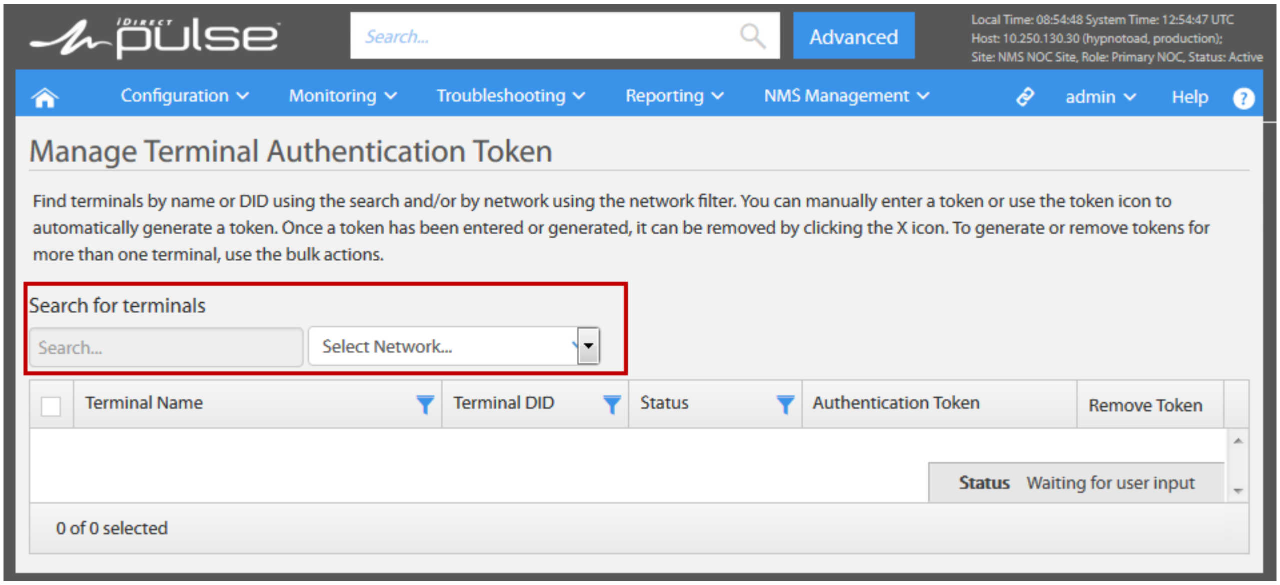
Figure 9-12. Download Certificate from Physical Element

9.13 Managing Terminal Authentication

The **Manage Terminal Authentication Token** operation, is used to create or generate a one-time use authentication token for one or more terminals. On an attempt to authenticate into the network, the terminal must use the assigned token. Tokens may be created for a single terminal or multiple terminals simultaneously, and may be automatically generated or entered manually by an authorized NMS user.

Once a terminal authenticates, it appears listed by **Terminal Name**, **Terminal DID**, and the **Status** shows as "Authenticated."

In case a terminal authentication token is ever compromised, a new token can be re-issued, which the terminal will use on the next authentication attempt.



Local Time: 08:54:48 System Time: 12:54:47 UTC
Host: 10.250.130.30 (hypnotoad, production);
Site: NMS NOC Site, Role: Primary NOC, Status: Active

Manage Terminal Authentication Token

Find terminals by name or DID using the search and/or by network using the network filter. You can manually enter a token or use the token icon to automatically generate a token. Once a token has been entered or generated, it can be removed by clicking the X icon. To generate or remove tokens for more than one terminal, use the bulk actions.

Status Waiting for user input

0 of 0 selected

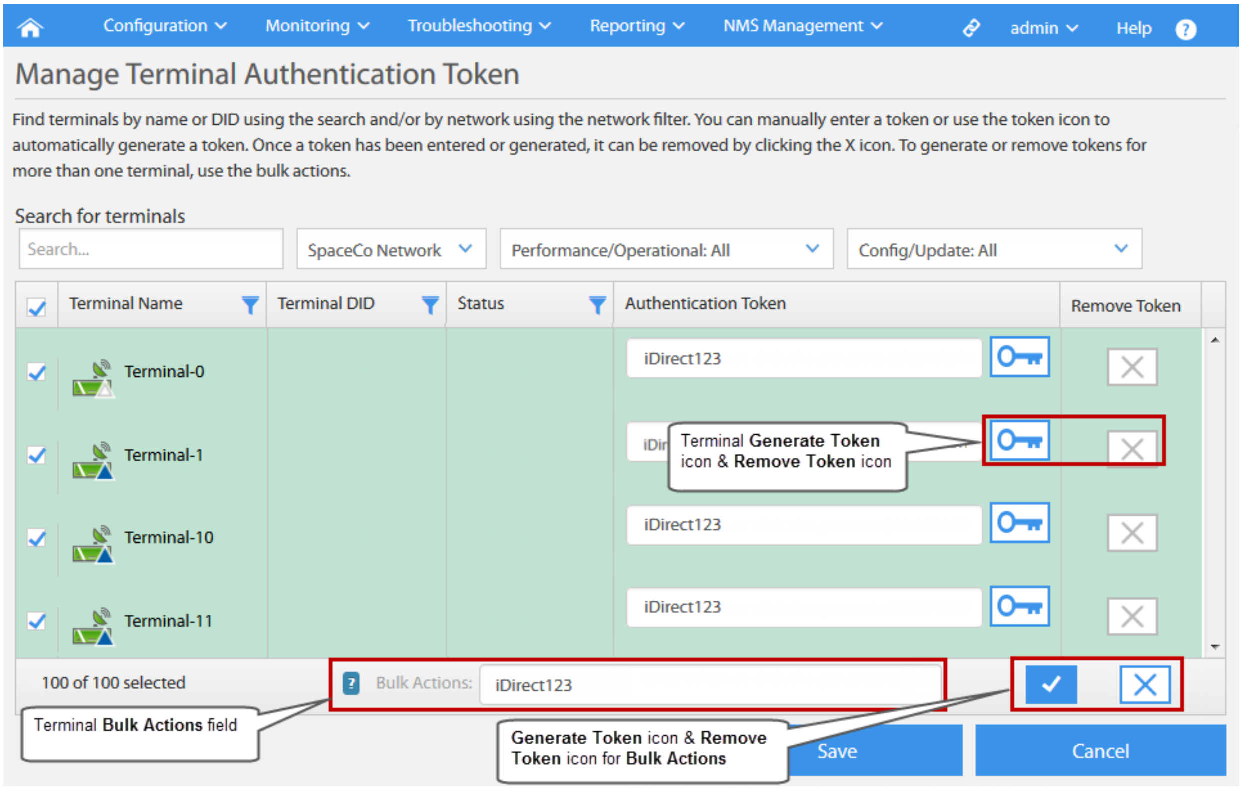
Figure 9-13. Manage Terminal Authentication Dialog

To create a authentication key for a single terminal:

1. Click the **NMS Management** tab > **Manage Terminal Authentication**.
2. Use the **Select Network** drop-down to select the network to which the terminals are associated. The terminals found in the NMS, under this network, are returned.
3. To specify one time token for use by a single terminal select the desired terminal and do one of the following:
    a. Click the **Generate Key** icon to automatically populate the **Authentication Key** field with a 156-bit key (64 HEX characters); or use the following as an alternative:
    b. In the **Authentication Key** field, manually enter a Hex string of 64 characters maximum or an ASCII string of 32 characters maximum. For example iDirect123.
4. Click the **Remove Key** icon to remove the terminal authentication key at any time.
5. Click **Save**. A green message indicates that the token was created successfully.

To create an authentication key for multiple terminals:

1. Click the **NMS Management** tab > **Manage Terminal Authentication**.
2. Use the **Select Pulse Network** drop-down to select the network to which the terminals are associated. The terminals found in the NMS, under this network, are listed in a browse like window.
3. To specify a one time common token for use by multiple terminals select the desired terminals and do one of the following:
    a. Click the **Generate Key** icon adjacent to the **Bulk Actions** field to populate the **Authentication Key** field of the selected terminals with the common generated key.
    b. In the **Bulk Action** field, manually enter a Hex string of 64 characters maximum or an ASCII string of 32 characters maximum - for example iDirect123; then click the adjacent **Generate Key** icon.
4. Click the **Remove Key** in-line with a terminal to remove the terminal authentication key; or click the **Remove Key** adjacent to the **Bulk Action** field to remove the terminal authentication key for several selected terminals.
5. Click **Save**. A green message indicate that the token was created successfully.



Manage Terminal Authentication Token

Find terminals by name or DID using the search and/or by network using the network filter. You can manually enter a token or use the token icon to automatically generate a token. Once a token has been entered or generated, it can be removed by clicking the X icon. To generate or remove tokens for more than one terminal, use the bulk actions.

Search for terminals

Search... | SpaceCo Network | Performance/Operational: All | Config/Update: All

☑	Terminal Name	Terminal DID	Status	Authentication Token	Remove Token
☑	Terminal-0			iDirect123	☒
☑	Terminal-1			iDir	☒
☑	Terminal-10			iDirect123	☒
☑	Terminal-11			iDirect123	☒

100 of 100 selected

Bulk Actions: iDirect123

Terminal **Generate Token** icon & **Remove Token** icon

Terminal **Bulk Actions** field

Generate Token icon & **Remove Token** icon for **Bulk Actions**

Figure 9-14. Manage Terminal Authentication Dialog

9.14 Security Elements Browse Actions

Using the **Browse Security Elements** command, users can interact with configured NMS Security elements in the Browse Results list to perform a variety of specific operations. These operations are called “Actions.” An action can be performed on a single selected element, or simultaneously on several selected elements.

What actions are actually possible, are based on the selected element type, and only those actions are displayed when that element type is selected.

Security element actions are listed and briefly described as follows:

Table 9-1. Security Elements — Browse Actions

Action	Brief Description
Delete Element	Remove the selected security element from the NMS. Applies to all security elements.
Lock	Lock access to the selected vault or CA element. Applies to the CA and vault elements only.
Unlock	Unlock access to the selected vault or CA element. Applies to the CA and vault elements only.
Set Default	Set the selected vault the default; or set the selected CA as the default. Applies to the CA and vault elements only.
Roll	Request that a vault table stop using the current set of keys for encryption in the current active window and generate a new set of keys to encrypt data for the new window. Applies to the vault only.
Change Password	Change the password for the selected vault or CA element. Applies to the vault only.
Migrate To	Migrate all encrypted data from one vault table to another vault.Applies to the vault only.
Revoke	Applies to the certificate only. See *Revoking a Certificate*.
Download	Applies to the certificate only. See *Downloading a Certificate*.

10 NMS Software Installs & Upgrades

This chapter is the final of three chapters that cover Pulse System Administration domain operations. In this chapter, you are introduced to the various NMS operations that involve management of the software components and software versions that are installed on iDirect network elements.

Pulse software installation and upgrade operations are covered in the following topics:

- *About Install and Upgrade Operations* on page 134
- *Uploading a Package Bundle Metadata File* on page 135
- *Uploading a Software Package* on page 136
- *Uploading a BLOB File* on page 137
- *Uploading a Third-Party Package* on page 138
- *Uploading PP Terminal Metadata* on page 139
- *About Managing Software Versions* on page 140
- *Installing and Upgrading a Software Package* on page 140
- *Installing a BLOB File* on page 142

10.1 About Install and Upgrade Operations

NMS Install and Upgrade operations are an important part of the ongoing life cycle of managing software versions and upgrades for networks elements such as hub Line Cards, NMS, PP and Squid Servers, Satellite Terminals, and Satellite Terminal components.

Pulse provides a set of software management operations that allow network administrators to upload iDirect and third-party software and BLOB files to the NMS server and to redistribute and install these files to the appropriate network elements. These operations are accessed from the **Install & Upgrade** sub-menu on the **NMS Management** tab, and in some cases, by using the **Actions** menu of an element selected in a browse window.

10.1.1 Software Release Components

Generally, the iDirect Network software is provided using the following components:

- **Bundle Metadata File** — a single file (*.pkg* format) that stores all relevant information for individual software packages of a software release. This file is required by the Update Manager on the NMS server to process, validate, and appropriately assign individual packages to the network elements in the case of a software upgrade.
- **Carton File (s)** — this is a compressed file (*.carton* format), which consists of all relevant software packages for either an NMS, PP, Hub line card, or Satellite Terminal.
- **Package Files** — these are individual software packages for each network element.
- **Third-party Package File (s)** — these are third-party software packages for Satellite Terminal ACU, BUC, and other non-iDirect components.

In addition to these software components, operators can upload a set of files (in any format) to the NMS for distribution to any network elements. This package type is called a *BLOB File*. The NMS handles uploading of a BLOB the same as any of the previously mentioned files.

Managing software release components and other System Administration Domain elements are accessed from the **Install & Upgrade** submenu of the **NMS Management** menu tab.

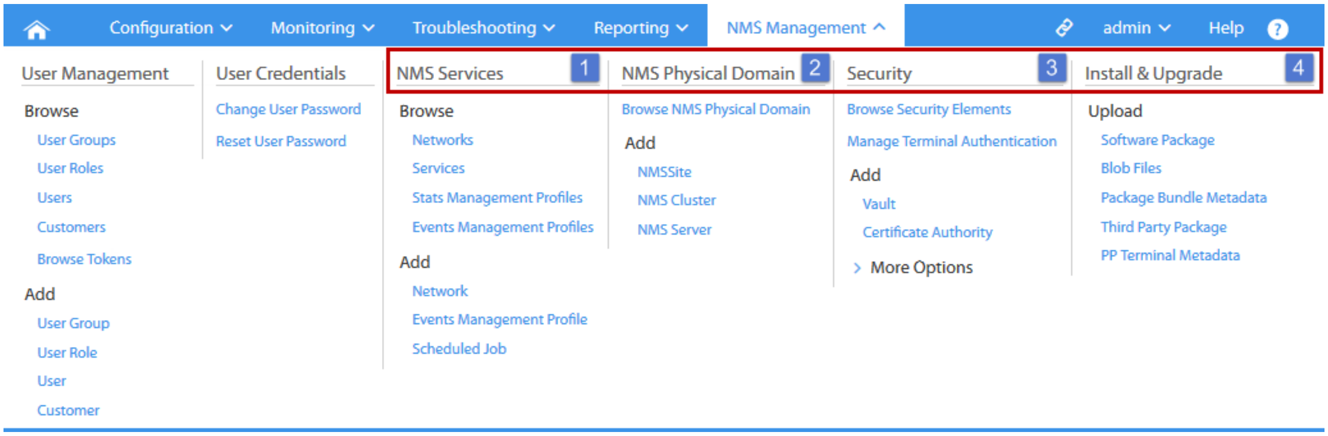
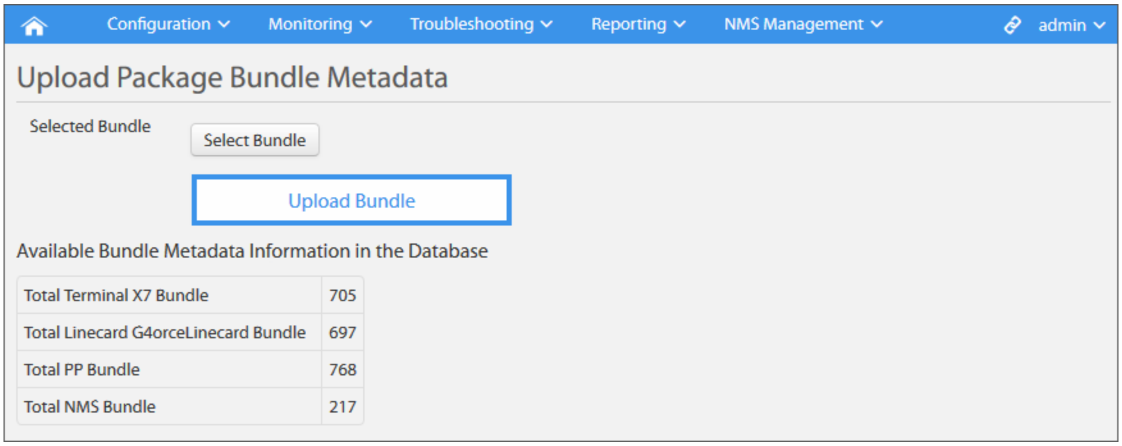


Figure 10-1. NMS Management — System Administration Operations

10.2 Uploading a Package Bundle Metadata File

From the **Upload Package Bundle Metadata** page, network administrators can upload Package Metadata files from the local machine to the NMS server. The page, when opened, shows bundled metadata, by element type, that are already available on the NMS server. Later this bundle, which has a list of all packages required by a specific element, will be used to verify whether all software packages have been uploaded to the NMS server.

Currently, only the PP server uses package bundle metadata since the PP has multiple packages associated with each update process.



Available Bundle Metadata Information in the Database

Total Terminal X7 Bundle	705
Total Linecard G4orceLinecard Bundle	697
Total PP Bundle	768
Total NMS Bundle	217

Figure 10-2. Import iDirect Bundle Metadata Information Dialog

To upload a package bundle metadata file to the NMS:

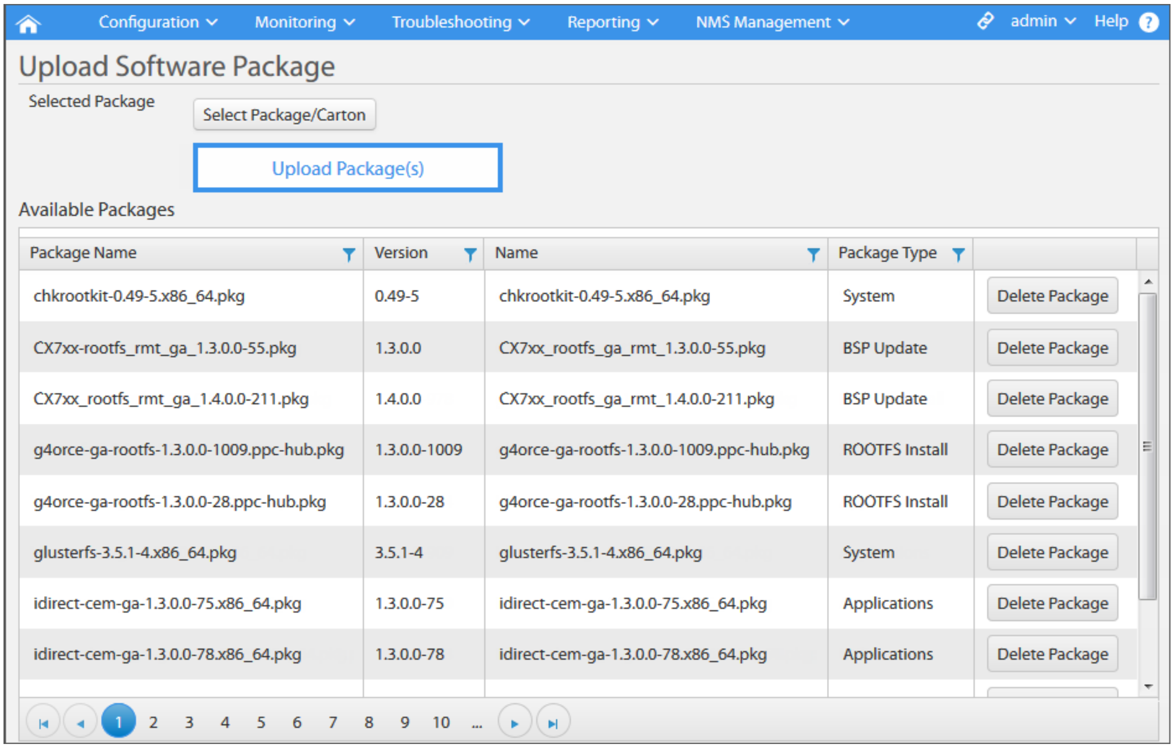
1. Click the **NMS Management** tab > **Install & Upgrade > Upload > Package Bundle Metadata.**This procedure is not required if the needed package metadata for a particular package is already listed as available in the NMS.
2. Click **Select Bundle** to open a new Explorer window. Locate and select the desired bundle metadata file, and then, click **Open** to add it to the list.
3. Click **Upload Bundle** to upload the file to the NMS server. Upon completion, the message *Package Bundle Metadata upload successfu*l is reported by the NMS.

10.3 Uploading a Software Package

Using the The **Upload Software Package** command, network operators have the option to upload iDirect packages or cartons to the NMS server. This page also provides a list of software packages that are already available on the NMS. Packages/Cartons that are no longer needed, may also be deleted from this page, by clicking the appropriate **Delete Package** button.

Once a package is available in the NMS, network administrators can apply the package to a specific element as a software upgrade using the **Action** menu of that element and choosing the **Manage Software Version** option.

The **Upload Package** command is accessed directly from the **NMS Management** menu, under **Install & Upgrade**, or from the **Actions** menu of the **Update Manager** service.



Package Name	Version	Name	Package Type	
chkrootkit-0.49-5.x86_64.pkg	0.49-5	chkrootkit-0.49-5.x86_64.pkg	System	Delete Package
CX7xx-rootfs_rmt_ga_1.3.0.0-55.pkg	1.3.0.0	CX7xx_rootfs_ga_rmt_1.3.0.0-55.pkg	BSP Update	Delete Package
CX7xx_rootfs_rmt_ga_1.4.0.0-211.pkg	1.4.0.0	CX7xx_rootfs_ga_rmt_1.4.0.0-211.pkg	BSP Update	Delete Package
g4orce-ga-rootfs-1.3.0.0-1009.ppc-hub.pkg	1.3.0.0-1009	g4orce-ga-rootfs-1.3.0.0-1009.ppc-hub.pkg	ROOTFS Install	Delete Package
g4orce-ga-rootfs-1.3.0.0-28.ppc-hub.pkg	1.3.0.0-28	g4orce-ga-rootfs-1.3.0.0-28.ppc-hub.pkg	ROOTFS Install	Delete Package
glusterfs-3.5.1-4.x86_64.pkg	3.5.1-4	glusterfs-3.5.1-4.x86_64.pkg	System	Delete Package
idirect-cem-ga-1.3.0.0-75.x86_64.pkg	1.3.0.0-75	idirect-cem-ga-1.3.0.0-75.x86_64.pkg	Applications	Delete Package
idirect-cem-ga-1.3.0.0-78.x86_64.pkg	1.3.0.0-78	idirect-cem-ga-1.3.0.0-78.x86_64.pkg	Applications	Delete Package

Figure 10-3. Import Package/Carton Dialog

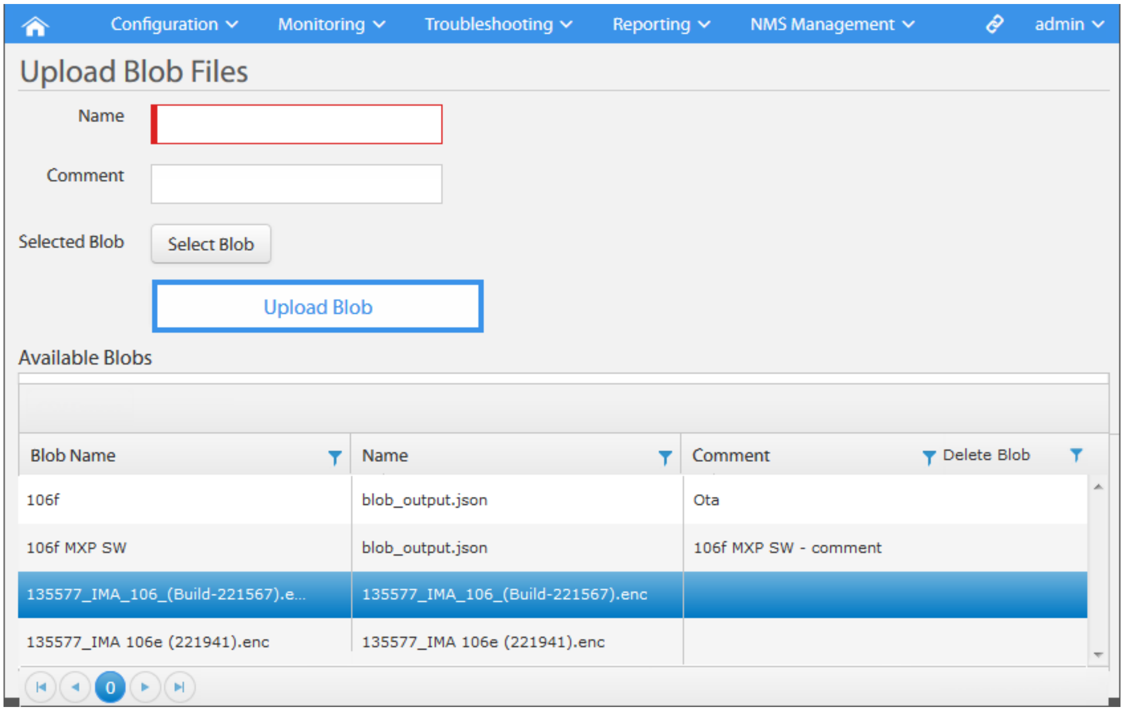
To upload a package to the NMS:

1. Click the **NMS Management** tab > **Install & Upgrade** > **Upload > Software Package.**
2. Click **Select Package/Carton** to open Windows Explorer and navigate to the target software package or carton on the local machine.
3. Locate and click the package/carton; then click **Open** to select the file for uploading.
4. With the file displayed on the dialog, adjacent to the **Select Package/Carton** button, click the **Upload Package(s)** button to upload the file to the NMS.
5. Verify that the software/packages have been successfully uploaded by locating them under the **Available Packages** list.

10.4 Uploading a BLOB File

Using the **Upload BLOB Files** page, network administrators can upload any files to the NMS Server for distribution to any network element.

With the **Available BLOBs** list displayed, network administrators have the option to delete a BLOB that is no longer needed by clicking the **Delete BLOB** button.



Blob Name	Name	Comment	Delete Blob
106f	blob_output.json	Ota	
106f MXP SW	blob_output.json	106f MXP SW - comment	
135577_IMA_106_(Build-221567).e...	135577_IMA_106_(Build-221567).enc		
135577_IMA 106e (221941).enc	135577_IMA 106e (221941).enc		

Figure 10-4. Upload BLOB Dialog

Once a BLOB file is available in the NMS, it can be applied to a network element by using the **Manage BLOB File** option, which is accessed from the **Actions** menu of a selected element. For example a BLOB file can be managed for NMS, PP, and SQUID Servers; and for Line Cards.

To upload a BLOB file to the NMS:

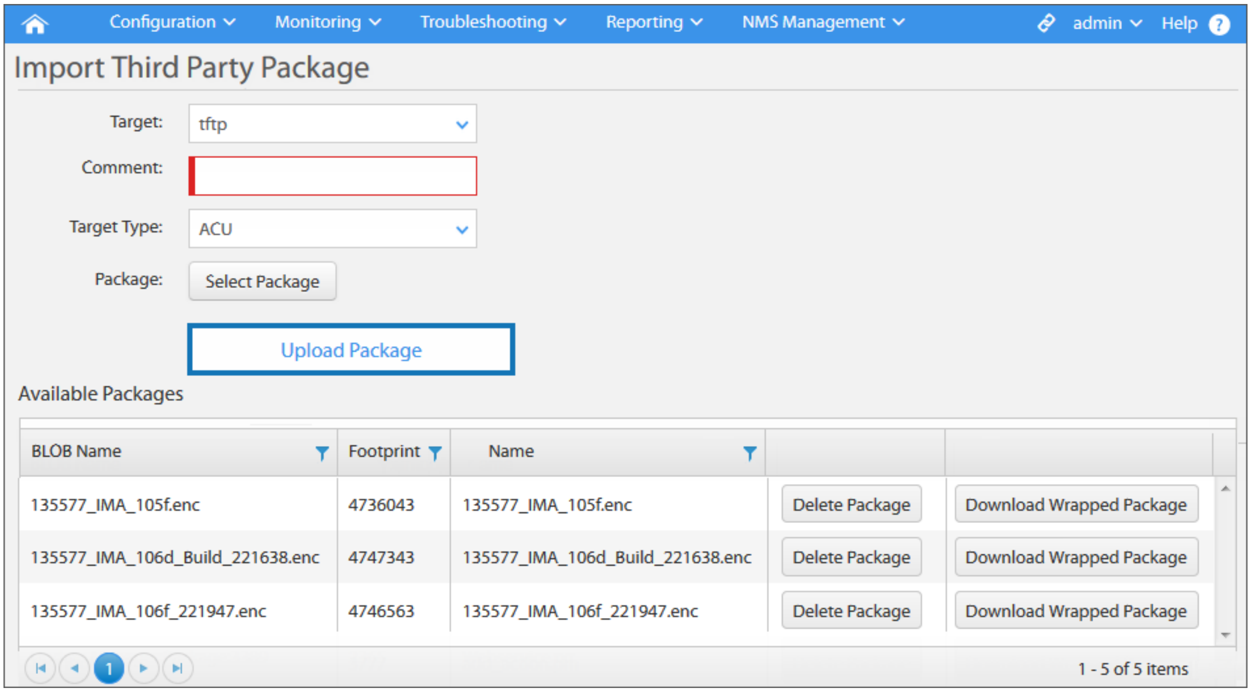
1. Click the **NMS Management** tab > **Install & Upgrade > Upload > BLOB Files. The Upload BLOB Files** page opens to a list of BLOB files currently available on the NMS server.
2. In the **Name** field, type a name for the BLOB file.
3. In the **Comment** field, enter a short comment/description for the BLOB file.
4. Click **Select Blob** to open Windows Explorer and navigate to a desired BLOB file.
5. Locate and click the BLOB file and click **Open** to select the file for uploading.
6. With the file displayed on the dialog, adjacent to the **Select Blob** button, click the **Upload Blob** button to upload the file to the NMS.
7. Click the **Delete BLOB** button on a specific file to remove it when it is no longer needed.

10.5 Uploading a Third-Party Package

Using the **Upload Third Party Package** command, network operators may upload to the NMS server, third-party software packages for Satellite Terminal ACU and BUC elements.

The **Upload Third-Party Package** page also lists third party packages currently found on the NMS server. Network operators have the option to delete any packages/cartons that are no longer needed or to download a wrapped package. A wrapped package is a third-party package that has been re-packaged as an iDirect package.

Once the package is available in the NMS, a network administrator can apply the package to a network element using the **Manage BLOB File** option from the **Action** menu of the element.



Import Third Party Package

Target: tftp

Comment:

Target Type: ACU

Package:

Available Packages

BLOB Name	Footprint	Name		
135577_IMA_105f.enc	4736043	135577_IMA_105f.enc	Delete Package	Download Wrapped Package
135577_IMA_106d_Build_221638.enc	4747343	135577_IMA_106d_Build_221638.enc	Delete Package	Download Wrapped Package
135577_IMA_106f_221947.enc	4746563	135577_IMA_106f_221947.enc	Delete Package	Download Wrapped Package

1 - 5 of 5 items

Figure 10-5. Upload Third-Party Package Dialog

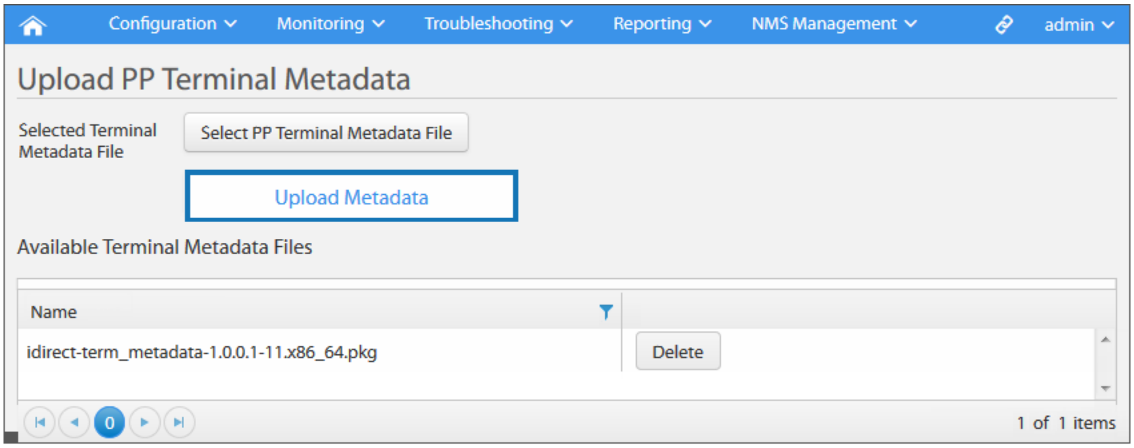
To upload a third-party package:

1. Click the **NMS Management** tab > **Install& Upgrade > Upload > Third Party Package**.
2. Use the **Target** drop-down list, and select **tftp** or **serial** as the upload option.
3. In the **Comment** field, enter a short comment/description for the third party package.
4. Use the **Target Type** drop-down list, and choose **ACU** or **BUC** as the target element for the third-party package.
5. Click **Select Package** to open Windows Explorer and navigate to the third-party package.
6. With the file displayed on the dialog, adjacent to the **Select Package** button, click the **Upload Package** button to upload the file to the NMS.

10.6 Uploading PP Terminal Metadata

The **Upload PP Terminal Metadata** page is used to upload PP Terminal metadata files to the NMS Server, for distribution to PP Clusters. Once the file is uploaded, the NMS delivers the data, in JSON format, to PP Clusters. The Protocol Processor pp_sync_opt process verifies the validity of the file and makes it available to the necessary PP processes as if it were an options file.

A *terminal metadata file* consists mainly of terminal model-specific information that is loaded during PP start-up. The file, similar in format to an options file, describes terminal models by including information such as model numbers, DVBS2 MODCOD tables, minimum and maximum symbol rates, and attenuator step sizes. The file also indicates whether specific features are supported by the terminal.


Configuration
Monitoring
Troubleshooting
Reporting
NMS Management
admin
Upload PP Terminal Metadata
Selected Terminal Metadata File
Select PP Terminal Metadata File
Upload Metadata
Available Terminal Metadata Files
Name
Delete
0
1 of 1 items

Name	
idirect-term_metadata-1.0.0.1-11.x86_64.pkg	Delete

Figure 10-6. Upload Protocol Processor Terminal Metadata Dialog

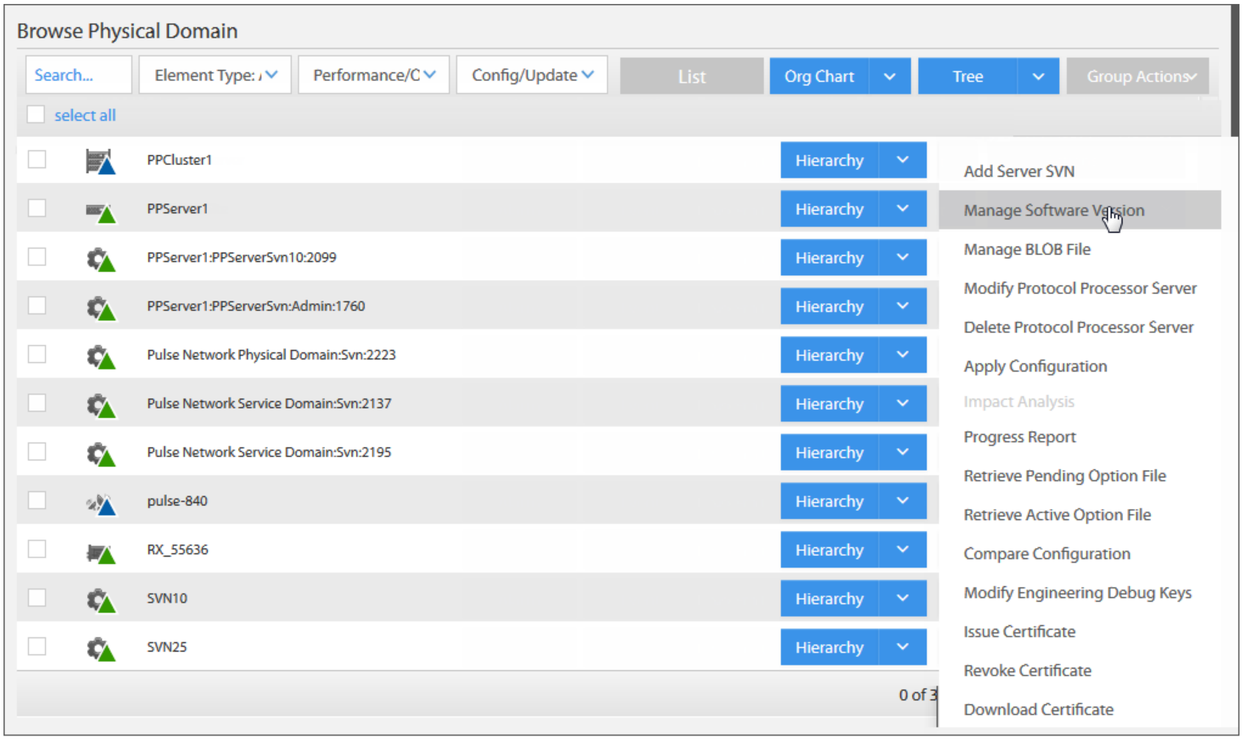
To upload PP Terminal Metadata File to the NMS:

1. Click the **NMS Management** tab > **Install& Upgrade > Upload > PP Terminal Metadata**.
2. Click the **Select PP Terminal Metadata File** button to open a Windows Explorer and navigate to the PP Terminal Metadata file on the local PC.
3. Select the file and click **Open** to select the file for uploading to the NMS.
4. With the file displayed on the dialog, adjacent to the **Selected Terminal Metadata File** label, click **Upload Metadata** to upload the file to the NMS. PP Metadata Files that are already on the NMS, if any, are listed in the **Available Terminal Metadata Files** pane.
5. Click the **Delete** button on a specific file to remove it when it is no longer needed.

10.7 About Managing Software Versions

From the NMS, both iDirect and third-party software packages and BLOB files are uploaded to the NMS using operations that are accessed from the **NMS Management** menu. These files are can then be managed and installed to the appropriate elements. Software packages and blob files are managed and installed either directly for the NMS Management tab or from the **Actions** menu of a selected element when listed in the Browse window.

Software management operations are a key part of the ongoing life cycle of software versions and upgrades for networks elements such as PP Server; Line Cards and Satellite Terminals; and Satellite Terminal components, including BUCs and ACUs.



- ☐ PPCluster1
- ☐ PPServer1
- ☐ PPServer1:PPServerSvn10:2099
- ☐ PPServer1:PPServerSvn:Admin:1760
- ☐ Pulse Network Physical Domain:Svn:2223
- ☐ Pulse Network Service Domain:Svn:2137
- ☐ Pulse Network Service Domain:Svn:2195
- ☐ pulse-840
- ☐ RX_55636
- ☐ SVN10
- ☐ SVN25

Figure 10-7. Software Management Using Actions Menu

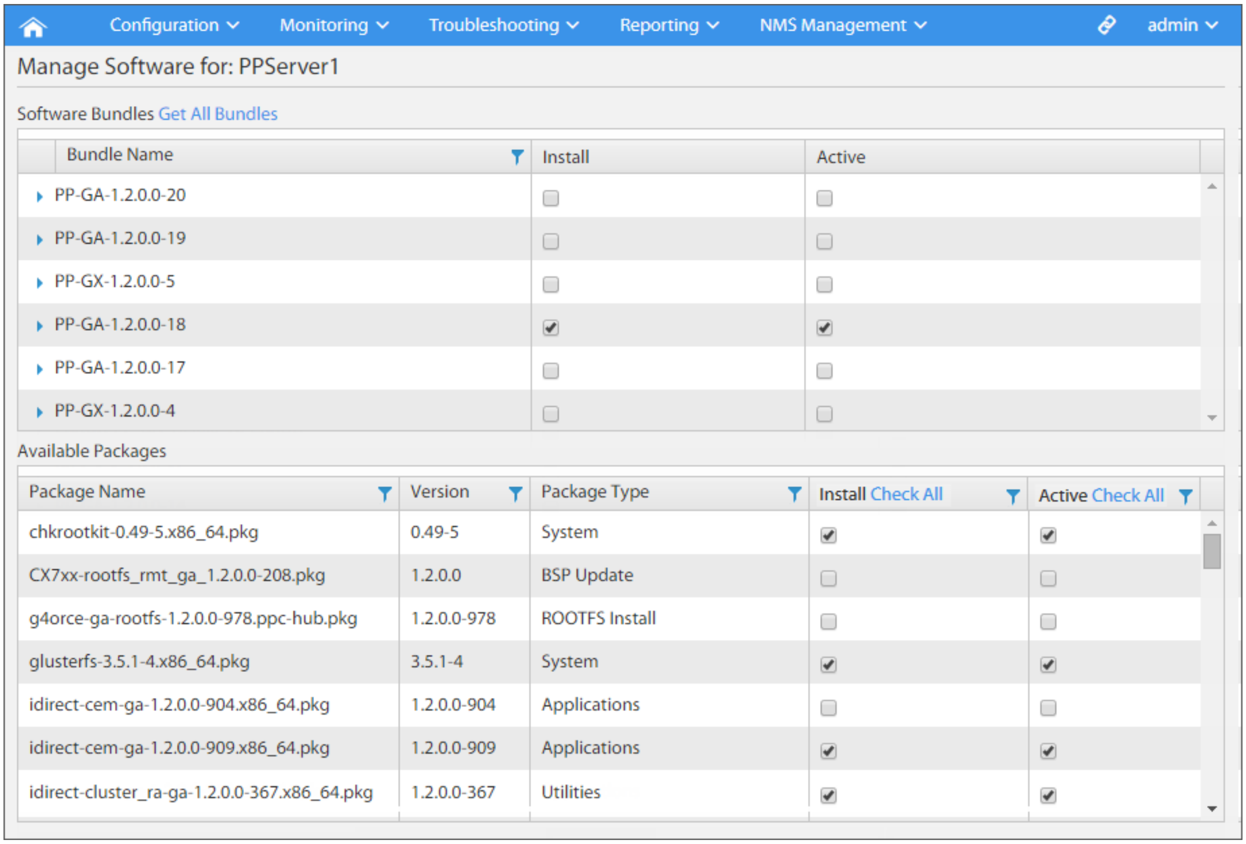
10.8 Installing and Upgrading a Software Package

A *package*, in the NMS, represents various software files and images required to upgrade an PP Server, Line Card, or Terminal to a particular software version. In the case of servers, a number of packages are generally required; with line cards and terminals, a package includes the release software and firmware images, and Linux board support package (BSP) updates.

From the **Browse Physical Domain** or **Browse Terminal Elements** results list, the **Manage Software** page is opened by clicking the **Actions** menu of a selected element and then selecting the **Manage Software Version** option.

The NMS supports the following operations from either the **Browse Physical Domain** results list or from the **Browse Terminal Elements** results list:

- Manage Software Package for: PP Server
- Manage Software Package for: Tx Line Card/Rx Line Card
- Manage Software Package for: Satellite Terminal



Manage Software for: PPServer1

Software Bundles Get All Bundles

Bundle Name	Install	Active
PP-GA-1.2.0.0-20	☐	☐
PP-GA-1.2.0.0-19	☐	☐
PP-GX-1.2.0.0-5	☐	☐
PP-GA-1.2.0.0-18	☑	☑
PP-GA-1.2.0.0-17	☐	☐
PP-GX-1.2.0.0-4	☐	☐

Available Packages

Package Name	Version	Package Type	Install Check All	Active Check All
chkrootkit-0.49-5.x86_64.pkg	0.49-5	System	☑	☑
CX7xx-rootfs_rmt_ga_1.2.0.0-208.pkg	1.2.0.0	BSP Update	☐	☐
g4orce-ga-rootfs-1.2.0.0-978.ppc-hub.pkg	1.2.0.0-978	ROOTFS Install	☐	☐
glusterfs-3.5.1-4.x86_64.pkg	3.5.1-4	System	☑	☑
idirect-cem-ga-1.2.0.0-904.x86_64.pkg	1.2.0.0-904	Applications	☐	☐
idirect-cem-ga-1.2.0.0-909.x86_64.pkg	1.2.0.0-909	Applications	☑	☑
idirect-cluster_ra-ga-1.2.0.0-367.x86_64.pkg	1.2.0.0-367	Utilities	☑	☑

Figure 10-8. Manage Software Install Package Dialog

To install a package for a PP Server element:

1. From the **Configuration** tab, use **Browse Physical Domain**, to list PP Servers.
2. Use the **Element Type** drop-down list to select **PP Server**.
3. Select the desired element and then click the **Actions** drop-down list and select **Manage Software Version** to open the **Manage Software** dialog.
4. Identify the appropriate **Software Bundle**, by **Bundle Name**, and select both the **Install** and the **Active** check box. Each Package that is part of a bundle is automatically marked in the second window where packages are listed.
5. Click **Submit.**

To install a package for a Line Card or Terminal element:

1. From the **Configuration** tab, use **Browse Terminal Elements**, to list Terminals**;** or use **Browse Physical Domain**, to list Line Cards.
2. Use the **Element Type** drop-down list to select a specific element type. For example, select **Line Cards** or **Terminals**.
3. Select the desired element and then click the **Actions** drop-down list and select **Manage Software Version** to open the **Manage Software** dialog.
4. Identify the appropriate **Software Package** from the lower window and select both the **Install** and the **Active** check box.
5. Click **Submit.**

10.9 Installing a BLOB File

A *BLOB (Binary Large OBject) file*, is a collection of binary data files stored as a single entity. In the NMS, a BLOB file is always associated with a specific network element.

From the **Browse Physical Domain** or **Browse Terminal Elements** results list, the **Manage BLOB File** page is opened from the **Actions** menu of a selected Physical Domain or Terminal Domain element, by selecting the **Manage BLOB File** option.

The NMS supports the following operations from either the **Browse Physical Domain** results list or from the **Browse Terminal Elements** results list:

- Manage BLOB File for PP Server, NMS Server, SQUID Server, Tx Line Card, Rx Line Card
- Manage BLOB File for Satellite Terminal

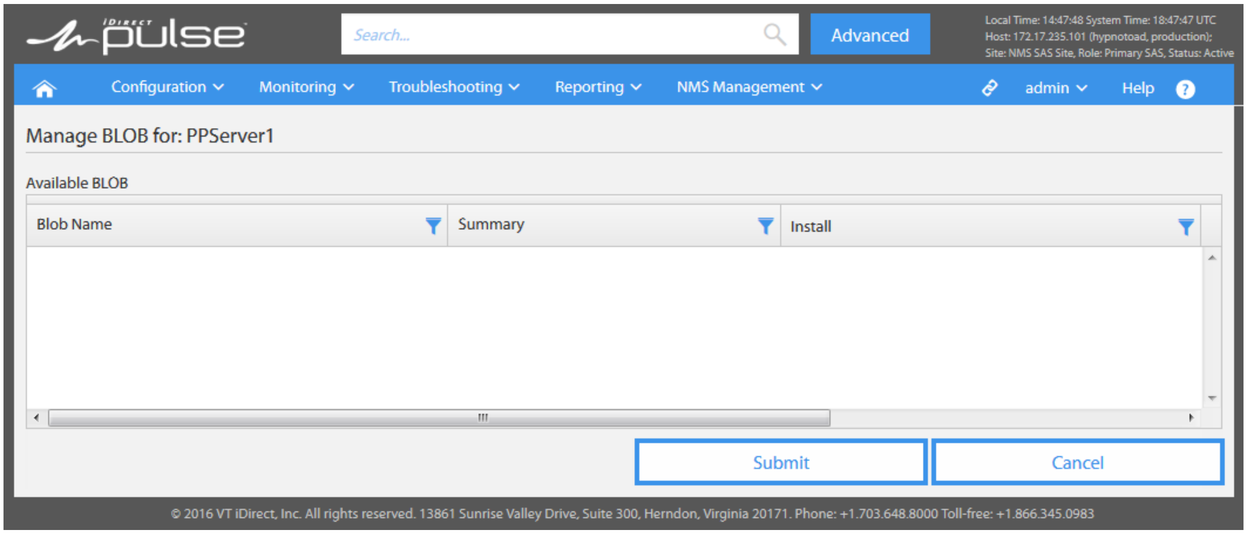

iDirect pulse
Search...
Advanced
Local Time: 14:47:48 System Time: 18:47:47 UTC
Host: 172.17.235.101 (hypnotoad, production);
Site: NMS SAS Site, Role: Primary SAS, Status: Active
Configuration
Monitoring
Troubleshooting
Reporting
NMS Management
admin
Help
Manage BLOB for: PPServer1
Available BLOB
Blob Name
Summary
Install
Submit
Cancel
© 2016 VT iDirect, Inc. All rights reserved. 13861 Sunrise Valley Drive, Suite 300, Herndon, Virginia 20171. Phone: +1.703.648.8000 Toll-free: +1.866.345.0983

Figure 10-9. Install BLOB Files Dialog

To install a BLOB for a specified network element:

1. From the **Configuration** tab, use the appropriate Browse command — for example, **Browse Terminal Elements**, to find Terminals**;** or **Browse Physical Domain**, to find Line Cards and Servers.
2. Use the **Element Type** drop-down list to select a specific element type. For example, select **Line Card**, **NMS Server**, **PP Server**, or **Satellite Terminal**.
3. Locate and select an element and then click the **Actions** drop-down list and choose **Manage BLOB File** to open the **Install BLOB** dialog.
4. From the **Available BLOB** records list, identify the appropriate BLOB, by **BLOB Name** and **Summary**, and select the associated **Install** check box.
5. Click **Submit.**

11 Network Configuration Management

Pulse Configuration Management includes concepts such as network element configuration states, configuration options files, and configuration inventories and action plans. These concepts, all deal with the development and management of network element configurations, and understanding the various stages of configuration and the states in which an element can exist during configuration. For example, an *options file* is used by the NMS to save the configuration of each network element.

Pulse configuration management operations are covered in the following topics:

11.1 NMS Object Types

Before examining the details of network object states, it is important to understand the types of iDirect network objects — the objects to which states are assigned:

- **Network Item** — Any network element, component, profile, or shared resource.
- **Network Element** — A physical or logical network object, which must also be a unique object known to the iDirect Network data path.
- **Profile** — An NMS-only object that provides a set of related configuration parameters that can be shared across multiple network elements. A profile is similar to a template, however, unlike a template, changes to a profile are also applied to all network elements that are instances of that profile.
- **Shared Resource** — A non-profile object whose configuration is partially inherited by child objects.
- **Component** — A part of a network element's configuration that is the result of applying a specific profile and additional element-specific parameters. The component is managed separately from any other part of the element configuration.

Although profiles, shared resources, and components share certain attributes, these object types are significantly different from one another. The characteristics of each of these objects are described in order to show their key differences.

Profile Characteristics:

- A profile may be assigned to multiple network elements- for example a subscriber service plan profile (SSPP) could be applied to create instances in multiple terminals.
- A profile may be assigned to multiple profiles.
- A profile may be inherited from another profile.
- A network element and an assigned profile have an inheritance relationship where all parameters specified in the assigned profile is inherited by the network element.

Shared Resource Characteristics:

- A shared resource has both shared and private parameters so that only shared parameters can be inherited by a network element.
- A shared resource and its assigned network element have a parent/child relationship.
- A shared resource may have multiple child elements (be assigned to many elements).
- A shared resource may be the parent of another shared resource.
- A shared resource is recognized by the data path as an independent entity.

Component Characteristics:

- A component has only one parent.
- A network element may have multiple components with different parents.

Since these objects have unique behaviors when interacting with one another, as well as when it comes to their functionality in the network, not all network object states are applicable when depicting the current configuration or operational state of an element.

11.2 NMS Element Icons

Each element of an iDirect Network, physical or logical, is symbolized by a unique Pulse icon shape. Whereas the shape alone distinguishes each element, in Pulse additional information will be attributed to the element, based on indicator colors and icon overlays.

Within a short time you will easily identify a terminal, an upstream carrier, downstream carrier, or a transmit line card, as well as any additional information associated with the element — for example its current operational state. Pulse element icons are shown below:

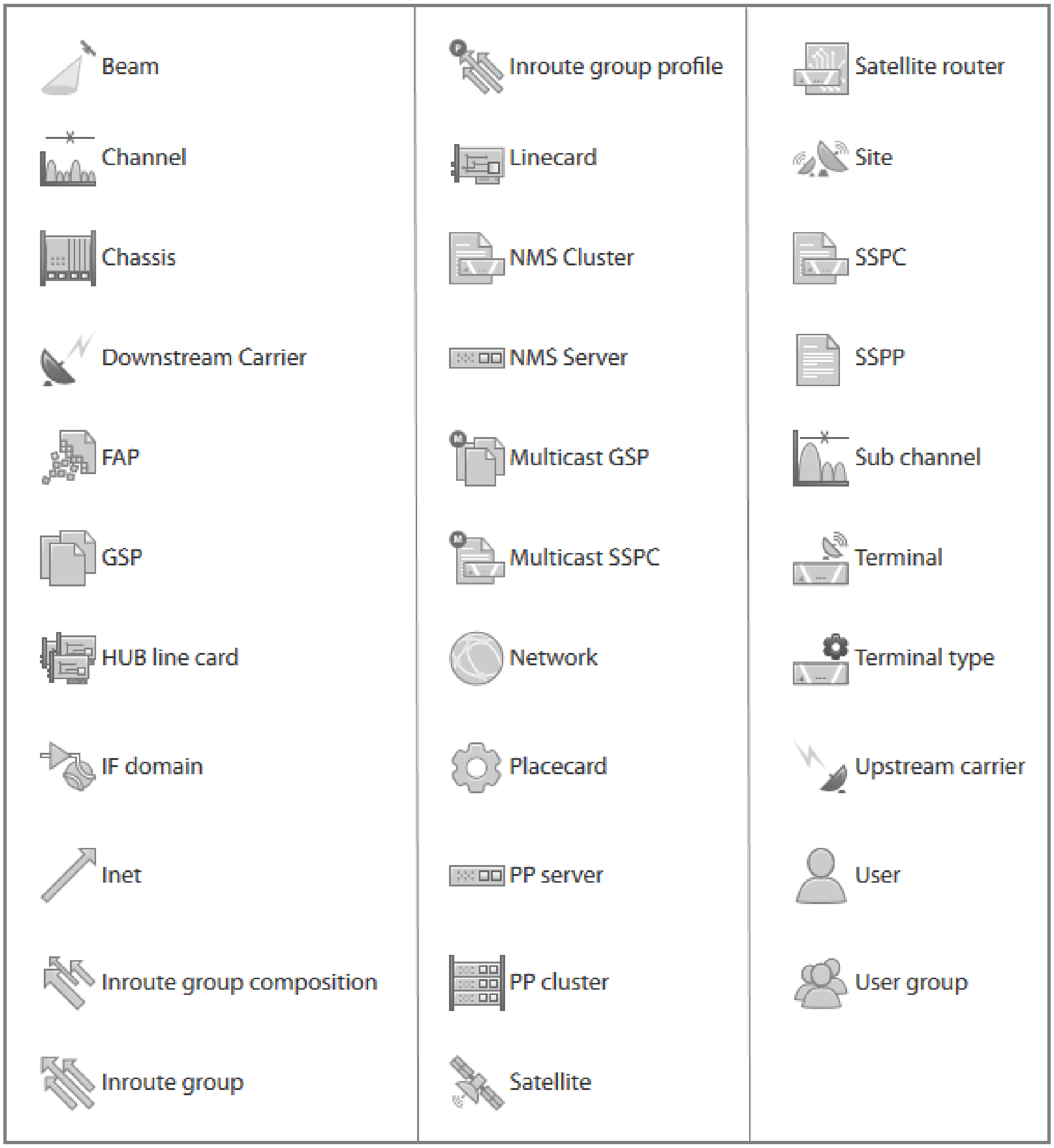


Figure 11-1. Pulse NMS Object Icons

11.3 NMS Element Management States

Central to the operation and understanding of the Pulse® NMS is the concept of "element management states." Management states represent network elements in terms of their current configuration/update, operational, and activation states. The various states of an element are based on a defined aggregation logic that is reflected in the element icon, using a specific color, a triangular overlay, a text message, or some combination of these indicators.

Pulse NMS object states, reflected in each element's icon, is based on the following three components, which are briefly described in the following sections.

- **Configuration/Update State** — reflected by a triangle in bottom right corner of the icon
- **Operational State** — reflected in the icon background color
- **Element Type** — defined by the icon shape positioned in the background

11.3.1 Configuration/Update States

The *configuration/update* state of an element is based upon a three-step change process that gives network operators control over operational network items, when it comes to making any configuration changes. These steps that only occur with operator initiation, are listed below:

1. **Create Network Item** — a new instance of a network item is created in the NMS.
2. **Modify Network Item** — configuration changes are made to an existing network item.
3. **Apply Changes to Item** — pending changes are made active in an existing network item.

This three step process results in the NMS database being temporarily out-of-sync with the actual network. This situation occurs after modifications are made, but are yet to be applied to the network. The element state during this transition is referred to as the *update state*.

The configuration/update state of an element is represented in the NMS as a triangular overlay icon, positioned at the right bottom corner of an element icon. The configuration/update states are generally seen when elements are listed in the Browse window or other NMS pages where the element is shown.

Table 11-1. Configuration/Update States & Icon Overlays

Icon Overlay	Config. State	Update State	Description
△	Incomplete	Error	All configuration parameters required for the network item are not yet configured, but the configuration has been saved.
▲	Changes Pending	Out of Sync	The configuration of an item is out-of-sync with the NMS due to recent changes that have not been applied to the item.
▲	Nominal	In Sync	The configuration of an item is in sync with the NMS. All needed parameters are configured and have been applied.
▲	Warning	Unknown	A recently updated item has applied all NMS changes initiated by network operator. This overlay is generally accompanied by a message that can be viewed by clicking on element icon.

11.3.2 Operational States

A new network element, once configured and activated in a network, periodically notifies the NMS of its operational state changes. These updates allow the network operator to view the live status of elements without having to manually request the element status. Similar to configuration/update states, the operational state is reflected by overlaying a different color on the standard network element icons. For example, the default icon shape of a terminal is overlayed with a green background when the terminal is "Online." See *NMS Element Icons*.

Table 11-2 illustrates how the icon overlay color reflects the operational states of a terminal.

Table 11-2. Element Icon and Operational State Overlay Colors

Icon	Color	Activation	Operational State	Aggregate State	Description
🟩	Green	*	Online	Online	Element is actively running in the network.
🟧	Orange	*	Online	Degraded	Element is actively running in the network, but its performance is degraded.
🟥	Red	*	Off-Line	Offline	Element is off-line. Immediate attention is required to return element to an active operational state.
⬛	Dark Gray	*	Unknown	No State	Element has become unknown to the network. This state may have resulted from unresponsiveness or inactivity for an
⬜	Light Gray	Deactivated	*	Deactivated	Element has been deactivated in network.

The NMS currently determines the operational states of all elements of the following types:

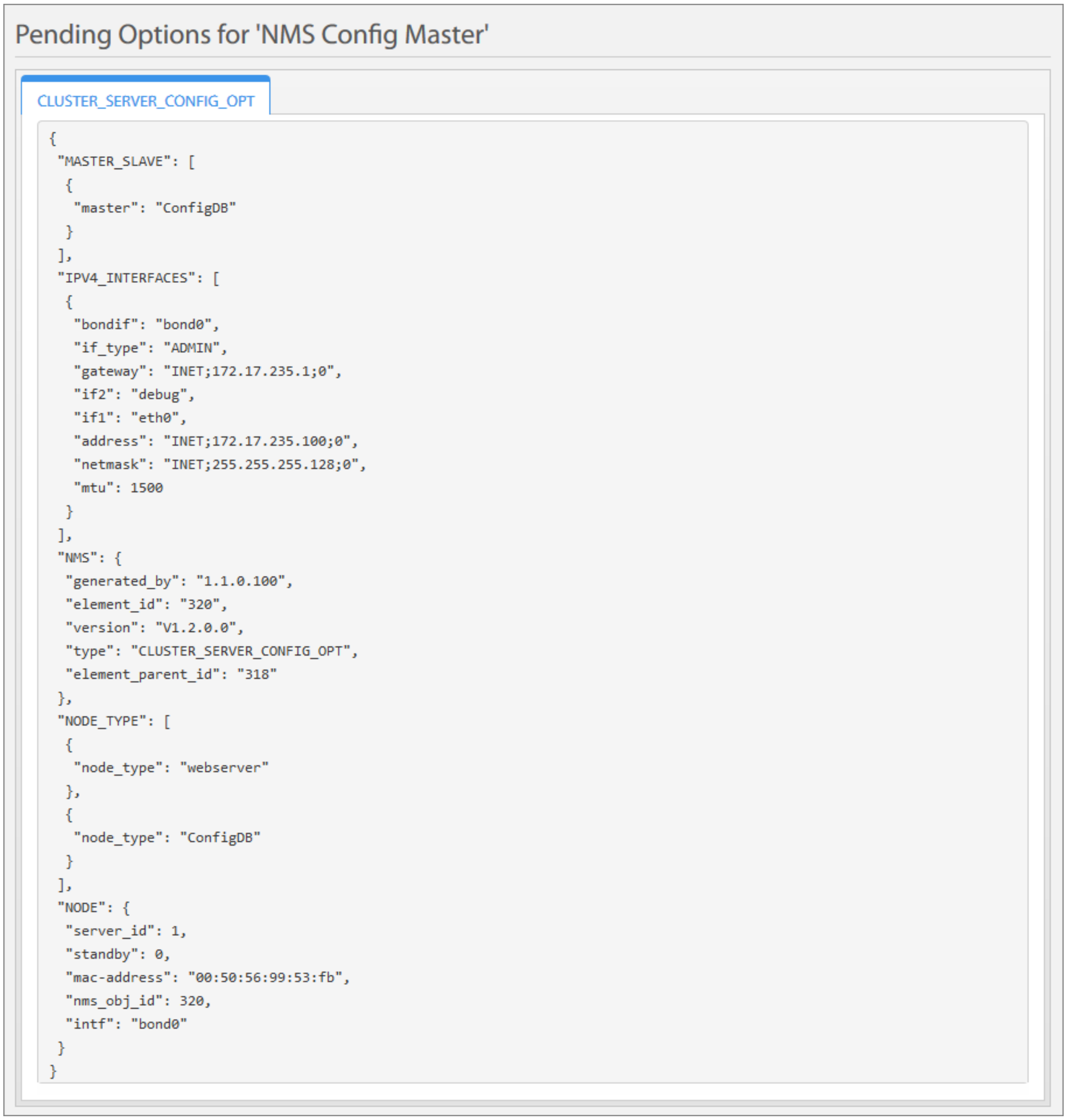
- iNet *
- Linecard *
- NMS Cluster
- NMS Server
- PP Cluster *
- PP Server *
- Terminal
- ASC *

NOTE: Not currently supported in Pulse GUI, and the associated element icon may always show as dark gray.

11.4 Configuration Options Files

An *options file,* in the NMS, contains the configuration parameters of a network element. Network elements such as Terminals and line cards have both an active configuration and a saved or ‘pending’ configuration. The *pending configuration* is the last saved or the configuration that is currently stored in the NMS database. The *active configuration* is the configuration that is resident on the network element.

When the configuration of an element is modified, but not yet applied, the saved configuration is pending. When recent changes are applied, the pending configuration is sent to the element and becomes the active configuration.


Pending Options for 'NMS Config Master'
CLUSTER_SERVER_CONFIG_OPT

```
{
 "MASTER_SLAVE": [
  {
   "master": "ConfigDB"
  }
 ],
 "IPV4_INTERFACES": [
  {
   "bondif": "bond0",
   "if_type": "ADMIN",
   "gateway": "INET;172.17.235.1;0",
   "if2": "debug",
   "if1": "eth0",
   "address": "INET;172.17.235.100;0",
   "netmask": "INET;255.255.255.128;0",
   "mtu": 1500
  }
 ],
 "NMS": {
  "generated_by": "1.1.0.100",
  "element_id": "320",
  "version": "V1.2.0.0",
  "type": "CLUSTER_SERVER_CONFIG_OPT",
  "element_parent_id": "318"
 },
 "NODE_TYPE": [
  {
   "node_type": "webserver"
  },
  {
   "node_type": "ConfigDB"
  }
 ],
 "NODE": {
  "server_id": 1,
  "standby": 0,
  "mac-address": "00:50:56:99:53:fb",
  "nms_obj_id": 320,
  "intf": "bond0"
 }
}
```

Figure 11-2. Retrieve Network Systems Options File

A configuration options file can be retrieved for the following elements:

- Terminal Domain — Satellite Terminal Only
- Physical Domain — All elements except IF Domain, Site SVN, and Global SVN
- Service Domain — All elements except SSPP, and Geographic Region
- Network Domain — iNet Profile, Inroute Group Profile
- Transport Domain — Satellite Only
- System Admin Domain — DDE, Stats, System Monitor, Update Manager, Scheduling

11.5 Applying Configuration Changes

After creating a new element configuration or after making changes to an existing element configuration, those changes, which are referred to as the “pending changes,” must then be applied to the element for the changes to have effect in the network. Configuration changes can be applied to a single element, or in some cases, for elements of the same type, the configuration changes may be simultaneously applied to multiple elements.

To apply configuration changes in the pending options file:

1. Use the appropriate browse command to open the Browse Results window to find a specific network element whose options file is to be retrieved.
2. Select the desired element, click the **Actions** button, and select **Retrieve Pending Option File** to view the most recently saved configurations options file for the element.
3. Select **Apply Configuration** to update the element with its pending changes. The **Impact Analysis** page is displayed to allow the impact of changes to be reviewed before applied. See *Reviewing Impact Analysis of Applying Changes* on page 154.

11.6 Retrieving Configuration Options Files

When modifications are made to the configuration of any element, the changes are saved in the NMS database in the Options file associated with the element. This saved or “Pending Configuration” can be retrieved and viewed before it is applied to the element. The **Retrieve Pending Option File** command is used to get the latest version of an element’s Options file. The **Retrieve Active Option File** command is used to get the Options file that is currently active on an element for viewing.

To retrieve the active or pending options file:

1. Use the appropriate browse command to open the Browse Results window to find a specific network item whose options file is to be retrieved.
2. Select the desired element, click the **Actions** button, and do one of the following:
    a. Select **Retrieve Pending Option File** to view the most recently saved configurations options file for the element.
    b. Select **Retrieve Active Option File** to view the configurations options file that is currently in active operation on the selected element.

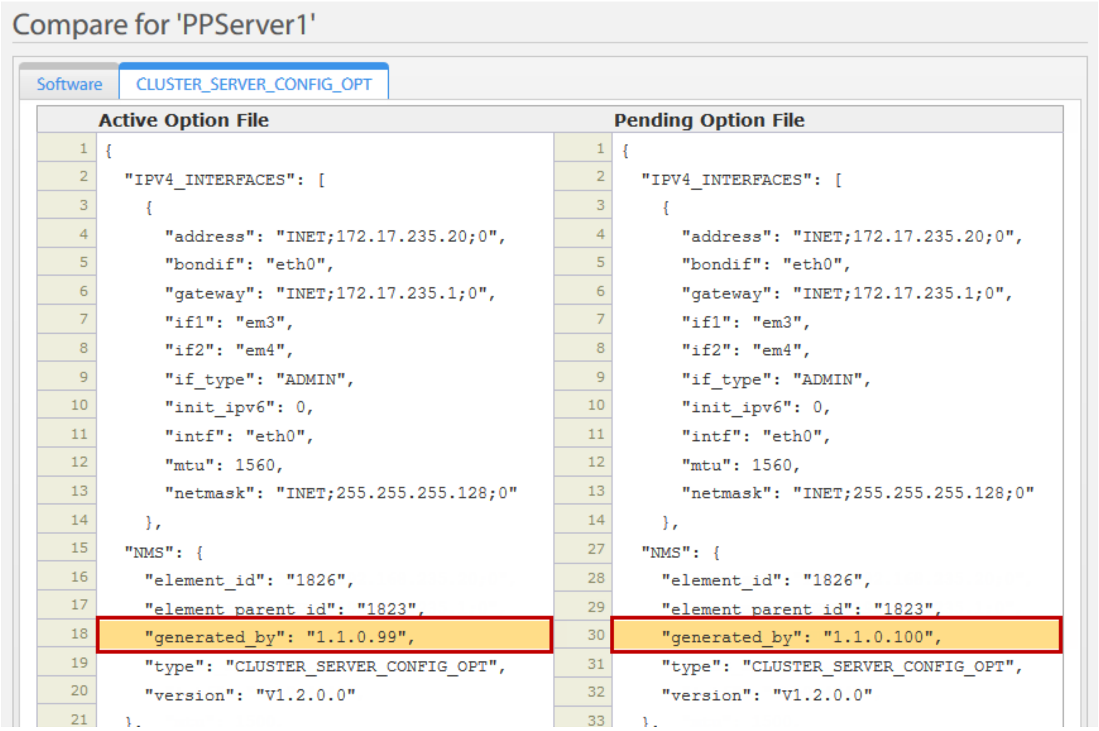
11.7 Comparing Configuration Options Files

Compare Configuration is an Pulse operation that supports side-by-side viewing of the active and pending options file of an element; as well as its manifest and configuration inventory.

The *configuration manifest* is the list of items — for example options files, packages, global PKI, and license files, that are targeted for installation on a particular network element. Each manifest item has a file **Type**, **Name** and **Version.** The *configuration inventory*, on the other hand, is a list of software items that are currently installed on the element. By comparing the manifest files to the inventory files, operators can verify whether all manifest items are installed, the installed version, and whether the file is activated on the network element.

The active and pending options files for an element are compared side-by-side. With the two files displayed side-by-side, recent changes are highlighted in orange to indicate what changes have been made and are different from the currently “Active” configuration.

For those elements for which this operation is supported, for example the **Physical Domain** and **Terminal Domain**, the operation is an element **Action** button option, initiated from the Browse Results window.



Active Option File

```
{
  "IPV4_INTERFACES": [
    {
      "address": "INET;172.17.235.20;0",
      "bondif": "eth0",
      "gateway": "INET;172.17.235.1;0",
      "if1": "em3",
      "if2": "em4",
      "if_type": "ADMIN",
      "init_ipv6": 0,
      "intf": "eth0",
      "mtu": 1560,
      "netmask": "INET;255.255.255.128;0"
    },
  "NMS": {
    "element_id": "1826",
    "element_parent_id": "1823",
    "generated_by": "1.1.0.99",
    "type": "CLUSTER_SERVER_CONFIG_OPT",
    "version": "V1.2.0.0"
  },
```

Pending Option File

```
{
  "IPV4_INTERFACES": [
    {
      "address": "INET;172.17.235.20;0",
      "bondif": "eth0",
      "gateway": "INET;172.17.235.1;0",
      "if1": "em3",
      "if2": "em4",
      "if_type": "ADMIN",
      "init_ipv6": 0,
      "intf": "eth0",
      "mtu": 1560,
      "netmask": "INET;255.255.255.128;0"
    },
  "NMS": {
    "element_id": "1826",
    "element_parent_id": "1823",
    "generated_by": "1.1.0.100",
    "type": "CLUSTER_SERVER_CONFIG_OPT",
    "version": "V1.2.0.0"
  },
```

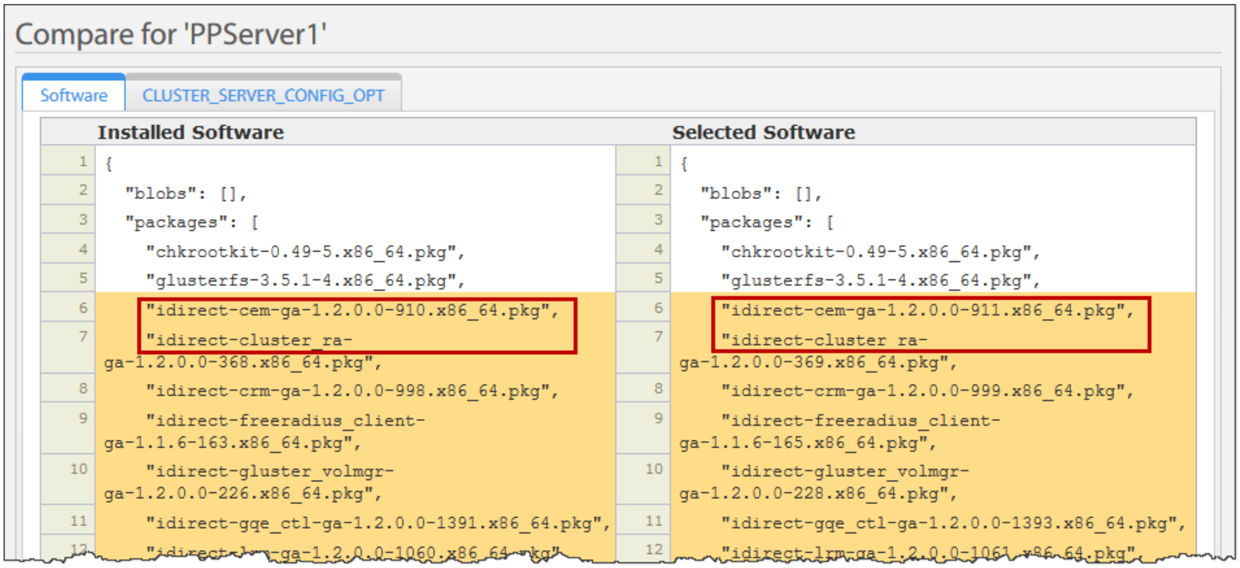
Figure 11-3. Comparing Active and Pending Options Files

To compare configuration files:

1. Use the appropriate **Browse** command to open the Browse Results window to find a specific network item whose configuration files (latest options/active options; manifest/inventory) are to be compared.
2. Select the desired element, click the **Actions** drop-down list and select **Compare Configuration** to view the configuration files side-by-side.

3. Click the **Options** tab (Object_Name_**OPT**) to view the **Active Option File** and **Pending Option File** side-by-side. The lines that are different are highlighted, in red to indicate deleted lines; green to indicate added lines, and orange to indicate modified lines.
4. Click the **Software** tab to view **Installed Software** and **Selected Software** side-by-side.
5. Use the **Back** arrow to return to the **Browse Results** window.

After comparing two files and confirming the changes, then the next step may be to apply the configuration to the element. See *Applying Configuration Changes*.



Installed Software

```
{
  "blobs": [],
  "packages": [
    "chkrootkit-0.49-5.x86_64.pkg",
    "glusterfs-3.5.1-4.x86_64.pkg",
    "idirect-cem-ga-1.2.0.0-910.x86_64.pkg",
    "idirect-cluster_ra-
ga-1.2.0.0-368.x86_64.pkg",
    "idirect-crm-ga-1.2.0.0-998.x86_64.pkg",
    "idirect-freeradius_client-
ga-1.1.6-163.x86_64.pkg",
    "idirect-gluster_volmgr-
ga-1.2.0.0-226.x86_64.pkg",
    "idirect-gqe_ctl-ga-1.2.0.0-1391.x86_64.pkg",
    "idirect-lrm-ga-1.2.0.0-1060.x86_64.pkg",
```

Selected Software

```
{
  "blobs": [],
  "packages": [
    "chkrootkit-0.49-5.x86_64.pkg",
    "glusterfs-3.5.1-4.x86_64.pkg",
    "idirect-cem-ga-1.2.0.0-911.x86_64.pkg",
    "idirect-cluster_ra-
ga-1.2.0.0-369.x86_64.pkg",
    "idirect-crm-ga-1.2.0.0-999.x86_64.pkg",
    "idirect-freeradius_client-
ga-1.1.6-165.x86_64.pkg",
    "idirect-gluster_volmgr-
ga-1.2.0.0-228.x86_64.pkg",
    "idirect-gqe_ctl-ga-1.2.0.0-1393.x86_64.pkg",
    "idirect-lrm-ga-1.2.0.0-1061.x86_64.pkg",
```

Figure 11-4. Comparing Inventory vs. Manifest Using Software Tab

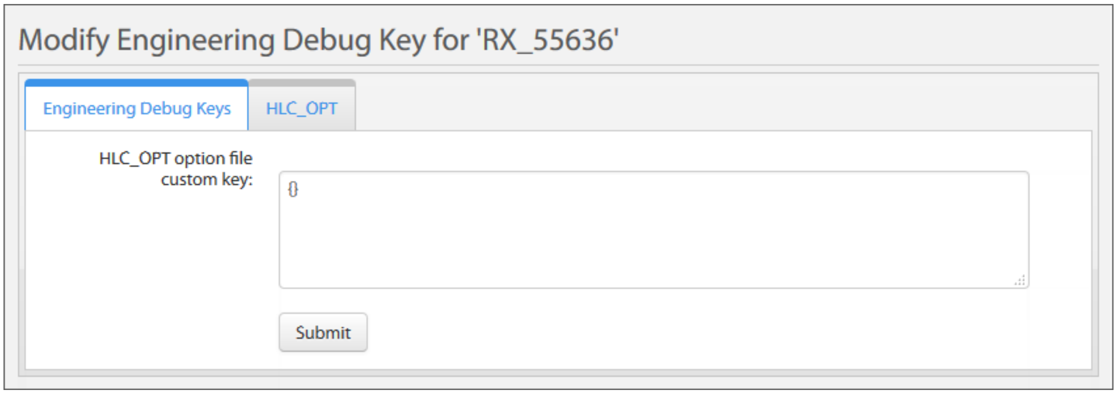
11.8 Modifying Engineering Debug Keys

An *engineering debug key* or *custom key*, is a method by which the functionality of a specific network feature or element is added or modified without adding fields to or modifying the NMS GUI. This method is generally implemented as a temporary debug fix to be later fully-implemented as part of the NMS-generated options file for the feature or element.

Access to the debug key for a specific element, for example a line card, is accessed from the Browse Results window, using the **Actions** drop-down list for the element. The custom key will generally affect specific parameters with specific values.

To modify the custom key for an element:

1. Use the appropriate **Browse** command to open the Browse Results window to find a specific network item whose configuration will be modified using a custom key.
2. Select the desired element, and click the **Actions** drop-down list and select **Modify Engineering Debug Keys** to open to the **Engineering Debug Keys** tab.
3. Click inside the **Custom Key** field to enter the required parameter and values, using appropriate syntax.
4. Click **Submit** to save the entry.



Modify Engineering Debug Key for 'RX_55636'

HLC_OPT option file custom key: {}

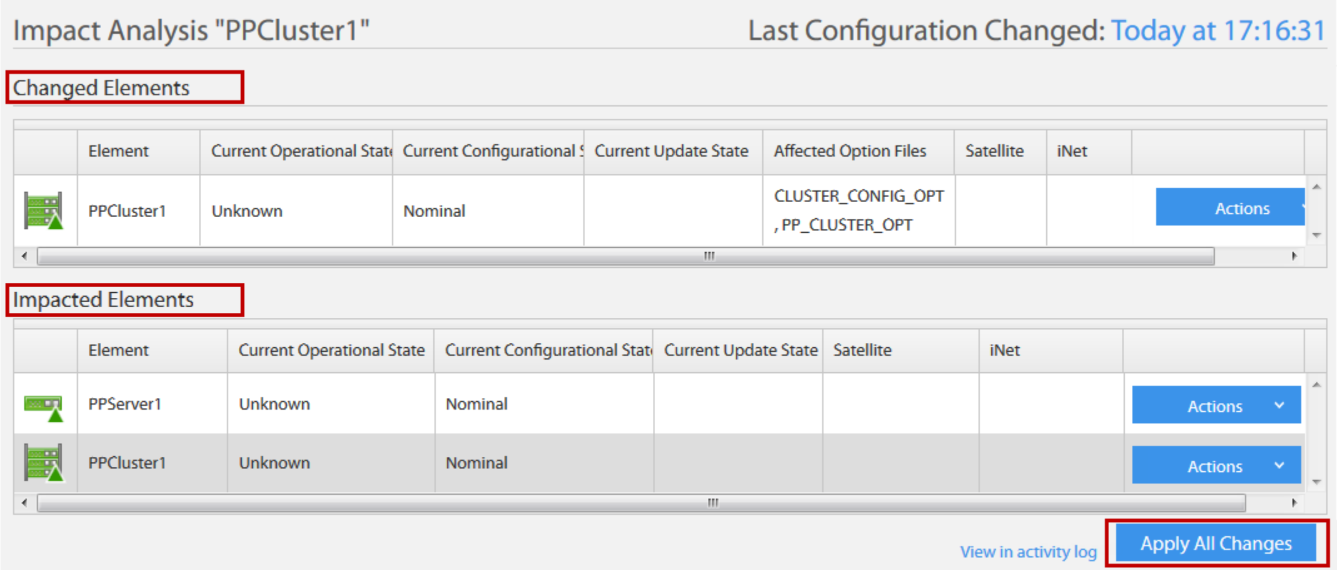
Figure 11-5. Engineering Debug Custom Key Dialog

11.9 Reviewing Impact Analysis of Applying Changes

After modifying the configuration of an element, the changes are saved in the NMS database and the associated Options file for the element is generated. Generally, the next step would be to use the Action command “**Apply Configuration**,” to have the changes take effect.

Prior to applying configuration changes to an element, it is useful to see the impact the change will have on other Options files and elements. Using the NMS **View Impact** operation, it is possible to obtain a summary report of the impact to other elements and Options files.

The **View Impact Analysis** operation can be accessed from the NMS configuration page of an element, where the configuration is saved, or from the **Actions** menu of that element. The user is also automatically redirected to the **Impact Analysis** page whenever the **Apply Changes** action is issued. See **Note**.



Impact Analysis "PPCluster1" Last Configuration Changed: Today at 17:16:31

Changed Elements

	Element	Current Operational Stat	Current Configurational S	Current Update State	Affected Option Files	Satellite	iNet	
	PPCluster1	Unknown	Nominal		CLUSTER_CONFIG_OPT , PP_CLUSTER_OPT			Actions

Impacted Elements

	Element	Current Operational State	Current Configurational Stat	Current Update State	Satellite	iNet	
	PPServer1	Unknown	Nominal				Actions
	PPCluster1	Unknown	Nominal				Actions

Figure 11-6. An Example Impact Analysis Report Page

To retrieve and review the impact analysis:

1. After the initial configuration or configuration changes to an element, for example a PP Cluster, to view the impact of the changes use one of the following methods:
    - a. From the element configuration page click **Save and View Impact**. The **Impact Analysis** page opens. The table shows the **Current Configuration State** of the element and what are the **Affected Options Files**.
    - b. From the Browse result window, find the element, click the **Actions** and select **Impact Analysis**. The **Impact Analysis** page opens. The table shows the **Current Operational State, Current Configuration State, and Configuration Update State** of the element; and the **Affected Options Files**.
2. Under **Changed Elements**, changed elements are listed; Under **Impacted Elements**, the elements that will be impacted are listed.
3. Click **Apply All Changes**, if after a review of the impact analysis the pending changes and impact to other elements and options files is acceptable.

NOTE: When many changes are simultaneously applied, and the data returned exceeds 2MB, the Impact Analysis page is not automatically loaded, as it would be impractical to view all of the impacts.

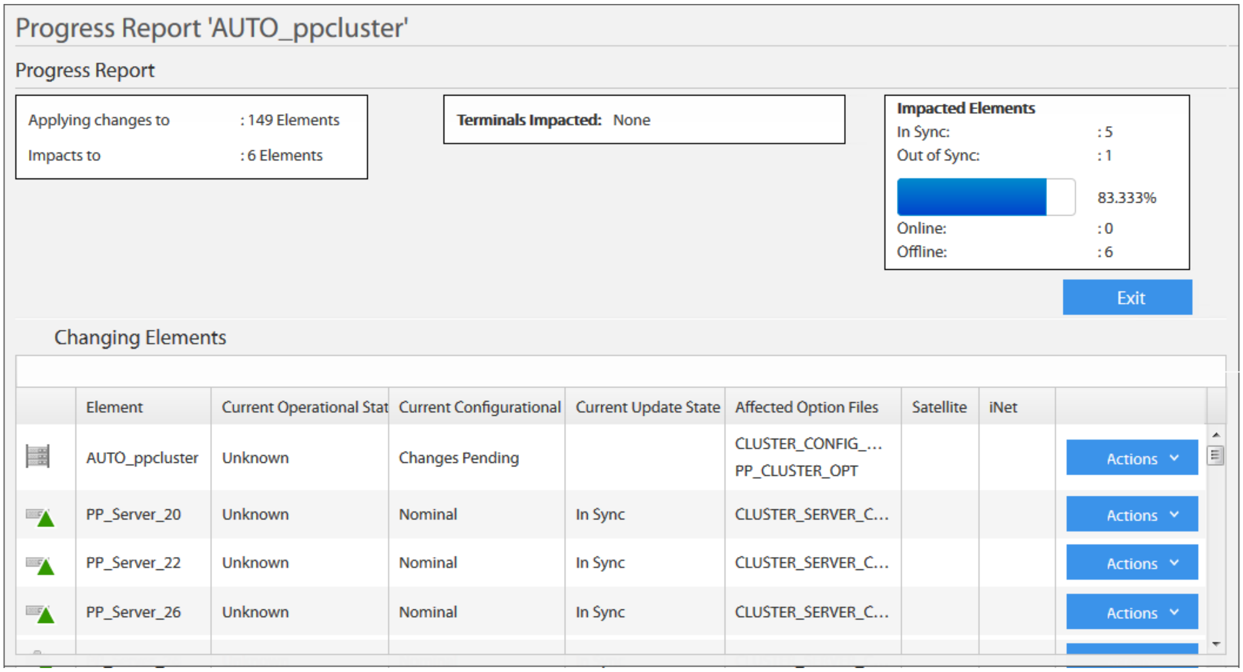
Instead, the user is prompted to confirm to continue with applying changes without redirecting to the Impact Analysis page, and is redirected to the Browse Networks page.

11.10 Review Apply Changes Progress Report

The **View Progress Report** operation, which is obtained by selecting the **View Progress Report** operations from the Actions menu of the particular element, is generally used after applying configuration changes to an element.

When executed, the operation returns a summary report of the operational, update, and configuration states of the elements and the Options files that are affected. The report also shows a count of impacted elements along with a progress bar that indicates whether the Options file has been delivered to the target. This element list also indicates whether impacted elements are **In-Sync** or **Out-of-Sync**.

The report shows the total number of elements for which changes are being applied; the number of other elements that on which there is an impact; a list of satellite terminals impacted; and a progress bar that shows the percentage of the total number of Update Manager actions items that are completed.



Progress Report 'AUTO_ppcluster'

Progress Report

Applying changes to : 149 Elements

Impacts to : 6 Elements

Terminals Impacted: None

Impacted Elements

In Sync: : 5

Out of Sync: : 1

83.333%

Online: : 0

Offline: : 6

Changing Elements

	Element	Current Operational Stat	Current Configurational	Current Update State	Affected Option Files	Satellite	iNet	
	AUTO_ppcluster	Unknown	Changes Pending		CLUSTER_CONFIG_... PP_CLUSTER_OPT			Actions
	PP_Server_20	Unknown	Nominal	In Sync	CLUSTER_SERVER_C...			Actions
	PP_Server_22	Unknown	Nominal	In Sync	CLUSTER_SERVER_C...			Actions
	PP_Server_26	Unknown	Nominal	In Sync	CLUSTER_SERVER_C...			Actions

Figure 11-7. Example Progress Report Page

To retrieve and review the progress report:

1. Use the appropriate browse command to open the Browse Results window to find and select a specific network item for which a progress report is required.
2. Click **Actions** and select **Progress Report**.
3. When done, click **Exit** to close the page and return to the Browse objects page.

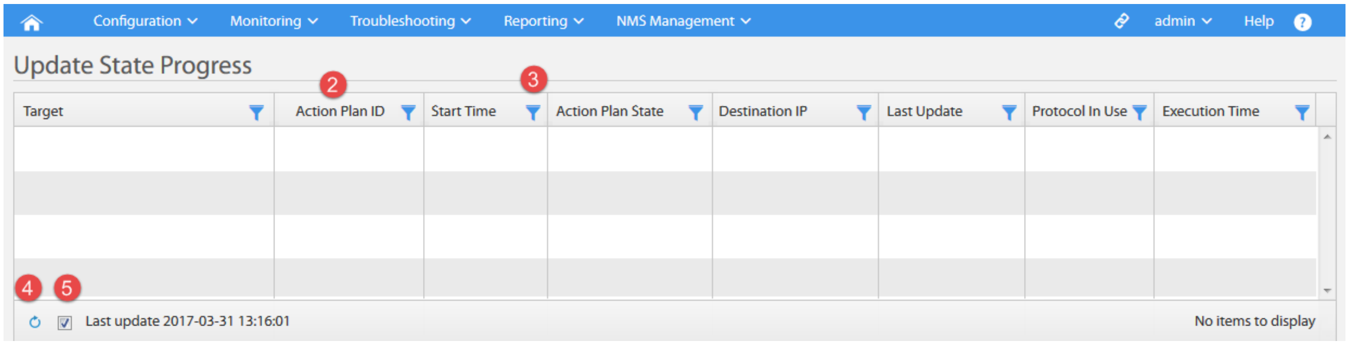
11.11 View Update State Progress

In an iDirect Network system, a network operator can use the NMS **Update State Progress** page to view, track, and debug in-progress configuration updates.

The **View Update State Progress** page is accessed from the Configuration tab, under Configuration Management.

From the **Update State Progress** page, users are able to view the real-time progress of all in-progress actions for all elements. The data is automatically refreshed every 30 seconds, and includes the following information about the progress of current configuration action plans:

- **Target** — The target elements associated with given Action Plans
- **Action Plan ID** — Action plan identifier
- **Start Time** — The Start Time of an Action Plan
- **Action Plan State** — Unknown, Waiting for Authorization, In Execution, Waiting Resync Inventory, All Targets in Sync/Action Plan Succeeded, Transaction Timeout
- **Last Update** — Date and Time of last update of action plan item
- **Protocol In Use** — The transmission protocol in use (TCP, UDP)
- **Execution Time** — Time to complete action



Update State Progress

Target	Action Plan ID	Start Time	Action Plan State	Destination IP	Last Update	Protocol In Use	Execution Time

☑ Last update 2017-03-31 13:16:01

No items to display

Figure 11-8. Activity Log Records

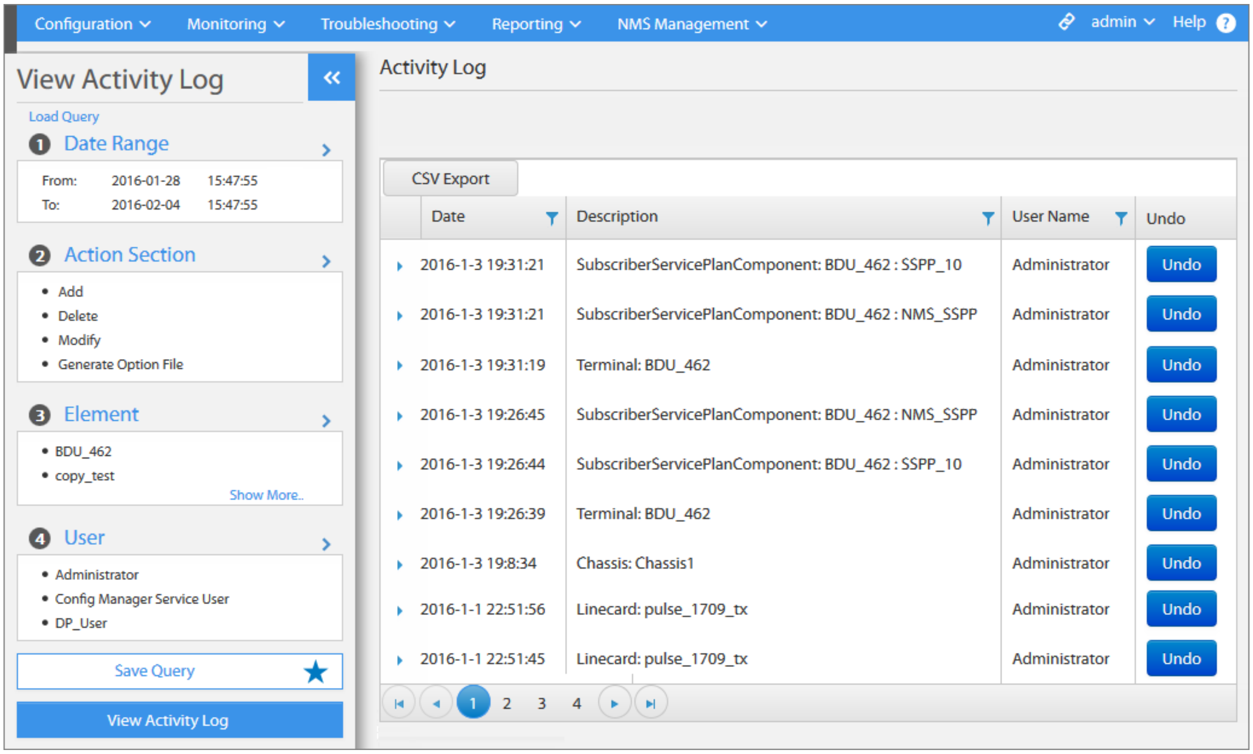
To undo configuration changes:

1. Click the **Configuration** tab >**Configuration Management > View Update State Progress**.
2. Click a column header to sort list on that column.
3. Use column filter icons to narrow list as required.
4. Click the refresh icon to update the report.
5. Select the refresh check box to enable continuous update.
6. Drag and drop columns in new position as required.

11.12 Viewing the Activity Log

The Pulse NMS maintains an *activity log* that records the time and details of each activity, whether performed by a human or machine user. NMS activities include basic operations such as login, logout, add, delete, and modify, as well as other operations. Each activity is logged with a **Date**, **Description**, and **User Name**. Using the Configurator Panel, the activity log report can be retrieved based on the following user specifications:

- A specific time frame, using the **Date Range** selector
- A specific **Action Type**, using the **Action** selector
- Involving a specific element or elements, using the **Element** selector
- A specific user, or all users, using the **User** selector



From: 2016-01-28 15:47:55
To: 2016-02-04 15:47:55

- Add
- Delete
- Modify
- Generate Option File

- BDU_462
- copy_test

- Administrator
- Config Manager Service User
- DP_User

Date	Description	User Name	Undo
2016-1-3 19:31:21	SubscriberServicePlanComponent: BDU_462 : SSPP_10	Administrator	Undo
2016-1-3 19:31:21	SubscriberServicePlanComponent: BDU_462 : NMS_SSPP	Administrator	Undo
2016-1-3 19:31:19	Terminal: BDU_462	Administrator	Undo
2016-1-3 19:26:45	SubscriberServicePlanComponent: BDU_462 : NMS_SSPP	Administrator	Undo
2016-1-3 19:26:44	SubscriberServicePlanComponent: BDU_462 : SSPP_10	Administrator	Undo
2016-1-3 19:26:39	Terminal: BDU_462	Administrator	Undo
2016-1-3 19:8:34	Chassis: Chassis1	Administrator	Undo
2016-1-1 22:51:56	Linecard: pulse_1709_tx	Administrator	Undo
2016-1-1 22:51:45	Linecard: pulse_1709_tx	Administrator	Undo

1 2 3 4

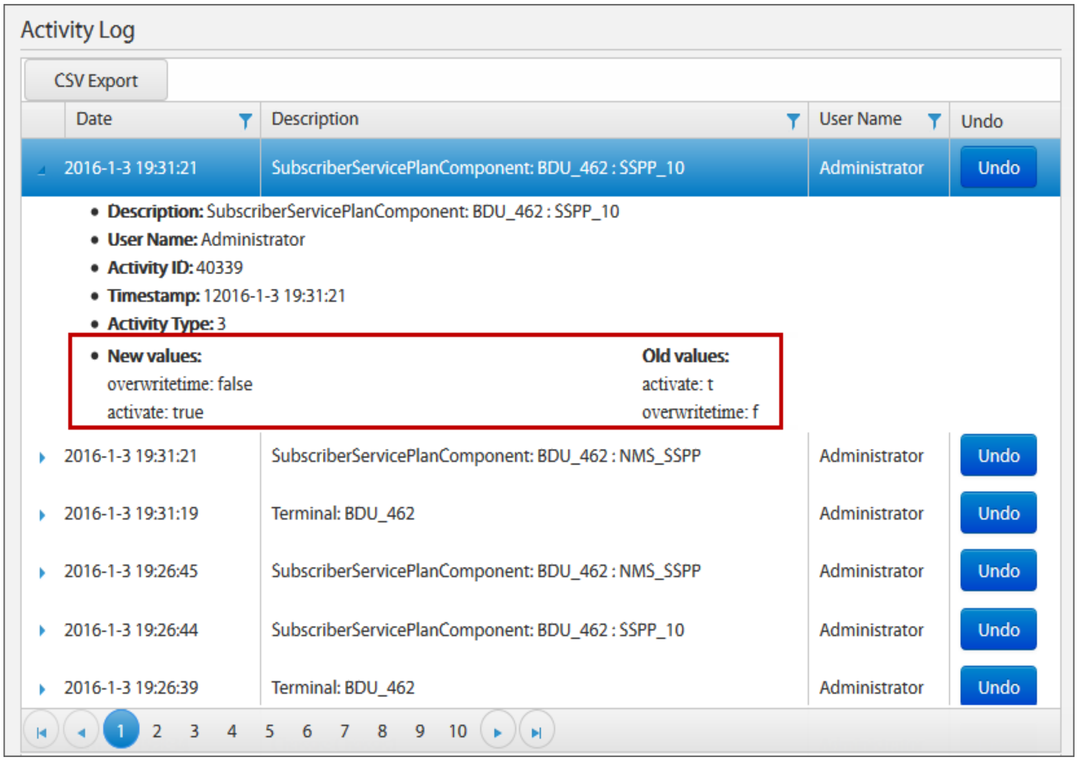
Figure 11-9. View Activity Log

When setting the Configurator parameters, to retrieve the activity log, the **Date Range**, **Action Type**, **Element**, and **User** may be specified singularly, or combined as filters. If only the **Date Range** is applied, for example, the entire activity log is retrieved for a specified period. For most elements, a maximum of three months of changes are retained; this period is much less for more complex objects like Satellite Terminal or Group Service Plan.

The activity log is accessed directly from the NMS **Configuration** tab under **Configuration Management,** or using the **Activity Log** button located on the **View Object** page for any physical or logical infrastructure object — for example from **View Line Card**.

To view the activity log:

1. Click the **Configuration** tab > **Configuration Management > Activity Log.**
2. Click the **Load Query** link if a previously saved query is to be loaded.
3. Click the **Date Range** bar, to enter a period for which to view the activity log. Use a date/time range or specify any one of the pre-defined periods.
4. Click the **Action Section**, and then click the **Action Type** drop-down list and select one or more action types for which to search. For example, choose **Login**, **Logout**, Add, **Delete**, **Modify**, **Change Permission**, **Generate Option File,** or select all of the actions.
5. Click **Element** to select one or more specific elements for which associated activities should be retrieved. Leave this field blank to retrieve activity of all NMS elements.
6. Click the **User bar**, find and select one or more users by which to filter the query. Leave this field blank to retrieve activity by all NMS users.
7. Click the **View Activity Log** button to retrieve the activity log viewer report.
8. Click the blue triangle icon to the left of an activity, to expand and view the details. This view shows the details of an activity or change. The **New Values** column show the changed values; the **Old Values** column show values prior to change.
9. Click the associated **UNDO** button to revert a change to the previous configuration.
10. Click **Save Query**, to save the activity log view for future use.



Date	Description	User Name	Undo
2016-1-3 19:31:21	SubscriberServicePlanComponent: BDU_462 : SSPP_10	Administrator	Undo

- **Description:** SubscriberServicePlanComponent: BDU_462 : SSPP_10
- **User Name:** Administrator
- **Activity ID:** 40339
- **Timestamp:** 12016-1-3 19:31:21
- **Activity Type:** 3
- **New values:** overwritetime: false activate: true **Old values:** activate: t overwritetime: f

Date	Description	User Name	Undo
2016-1-3 19:31:21	SubscriberServicePlanComponent: BDU_462 : NMS_SSPP	Administrator	Undo
2016-1-3 19:31:19	Terminal: BDU_462	Administrator	Undo
2016-1-3 19:26:45	SubscriberServicePlanComponent: BDU_462 : NMS_SSPP	Administrator	Undo
2016-1-3 19:26:44	SubscriberServicePlanComponent: BDU_462 : SSPP_10	Administrator	Undo
2016-1-3 19:26:39	Terminal: BDU_462	Administrator	Undo

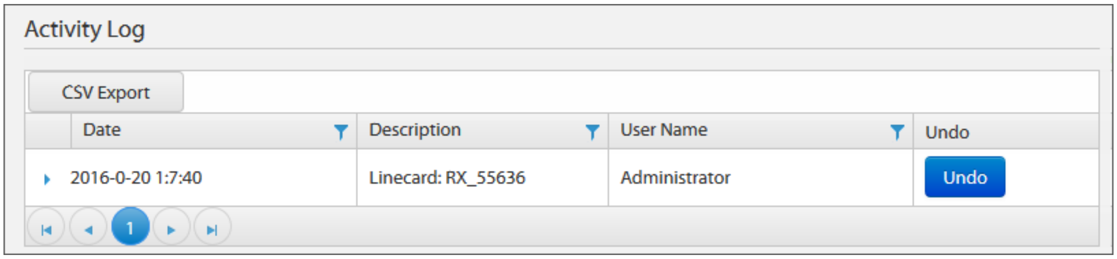
Figure 11-10. Activity Log - Expanded View

11.13 Undoing Changes from a View Object Page

In an iDirect Network system, *configuration rollback* is the process of undoing previously made additions, deletions, or modifications to the configuration of an element. Undoing a change reverts to the most recent configuration prior to the last change.

Although most configuration changes are possible, undoing more complex changes, such as a change that deleted a parent node in a hierarchy, may not always be possible. Prior to accepting a complex configuration change that cannot be undone, the NMS issues a warning that allows users to abort the operation before it is saved.

Configuration rollback is carried out from the NMS Activity Log, which can be accessed directly by using the **Activity Log** command, on the Configuration management menu; or it can be accessed directly for a specific element, using the **View Object** operation from the **Actions** menu of the element when the element is displayed in the Browse window.



Activity Log

CSV Export

Date	Description	User Name	Undo
2016-0-20 1:7:40	Linecard: RX_55636	Administrator	Undo

Figure 11-11. Activity Log Records

To undo configuration changes:

1. Click the **Configuration** tab, and from the desired element domain, select one of the **Browse** commands to return a list of configured elements from the NMS — for example **Physical Domain, Transport Domain**, or **Terminal Domain**.
2. Click in the **Search** field, and start typing an **Element Name**, **DID**, or **IP Address**.
3. Select the desired element, if in view, or use one of the additional filtering methods to narrow the search results.
   - **a.** Use the **Element Type** to display only elements of the selected type.
   - **b.** Use the **Operational** to display only elements currently in the selected operational state. For example — only **Online** elements.
   - **c.** Use the **Config/Update** drop-down to display only elements currently in the selected configuration state. For example — only list elements that have **Changes Pending**.
4. Select the target element when it appears.
5. Click the **Actions** button for the desired element, and select **View Object** — for example, **View Chassis.** The element configuration dialog is opened in a read-only view.
6. Click the element **Activity Log** button at the page bottom.
7. Click the associated **UNDO** button to revert the previous configuration for the element.

12 Monitoring Operations

Pulse NMS Monitoring operations provide network operators with real-time views of network events, alarms, and incidents. Also available are real-time status reports that report on the real-time state of network elements; and real-time statistics reports of the operational and performance of both physical and logical network elements.

Pulse Monitoring operations are covered in the following topics:

12.1 Pulse Real-Time Monitoring Operations

The operations of the **NMS Monitoring** tab are divided into five sub-menus. These operations categories are briefly described as follows:

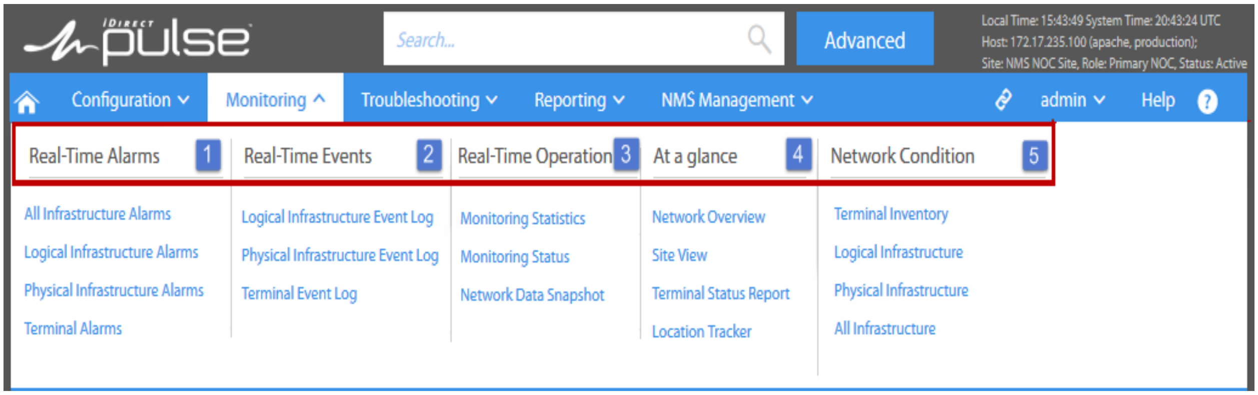


Figure 12-1. Pulse Monitoring Menu Operations

iDirect Pulse Monitoring operations supports the following types of real-time requests:

The operations of the **NMS Monitoring** tab are divided into five sub-menus. These operations categories are briefly described as follows:

- **Real-Time Alarms** — These operations are used to automatically obtain a report of current network alarms based on the selected operation — for example, all alarms; all physical infrastructure alarms; a logical infrastructure elements; or all terminal alarms.
- **Real-Time Events** — These operations are used to automatically obtain a report of current network events for the selected object type — for example, all logical infrastructure events; all physical infrastructure events; or all terminal events.
- **Real-Time Operation** — With these tools you can monitor the real-time discrete status of any one or more elements, for example terminal Fan Status, current beam, or current channel; or capture operational statistics of one or more elements, for example, total data volume transmitted, or total data volume received.
- **At a Glance** — These operations are used to obtain a real-time view of the status of network infrastructure elements, either from a remote-side view, a hub-side view, or an network view.
- **Network Condition** — These operations provide a quick access point to shortcuts to browse listings of physical and logical infrastructure elements and terminal elements.

12.2 NMS Events, Alarms, and Incidents

In an iDirect network, an *event* is as a noteworthy condition associated with a physical or logical network element, which should be logged. Thus, events may be raised by software exceptions, actions in the network (such as terminal registration), hardware monitoring results, and many other conditions. In the iDirect network, events are what trigger alarms. An example of an event is "latency above threshold."

Broadly speaking, an *alarm* is a condition that is important enough to bring to the attention of the network operator, and generally needs some corrective action or further investigation. Each alarm is a state condition triggered by the occurrence of one or more specific network events. Alarms are triggered for physical and logical infrastructure elements, including the satellite terminal. An example of an alarm is "latency high."

An i*ncident* is a condition that is triggered by the occurrence of two or more specific alarms, and is derived by the NMS or is manually defined and created by a user. Incidents and alarms are essentially the same object type, which makes it possible for an incident that consists of a set of multiple alarms and/or other incidents.

12.3 Severity Levels of Events, Alarms, and Incidents

Each network alarm has an associated severity level — for example a *Warning*, *Minor*, *Major*, or *Critical*. The display of events, alarms, and incidents, in the associated report, is color-coded based on the condition severity. Generalized definitions for these severity levels are given in the table below.

An alarm is normally removed from the display when the triggering fault condition has cleared and the operator has acknowledged the alarm. From the NMS, the operator is able to acknowledge alarms and update alarms in a variety of ways, including the reset of an alarm, which is a manual "force clearing" of the alarm or an overriding of the alarm indication.

Table 12-1. NMS Monitoring Sub-Menus

Severity	Severity Icon/Color	Brief Description
Indeterminate	Indeterminate	this level of severity indicates that the state of the condition cannot be determined by the system.
Informational	Informational	this level of severity is used for operator information only and has no implication of network problems.
Warning	Warning	at this severity level, the system continues to operate, but is impacted in some non-urgent manner.
Minor	Minor	at this severity level, the system continues to operate, but has a fault or misconfiguration.
Major	Major	at this severity level, there is a serious fault that will impact nominal operation.
Critical	Critical	at this level, a condition is causing an immediate impact on the health and functionality of the system and must be addressed immediately.

12.4 Real-Time Network Alarms

The **Real-Time Alarms** monitoring operations provide access to real-time reporting of network alarms associated with logical and physical infrastructure elements, and terminal elements. When one of these reports is generated, the **NMS** automatically opens to a display of all alarms found in the NMS, based on the selected operation and on the default presets for the Status View.

The **Date Range** is preset to the current date, the current time, and **Stream** is ON to allow new alarms to display as they occur. The **Elements** selector is set to **Select All**, to include alarms triggered by all elements of the selected operation (for example all logical); and **Severity** is preset to include all levels. Finally, the **Status View** is default settings of **State**, **Latched State**, **Acknowledgment**, and **Alarm/Incident** are all set to **Select All**.

Based on the selected operation, the report produces a streaming Alarms Report of all alarms of the selected type. The report will include all **Severity** levels; all **Raised** and **Cleared** alarms**;** and all alarms that are **Acknowledged** and that are **Un-Acknowledged** as they occur.

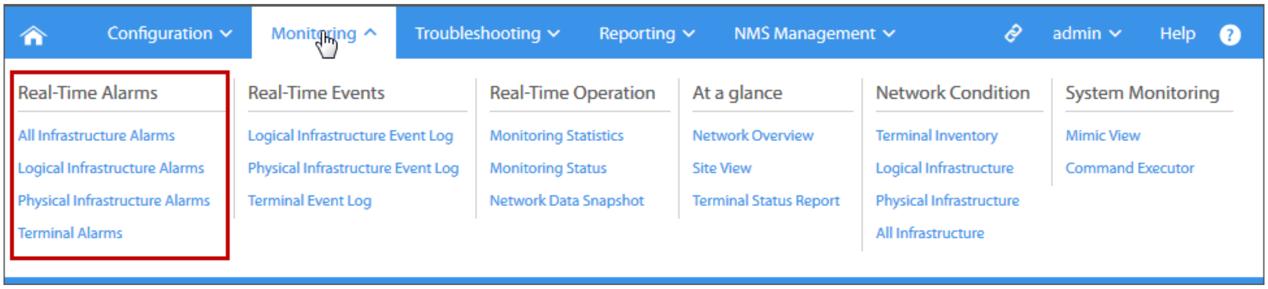


Figure 12-2. Pulse Monitoring Menu - Real-Time Alarms Operations

To monitor network alarms in real-time:

1. Click the **Monitoring** tab > **Real-Time Alarms**, then select one of the following:
   a. **All Infrastructure Alarms:** to display all infrastructure alarms found in the NMS.
   a. **Logical Infrastructure Alarms:** to display all alarms found in the NMS, associated with logical infrastructure elements such as Beams, Channels, iNets, and Carriers.
   b. **Physical Infrastructure Alarms:** to display all alarms found in the NMS, associated with physical infrastructure elements such as Line Cards, Servers, or Chassis.
   c. **Terminal Alarms:** to display alarms found in the NMS associated with all Terminals.
2. Click on a column heading, for example **Element Name** to sort if necessary.
3. Click on a filter icon, for a column, to filter the list of displayed alarms if necessary.
4. See *Alarms Monitoring in Status View*, and *Expanding the Status View* for further details.
5. See *Managing Network Events, Alarms, and Incidents*, for instructions on using the **Attach**, **Create**, and **Update** buttons.

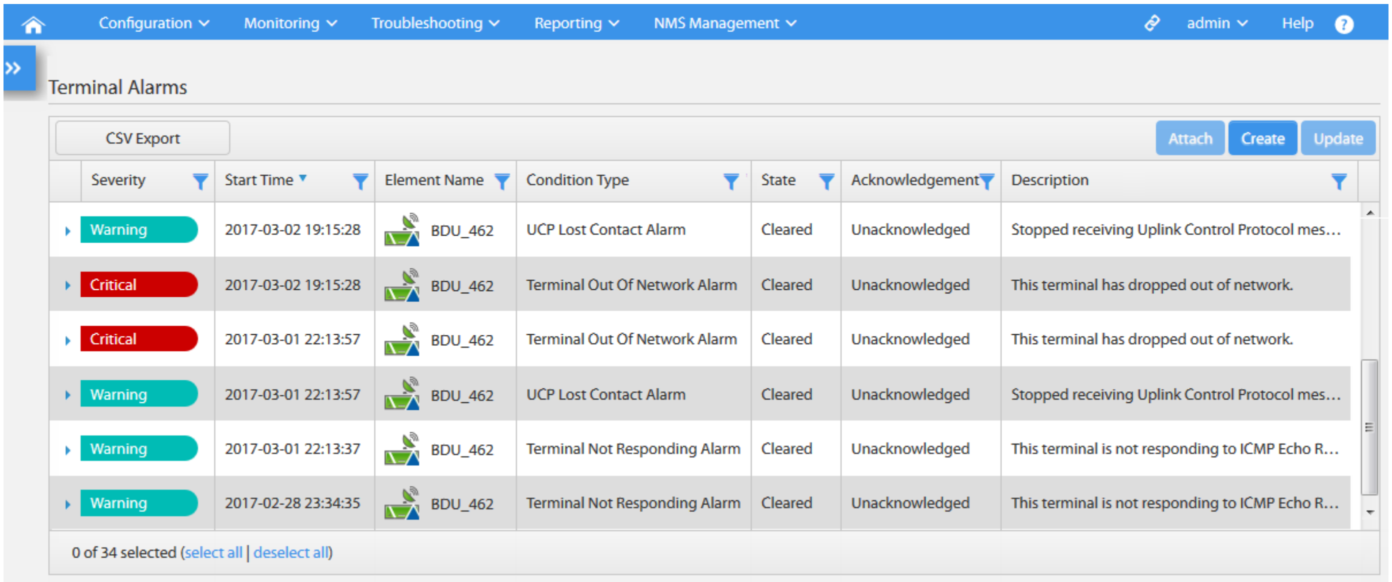
If more than 500 alarms were found, then the oldest alarms are removed from the list. Filtering may be required to ensure that specific alarms are listed and not removed.

12.4.1 Alarms Monitoring in Status View

The **Status View** is presents a listing of network alarms, in real-time, indicating whether an alarm is **Acknowledged** or **Unacknowledged**, still **Raised** or **Cleared**.

Alarms are listed in a grid, with each entry listed in a row, ordered by most recent listed first. Each row has default columns including **Severity**, **Start Time** (time of occurrence), **Element Name**, **Condition Type**, **State**, **Acknowledgment** status, and **Description**. From this view, additional information about an element can be accessed by clicking on the element icon.

A brief description of the default columns of the **Status View** is provided below:



Severity	Start Time	Element Name	Condition Type	State	Acknowledgement	Description
Warning	2017-03-02 19:15:28	BDU_462	UCP Lost Contact Alarm	Cleared	Unacknowledged	Stopped receiving Uplink Control Protocol mes…
Critical	2017-03-02 19:15:28	BDU_462	Terminal Out Of Network Alarm	Cleared	Unacknowledged	This terminal has dropped out of network.
Critical	2017-03-01 22:13:57	BDU_462	Terminal Out Of Network Alarm	Cleared	Unacknowledged	This terminal has dropped out of network.
Warning	2017-03-01 22:13:57	BDU_462	UCP Lost Contact Alarm	Cleared	Unacknowledged	Stopped receiving Uplink Control Protocol mes…
Warning	2017-03-01 22:13:37	BDU_462	Terminal Not Responding Alarm	Cleared	Unacknowledged	This terminal is not responding to ICMP Echo R…
Warning	2017-02-28 23:34:35	BDU_462	Terminal Not Responding Alarm	Cleared	Unacknowledged	This terminal is not responding to ICMP Echo R…

0 of 34 selected (select all | deselect all)

Figure 12-3. Viewing Alarms in Status View

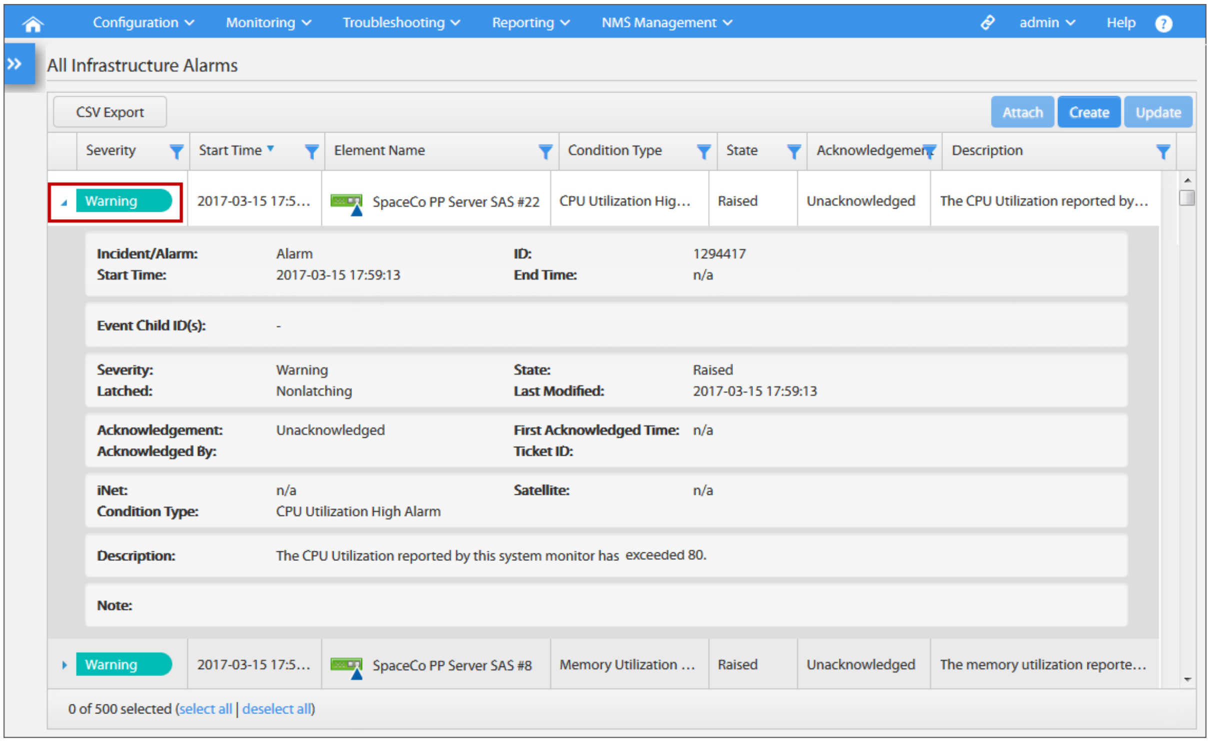
A brief description of each **Status View** default column is provided below:

- **Severity:** NMS assigned levels of severity of an alarm condition. The levels are *Informational*, *Warning*, *Minor*, *Major*, *Critical*, and *Indeterminate*.
- **Start Time:** the date/time at which the alarm/incident was logged in the NMS.
- **Element Name:** the NMS configured name of the element associated with this alarm.
- **Condition Type:** one of several NMS classifications of alarm conditions.
- **State:** state of an alarm. **Raised** indicates the alarm is still present; **Cleared** indicates the alarm has gone away automatically or as the result of operator intervention.
- **Acknowledgment:** indicates the current operator response to an alarm. Possible responses include **Acknowledged**, and **Unacknowledged**.
- **Description:** a brief explanation of the alarm.
- **CSV Export:** initiates export of the alarms report to a CSV file.

12.4.2 Expanding the Status View

An expanded **Status View** of an individual Alarm record can be viewed by clicking the **Show/Hide** icon located just to the left of each Alarm. The icon is used to toggle between a normal and expanded record, to show or to hide the expanded Alarm properties detail.

A brief description of the expanded fields of the **Status View** is provided below:



Severity	Start Time	Element Name	Condition Type	State	Acknowledgement	Description
Warning	2017-03-15 17:5…	SpaceCo PP Server SAS #22	CPU Utilization Hig…	Raised	Unacknowledged	The CPU Utilization reported by…
Warning	2017-03-15 17:5…	SpaceCo PP Server SAS #8	Memory Utilization …	Raised	Unacknowledged	The memory utilization reporte…

Incident/Alarm: Alarm
ID: 1294417
Start Time: 2017-03-15 17:59:13
End Time: n/a
Event Child ID(s): -
Severity: Warning
State: Raised
Latched: Nonlatching
Last Modified: 2017-03-15 17:59:13
Acknowledgement: Unacknowledged
First Acknowledged Time: n/a
Acknowledged By:
Ticket ID:
iNet: n/a
Satellite: n/a
Condition Type: CPU Utilization High Alarm
Description: The CPU Utilization reported by this system monitor has exceeded 80.
Note:

0 of 500 selected (select all | deselect all)

Figure 12-4. Status View - Expanded Details

- **Incident/Alarm:** indicates whether the condition is classified as an alarm or incident.
- **ID:** the identification number assigned to an alarm/incident.
- **End Time:** the date/time at which the alarm/incident was cleared in the NMS.
- **Event Child ID(s):** one or more child events that trigger the alarm/incident.
- **Latched:** indicates whether the alarm/incident is “Latched,” “Unlatched,” or whether the object is configured as a “Non-latching” alarm/incident. See *Creating an Alarm*.
- **Last Modified:** the date and time the severity of this alarm/incident was last modified.
- **First Acknowledged Time:** the time the alarm/incident was first acknowledged.
- **Acknowledged By:** the user that acknowledged occurrence of the alarm/incident.
- **Ticket ID:** the ticket number assigned to this issue, if applicable.
- **iNet:** the iNet in which this alarm/incident occurred, if applicable.
- **Satellite:** the satellite in which this alarm/incident occurred, if applicable.
- **Note:** an operator entered note, regarding the occurrence of this alarm/incident.

12.5 Real-Time Network Events

The **Real-Time Events** monitoring operations, of the Pulse **Monitoring** menu, provide access to reporting of network events associated with logical and physical infrastructure elements, and with terminal elements. When one of these operations is selected, the NMS automatically opens to a real-time display of triggered events found in the NMS, based on the selected operation and on the default presets for the Log View.

The **Date Range** is preset to the current date, the current time, and **Stream** is ON to allow new alarms to display as they occur. The **Element Selector** is set to **Select All**, to include the events triggered by all elements of the selected operation (for example all physical); and **Severity** is preset to include all levels. Finally, the **Log View** default setting for the **Condition Type** is set to **Select All**, to thereby report all network events for all condition types.

Based on the selected operation, the report produces a streaming Events Report of all events of the selected type. The report will include all **Severity** levels and all **Condition Types** as they occur.

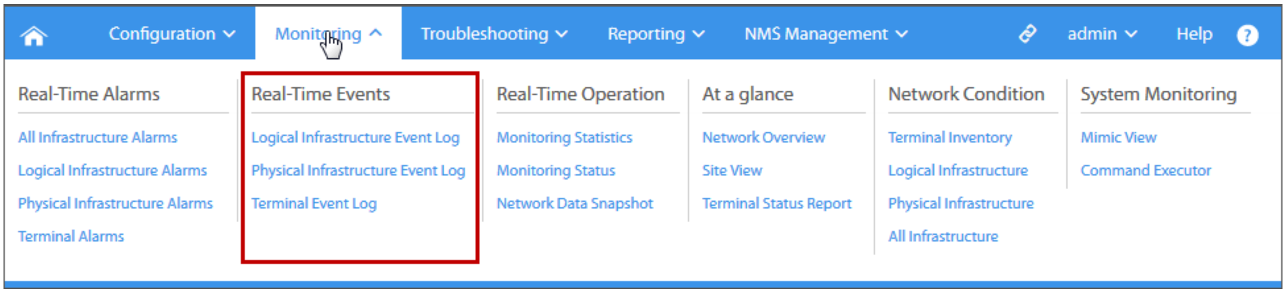


Figure 12-5. Pulse Monitoring Menu - Real-Time Events Operations

To monitor network events in real-time:

1. Click the **Monitoring** tab > **Real-Time Events**, then select one of the following:
    a. **Logical Infrastructure Event Log:** to display all events found in the NMS, associated with logical infrastructure elements such as Beams, Channels, iNets, and Carriers.
    b. **Physical Infrastructure Event Log:** to display all events found in the NMS, associated with physical infrastructure elements such as Line Cards, Servers, or Chassis.
    c. **Terminal Event Log:** to display all events in the NMS associated with Terminals.
2. Click on a column heading, for example **Severity** or **Element Name,** to sort if necessary.
3. Click on a filter icon, for a column, to filter the list of displayed events if necessary.
4. See *Events Monitoring in Log View*, and *Expanding the Log View* for additional details.
5. See *Managing Network Events, Alarms, and Incidents*, for instructions on using the **Attach** button with a selected Event.

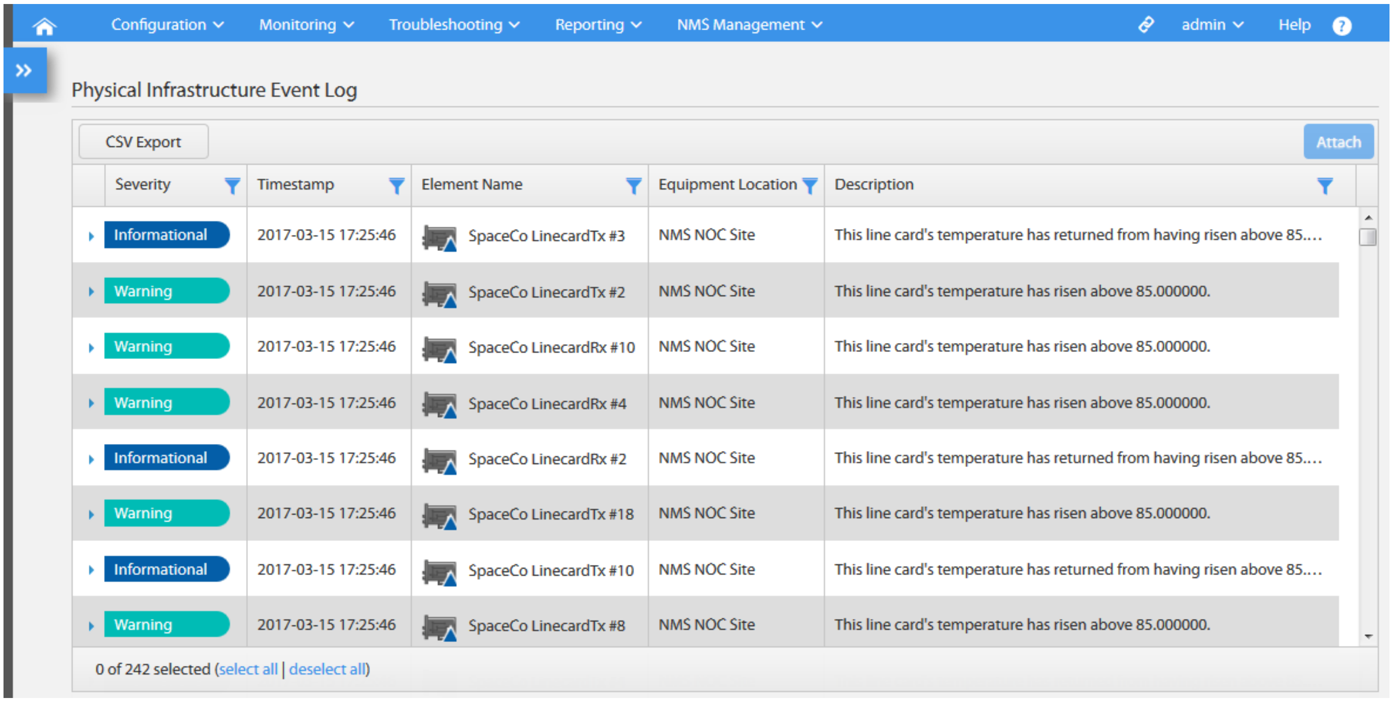
A maximum of 500 events are displayed. Filtering may be required to ensure that specific events are listed and not removed, because of the display limitation.

12.5.1 Events Monitoring in Log View

The **Log View** is present a log listing of network events in real-time. In general, events trigger alarms and events clear alarms.

Events are listed in a grid format, with each entry listed in a row, with defaults columns that include event **Severity**, **Timestamp**, **Element Name**, **Equipment Location**, and **Description**. The actual placement of each **Log View** column is also user-configurable by dragging a column to a new location. From this view, additional information about an element can be accessed by clicking on the element icon.

A brief description of the default columns of the **Log View** is provided below:



Severity	Timestamp	Element Name	Equipment Location	Description
Informational	2017-03-15 17:25:46	SpaceCo LinecardTx #3	NMS NOC Site	This line card's temperature has returned from having risen above 85....
Warning	2017-03-15 17:25:46	SpaceCo LinecardTx #2	NMS NOC Site	This line card's temperature has risen above 85.000000.
Warning	2017-03-15 17:25:46	SpaceCo LinecardRx #10	NMS NOC Site	This line card's temperature has risen above 85.000000.
Warning	2017-03-15 17:25:46	SpaceCo LinecardRx #4	NMS NOC Site	This line card's temperature has risen above 85.000000.
Informational	2017-03-15 17:25:46	SpaceCo LinecardRx #2	NMS NOC Site	This line card's temperature has returned from having risen above 85....
Warning	2017-03-15 17:25:46	SpaceCo LinecardTx #18	NMS NOC Site	This line card's temperature has risen above 85.000000.
Informational	2017-03-15 17:25:46	SpaceCo LinecardTx #10	NMS NOC Site	This line card's temperature has returned from having risen above 85....
Warning	2017-03-15 17:25:46	SpaceCo LinecardTx #8	NMS NOC Site	This line card's temperature has risen above 85.000000.

0 of 242 selected (select all | deselect all)

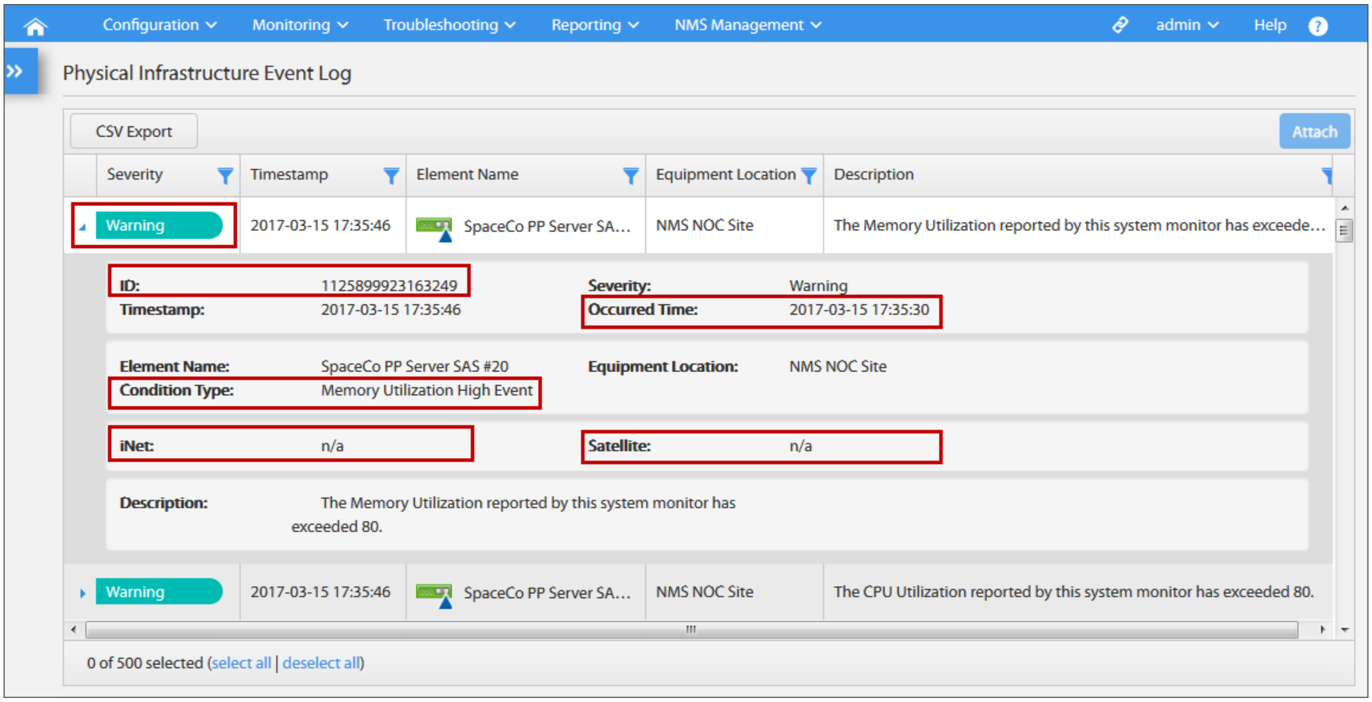
Figure 12-6. Viewing Physical Infrastructure Events in Log View

- **Severity:** NMS assigned levels of severity of an event condition — for example **Critical**.
- **Timestamp:** the date/time at which the event was logged in the NMS.
- **Element Name:** the NMS configured name of the element associated with this event.
- **Equipment Location:** the site at which the event originated based on the associated physical or logical network element.
- **Description:** a brief explanation of the event.
- **CSV Export:** initiates export of the events report to a CSV file.

12.5.2 Expanding the Log View

An expanded **Log View** of an individual Event record can be viewed by clicking the **Show/Hide** icon located just to the left of each Event. The icon is used to toggle between a normal and expanded record, to show or to hide the expanded Event properties detail.

A brief description of the expanded fields of the **Log View** is provided below:



Physical Infrastructure Event Log

Severity	Timestamp	Element Name	Equipment Location	Description
Warning	2017-03-15 17:35:46	SpaceCo PP Server SA…	NMS NOC Site	The Memory Utilization reported by this system monitor has exceede…
Warning	2017-03-15 17:35:46	SpaceCo PP Server SA…	NMS NOC Site	The CPU Utilization reported by this system monitor has exceeded 80.

ID:	1125899923163249	**Severity:**	Warning
Timestamp:	2017-03-15 17:35:46	**Occurred Time:**	2017-03-15 17:35:30
Element Name:	SpaceCo PP Server SAS #20	**Equipment Location:**	NMS NOC Site
Condition Type:	Memory Utilization High Event		
iNet:	n/a	**Satellite:**	n/a
Description:	The Memory Utilization reported by this system monitor has exceeded 80.		

0 of 500 selected (select all | deselect all)

Figure 12-7. Log View - Expanded Details

- **ID:** the identification number assigned to an event condition.
- **Occurred Time:** the date/time at which the event was triggered in the NMS.
- **Condition Type:** one of several NMS classifications of event conditions.
- **iNet:** identifies the iNet in which the event occurred, if applicable.
- **Satellite:** identifies the Satellite in which the event occurred, if applicable.

12.6 Managing Network Events, Alarms, and Incidents

Pulse provides several operations that enhance the ability of network operators to monitor and identify alarms and conditions. For example, an operator may create a “super alarm,” otherwise known as an “Incident,” which can represent the occurrence of a specific set of alarm conditions that are defined by the creator as an incident.

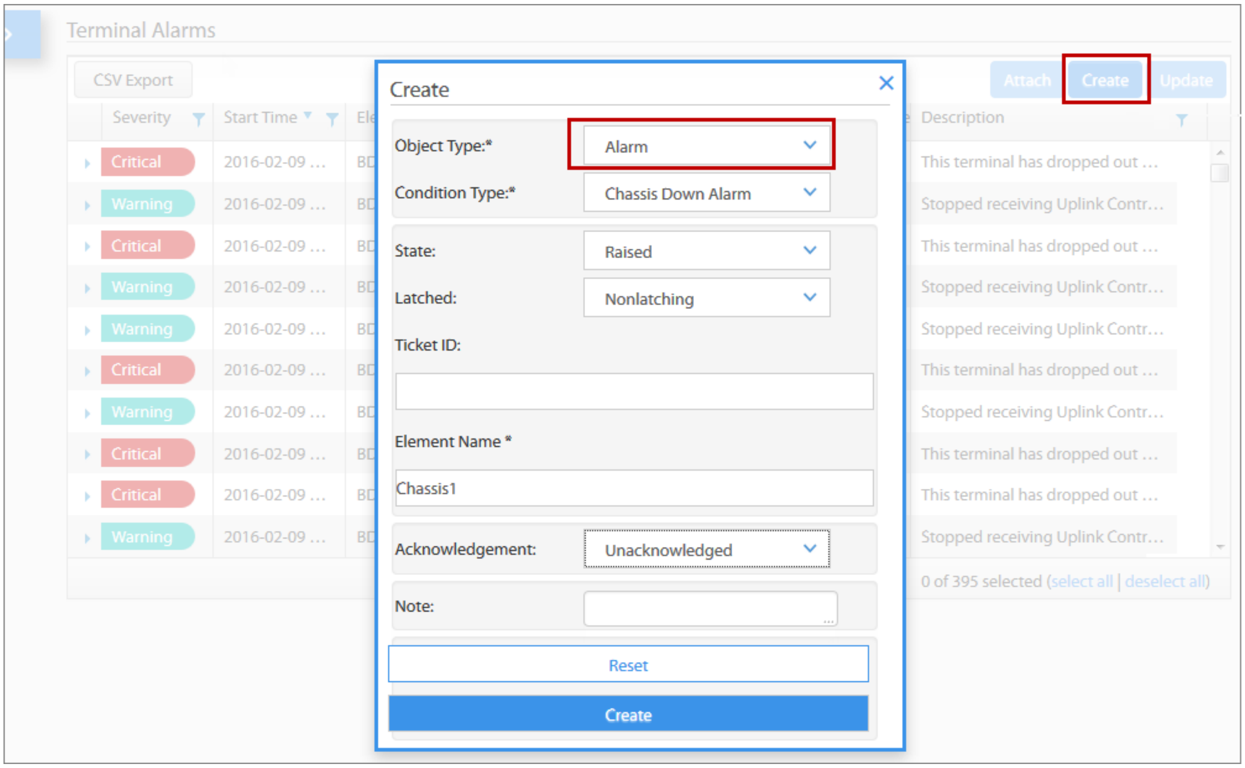
Operations for managing network events, alarms, and incidents are accessed from the alarms and events monitoring and reporting windows, and are based on user permissions.

The following Event, Alarm, and Incident, operations may be performed:

- Manually Create Alarm or Incident
- Update Alarm or Incident Properties (Acknowledge, Clear, Add Notes, Attach Ticket)
- Attach Alarms to an Incident (add additional alarms to a user-created incident)
- Attach Events to an Alarm (add additional events to a user-created alarm)

12.6.1 Creating an Alarm

In normal operation alarms are generated from events that are triggered by rules defined in the discrete data engine. When a triggering rule is met, the associated alarm is generated. In some cases, however, an operator may need to manually create what is called a *derived alarm*, which is an alarm based on a set of user-selected events. A user with permission can create a new Alarm in the NMS, using the **Create** dialog.



Severity	Start Time	Description
Critical	2016-02-09 …	This terminal has dropped out …
Warning	2016-02-09 …	Stopped receiving Uplink Contr…
Critical	2016-02-09 …	This terminal has dropped out …
Warning	2016-02-09 …	Stopped receiving Uplink Contr…
Warning	2016-02-09 …	Stopped receiving Uplink Contr…
Critical	2016-02-09 …	This terminal has dropped out …
Warning	2016-02-09 …	Stopped receiving Uplink Contr…
Critical	2016-02-09 …	This terminal has dropped out …
Critical	2016-02-09 …	This terminal has dropped out …
Warning	2016-02-09 …	Stopped receiving Uplink Contr…

0 of 395 selected (select all | deselect all)

Create

Object Type:* Alarm
Condition Type:* Chassis Down Alarm
State: Raised
Latched: Nonlatching
Ticket ID:
Element Name * Chassis1
Acknowledgement: Unacknowledged
Note:

Figure 12-8. Create Dialog — Create Alarm

The creation of a derived alarm is done in two steps — first the creation of the alarm object, where certain attributes are defined; then user-specified events are attached to the alarm.

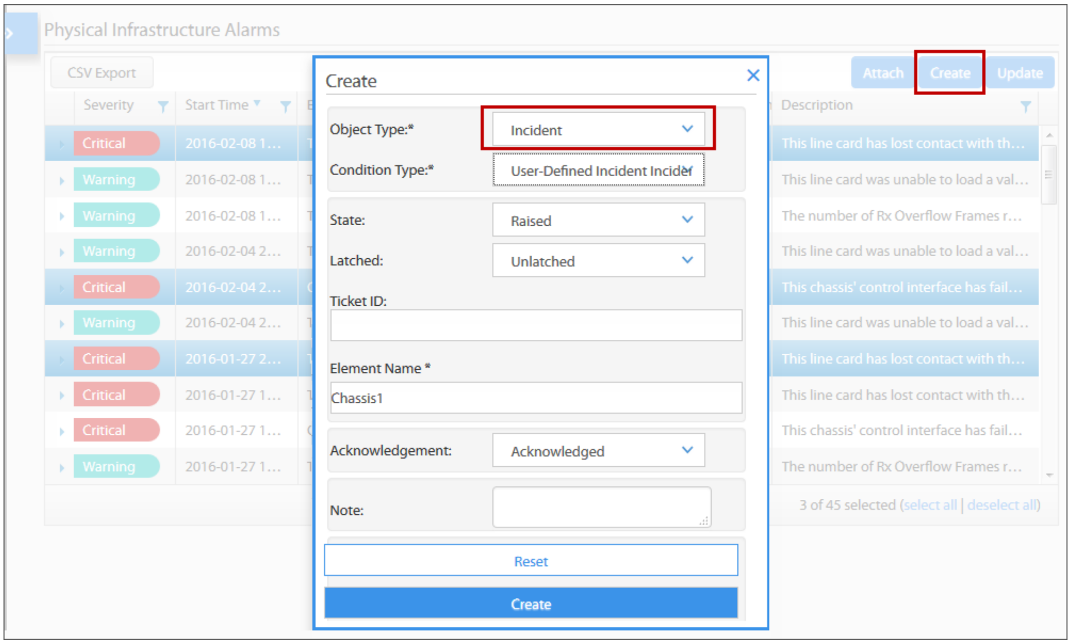
To create an alarm:

1. With alarms in the results window, from a real-time monitoring or historical reporting operation, click the **Create** button. The **Create** dialog opens.
2. Use the **Object Type** drop-down and choose **Alarm** as the object type to create.
3. Use the **Condition Type** drop-down and choose the condition type to trigger the alarm.
4. Choose the initial **State** of the alarm as **Raised** or **Cleared**.
5. Use the **Latched** drop-down to specify the initial state/behavior of this new alarm as one of the following:
   a. **Latched:** set the alarm to latched. In this mode an alarm once triggered, remains raised and present in the NMS until the triggering event is cleared and the alarm is acknowledged by the operator.
   b. **Unlatched:** an alarm that is currently not latched, or that has been cleared and acknowledged.
   c. **Non-Latching:** the default alarm type. A non-latching alarm, once triggered, remains raised in the NMS until cleared automatically when the trigger event no longer exists.
6. If applicable, assign a trouble **Ticket ID** to the new Alarm.
7. Click in **Element Name**, to open the Search window to find the element to which the alarm is associated.
8. Use the **Acknowledgment** drop-down list to set the initial **Acknowledged State** of the new alarm/incident as **Acknowledged** or as **Unacknowledged**.
9. If applicable, use the **Note** field to enter any useful information about the new object.
10. Click **Create** to save the new Alarm or click **Reset** to return to the dialog to the default settings. An **Alarm ID** is assigned to the new alarm. You will need to reference this **Alarm ID** later when attaching Events to the Alarm.

12.6.2 Creating an Incident

An *incident* is a super alarm that is normally internal in the NMS, and based on the linking of multiple specific alarm conditions. In some cases, however, an operator may need to create what is called a *derived incident*, which is a special alarm type in which several linked alarms result in an incident. An incident, in fact, can be the result of a combination of alarms, a combination of incidents, or a combination of alarms and incidents.

The creation of an incident, like the creation of an alarm, is done in two steps — first the creation of the incident object, where certain attributes are defined; then user-specified alarms/incidents are attached to the incident. A user with permission can create a new Incident in the NMS, using the Create dialog.



Severity	Start Time	Description
Critical	2016-02-08 1…	This line card has lost contact with th…
Warning	2016-02-08 1…	This line card was unable to load a val…
Warning	2016-02-08 1…	The number of Rx Overflow Frames r…
Warning	2016-02-04 2…	This line card was unable to load a val…
Critical	2016-02-04 2…	This chassis' control interface has fail…
Warning	2016-02-04 2…	This line card was unable to load a val…
Critical	2016-01-27 2…	This line card has lost contact with th…
Critical	2016-01-27 1…	This line card has lost contact with th…
Critical	2016-01-27 1…	This chassis' control interface has fail…
Warning	2016-01-27 1…	The number of Rx Overflow Frames r…

3 of 45 selected (select all | deselect all)

Object Type:* Incident
Condition Type:* User-Defined Incident Incider
State: Raised
Latched: Unlatched
Ticket ID:
Element Name * Chassis1
Acknowledgement: Acknowledged
Note:

Figure 12-9. Create Dialog — Create Incident

To create an incident:

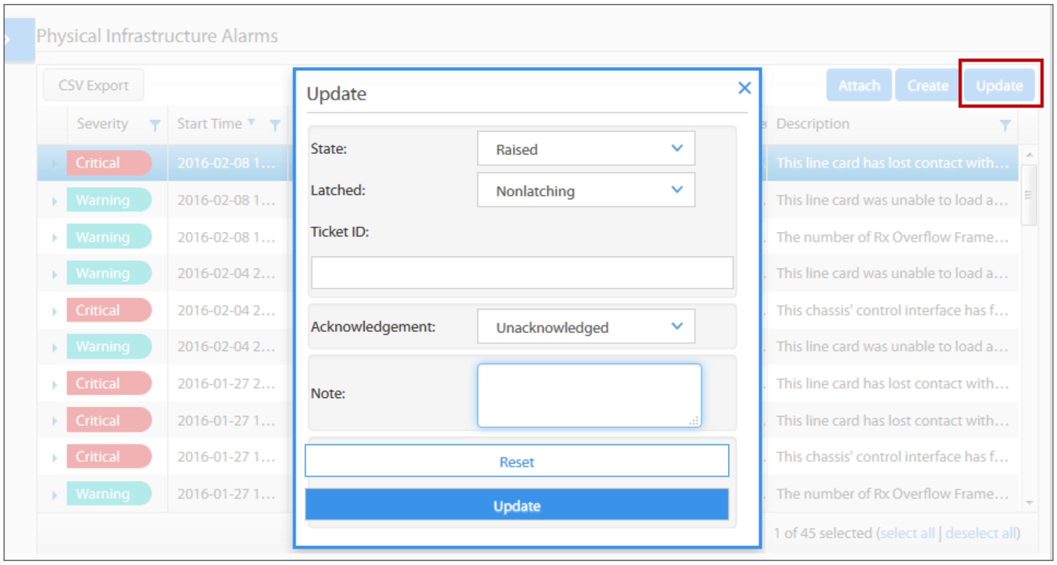
1. With alarms/incidents listed in the results window, from a real-time monitoring or historical reporting operation, click the **Create** button.
2. Use the **Object Type** drop-down list and choose **Incident** as the object type to create.
3. Use the **Condition Type** drop-down list and choose **User-Defined Incident**.
4. Choose the initial **State** of the incident as **Raised** or **Cleared**.
5. Use the **Latched** drop-down to select the initial incident state as one of the following:
    a. **Latched:** an alarm type that, once triggered, remains raised and present in the NMS until both cleared (manually or automatically) and acknowledged.
    b. **Unlatched:** an alarm that is currently not latched, or that has been cleared and acknowledged.

   c. **Non-Latching:** the default incident type. A non-latching alarm, once triggered, remains raised in the NMS until cleared automatically when the trigger event no longer exists.

6. If applicable, assign a trouble **Ticket ID** to the new Incident.
7. Click in **Element Name**, to open the basic Search window to select one or more elements to associate with the incident.
8. Use the **Acknowledgment** drop-down to choose **Acknowledged** or as **Unacknowledged** as the initial state of the new incident.
9. If applicable, use the **Note** field to enter any useful information about the new Incident.
10. Click **Create** to save the new Incident or click **Reset** to return the dialog to the default settings. An **Incident ID** is assigned to the new incident. The **Incident ID** can be referenced later, when attaching Alarms/Incidents to the Incident. See *Attaching Alarm Conditions to an Incident*.

12.6.3 Updating an Alarm or Incident

A user with appropriate permission can manually change or update specific properties associated with an alarm or incident. An alarm or incident, for example, can be manually moved from **Unacknowledged** to **Acknowledged** or from **Raised** to **Cleared;** or from **Latched** to **Unlatched**, or **Non-Latching**. The **Note** field allows a note to be created for oneself or for the next operator; and a trouble **Ticket ID** can be assigned and later referenced. An Alarm/Incident might also be updated temporarily for diagnostic/troubleshooting purposes.



Severity	Start Time	Description
Critical	2016-02-08 1…	This line card has lost contact with…
Warning	2016-02-08 1…	This line card was unable to load a…
Warning	2016-02-08 1…	The number of Rx Overflow Frame…
Warning	2016-02-04 2…	This line card was unable to load a…
Critical	2016-02-04 2…	This chassis' control interface has f…
Warning	2016-02-04 2…	This line card was unable to load a…
Critical	2016-01-27 2…	This line card has lost contact with…
Critical	2016-01-27 1…	This line card has lost contact with…
Critical	2016-01-27 1…	This chassis' control interface has f…
Warning	2016-01-27 1…	The number of Rx Overflow Frame…

1 of 45 selected (select all | deselect all)

Update

State: Raised

Latched: Nonlatching

Ticket ID:

Acknowledgement: Unacknowledged

Note:

Figure 12-10. Update Alarm/Incident Dialog

To update an alarm or an incident:

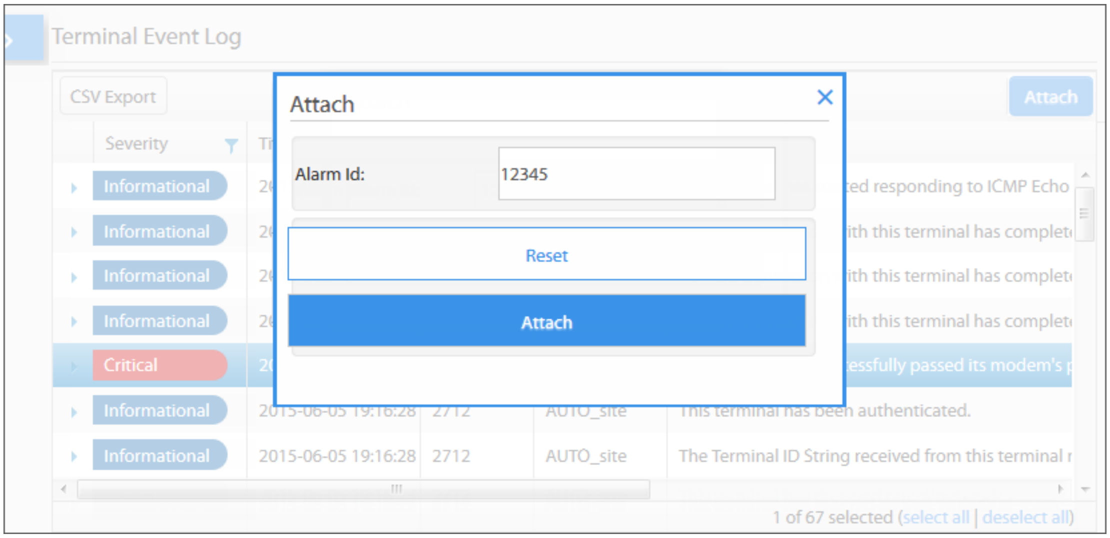
1. With alarms/incidents listed in the results window, from a real-time alarms monitoring or historical alarms report, select one or more alarms/incidents to be updated.

2. Click the **Update** button to modify an alarm/incident. The **Update** dialog opens.
3. Set the **State** of the alarm as **Raised** or **Cleared** as required.
4. Use the **Latched** drop-down to select the modify the latch type of the alarm/incident:
   a. **Latched:** update the alarm/incident to *latched.* In this mode, an alarm/incident once triggered, remains raised in the NMS until both cleared and acknowledged.
   b. **Unlatched:** update the alarm/incident to *unlatched.*
   c. **Non-Latching:** set the alarm/incident to the default type. A non-latching alarm, once triggered, remains raised in the NMS until cleared automatically when the trigger event no longer exists.
5. If applicable, the alarm/incident can be updated with a trouble **Ticket ID**.
6. Use the **Acknowledgment** drop-down list to select the alarm/incident **Acknowledged State** as one of the following:
   a. **Acknowledged:** the alarm/incident has been acknowledged by the operator. Multiple alarms/incidents may be acknowledged simultaneously.
   b. **Unacknowledged:** the alarm is not yet acknowledged by the operator.
7. If applicable, use the **Note** field to enter any information about the Alarm/Incident.
8. Click **Update** to save the updated alarm object or click **Cancel** to discard the object.

12.6.4 Attaching Event Conditions to an Alarm

Using the **Attach** dialog, a user with permission can do either of the following operations:

- Attach Events to a newly created Alarm
- Attach Events to an existing Alarm



Attach

Alarm Id: 12345

Severity				
Informational	2015-06-05 19:16:28	2712	AUTO_site	This terminal has been authenticated.
Informational	2015-06-05 19:16:28	2712	AUTO_site	The Terminal ID String received from this terminal r

Figure 12-11. Attach Event Condition to Alarm Dialog

The Events to be attached may be selected from Events listed in a real-time monitoring or historical reporting operation.

To attach one or more selected events to an alarm:

1. With the Events log listed from a **Monitoring** or **Reporting** operation, select one or more Events that should be attached to an existing or newly created Alarm.
2. Click the **Attach** button. The **Attach** dialog opens.
3. In **Alarm ID,** enter the ID of the alarm to which the selected Events are to be attached.
4. Click **Attach** to attach the selected Events to the specified **Alarm ID** or click **Reset** to discard the attachment.
5. To verify that the Events are assigned to the Alarm, open the Alarm in a **Real-Time Monitoring** or **Historical Reporting** operation view and expand the Alarm details.

12.6.5 Attaching Alarm Conditions to an Incident

As mentioned earlier, incidents are normally generated internally in the NMS from several linked alarms, but in some circumstances an operator may need to create a new incident (super alarm) that is triggered by a combination of alarms and/or incidents. Additional alarms or incidents may also be added to an existing incident at a later point.

Using the **Attach** dialog, a user with permission can perform the following operations:

- Attach one or more selected Alarms to a newly created Incident
- Attach one or more selected Alarms or Incidents to an existing Incident

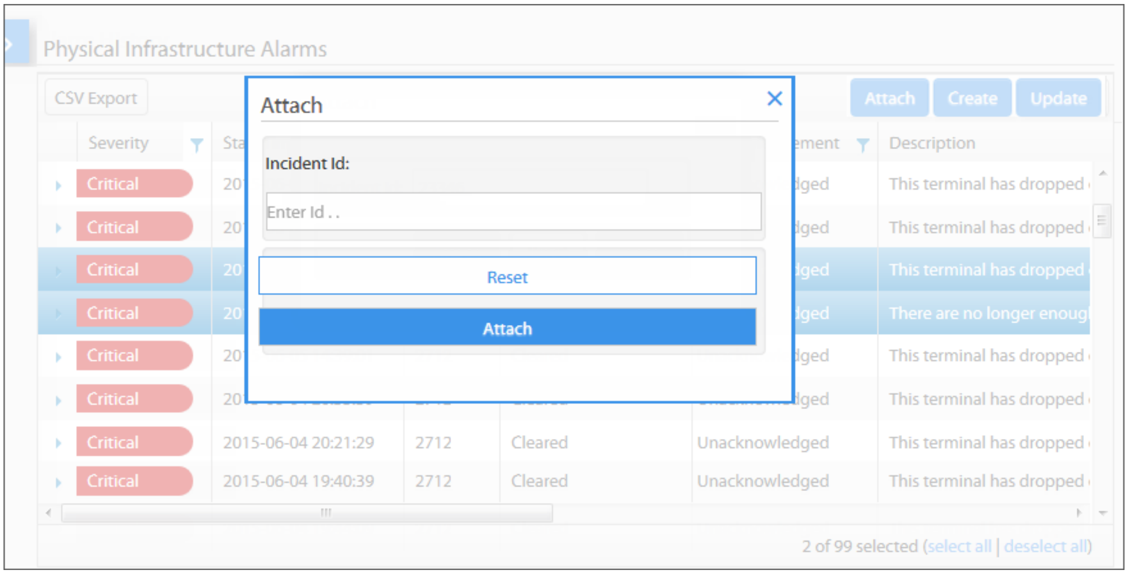


Figure 12-12. Attach Alarm to Incident Dialog

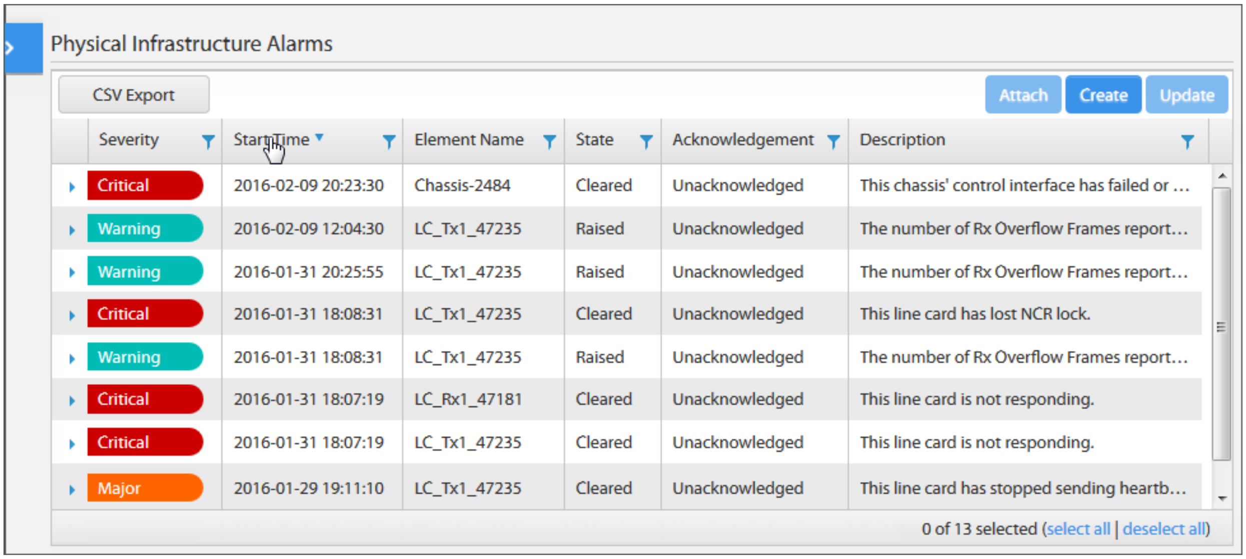
1. With Alarms listed from a **Monitoring** or **Reporting** operation, select one or more Alarms that should be attached to an existing or newly created Incident.

2. Click the **Attach** button. The **Attach** dialog opens.
3. Click **Incident ID**, to enter the ID of the incident to which the Alarms are to be attached.
4. Click **Attach** to attach the selected Alarms to the specified **Incident ID** or click **Reset** to discard the attachment. The individual alarms attached to the incident are no longer listed in the alarms display, but are now rolled-up in the incident.
5. To verify that the Alarms are assigned to the Incident, open the Incident (Alarm) in a **Monitoring** or **Reporting** operation view and expand the Incident (Alarm) details.

12.6.6 Sorting Events, Alarms, and Incidents

The NMS monitoring and reporting pages consists of multiple data records. The data in these records can be sorted to achieve a desired view. Each column has a *header name* that identifies the column data. By default the data records are sorted by time stamp, in descending order. This descending order, is indicated by the down-pointing arrow shown adjacent to the heading.

When the down-arrow is displayed, the list is in descending order from the highest to the lowest. A single click on the down-arrow triggers an ascending sort, which displays the up arrow. The up-arrow indicates the list is in ascending order from the lowest to the highest. A single click on the up-arrow triggers a descending sort.



Severity	Start Time	Element Name	State	Acknowledgement	Description
Critical	2016-02-09 20:23:30	Chassis-2484	Cleared	Unacknowledged	This chassis' control interface has failed or …
Warning	2016-02-09 12:04:30	LC_Tx1_47235	Raised	Unacknowledged	The number of Rx Overflow Frames report…
Warning	2016-01-31 20:25:55	LC_Tx1_47235	Raised	Unacknowledged	The number of Rx Overflow Frames report…
Critical	2016-01-31 18:08:31	LC_Tx1_47235	Cleared	Unacknowledged	This line card has lost NCR lock.
Warning	2016-01-31 18:08:31	LC_Tx1_47235	Raised	Unacknowledged	The number of Rx Overflow Frames report…
Critical	2016-01-31 18:07:19	LC_Rx1_47181	Cleared	Unacknowledged	This line card is not responding.
Critical	2016-01-31 18:07:19	LC_Tx1_47235	Cleared	Unacknowledged	This line card is not responding.
Major	2016-01-29 19:11:10	LC_Tx1_47235	Cleared	Unacknowledged	This line card has stopped sending heartb…

0 of 13 selected (select all | deselect all)

Figure 12-13. Sorting Data Records by Start Time in Descending Order

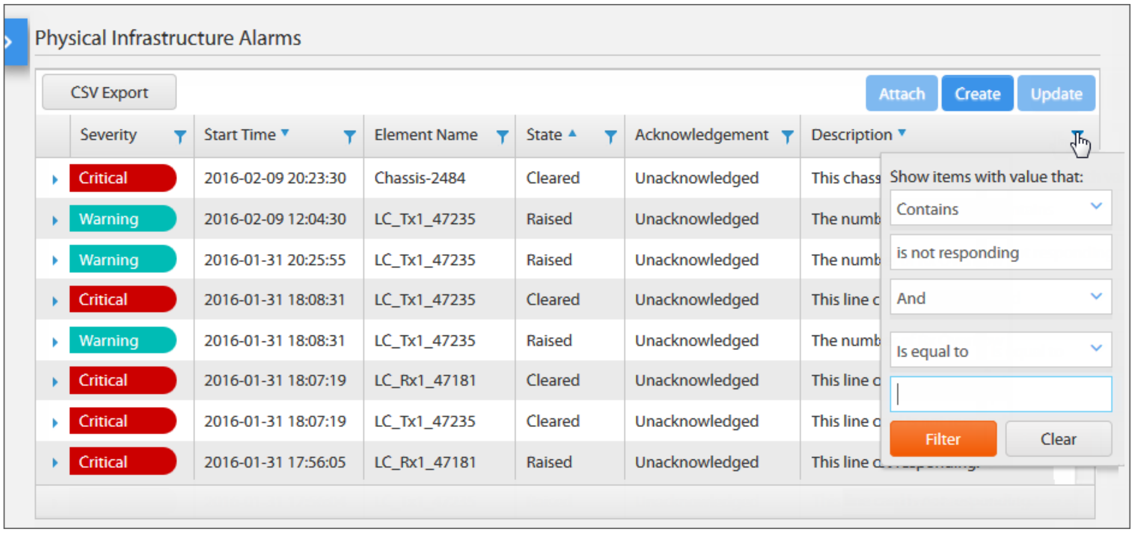
To sort tabular data records:

1. Click a column heading to sort the grid data records on a specific field in ascending order or descending order. Note the sort directional arrow.
2. Click on a specific column heading to re-sort the grid records based on that heading. Click the up-arrow icon for descending sort; click down-arrow icon for an ascending sort.

12.6.7 Filtering Events, Alarms, and Incidents

In addition to a **Header Name**, each column also has a *filter icon*, which is used to limit the display of data records, when a large number of records are listed. Filtering is possible on any column that has a filter icon. Filtering is often required in some real-time or historical reports that involves many elements.

With a single click on a filter icon, the filter dialog of the column is opened. The filter dialog always supports the insertion of two compare match statements, which can be combined using logical operators **AND**/**OR**. Only one statement is actually required to complete a filter.



Severity	Start Time	Element Name	State	Acknowledgement	Description
Critical	2016-02-09 20:23:30	Chassis-2484	Cleared	Unacknowledged	This chass
Warning	2016-02-09 12:04:30	LC_Tx1_47235	Raised	Unacknowledged	The numb
Warning	2016-01-31 20:25:55	LC_Tx1_47235	Raised	Unacknowledged	The numb
Critical	2016-01-31 18:08:31	LC_Tx1_47235	Cleared	Unacknowledged	This line c
Warning	2016-01-31 18:08:31	LC_Tx1_47235	Raised	Unacknowledged	The numb
Critical	2016-01-31 18:07:19	LC_Rx1_47181	Cleared	Unacknowledged	This line c
Critical	2016-01-31 18:07:19	LC_Tx1_47235	Cleared	Unacknowledged	This line c
Critical	2016-01-31 17:56:05	LC_Rx1_47181	Raised	Unacknowledged	This line c

Show items with value that:
Contains
is not responding
And
Is equal to

Figure 12-14. Filtering Data Records Example

To filter tabular data records:

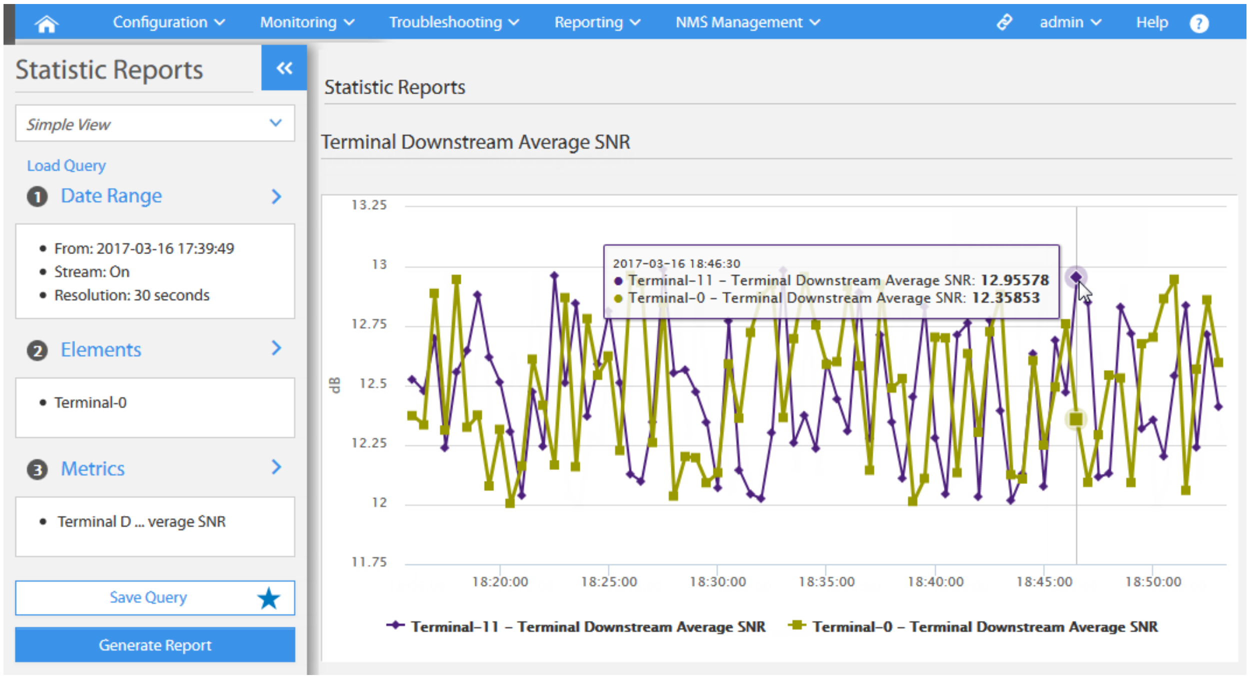
1. With a grid display open, click the filter icon on a column by which to filter the records.
2. Use the first drop-down list to select a comparator for the first filter statement. The compare options are context-sensitive and based on the column data type. For example, **Description** is a text field and the compare options are *equal to*, *not equal to*, *starts with*, *contains*, *does not contain*, and *ends with*. In the example **Contains** is selected.
3. In the value field, immediately following the first compare drop-down list field, enter a value or text string as the match criteria to complete the first filter statement.
4. Click the second drop-down list and select **AND** or **OR** to logically combine statements. This parameter is irrelevant if the second filter statement is not entered. In the example “dropped out of network” is entered.
5. If applicable, use the second drop-down list to select a comparator for the second filter statement, and then in the value field, immediately following the second filter, enter a value or text string as the match criteria to complete the second statement.
6. Click the **Filter** button to execute the filter, when at least one filter clause is entered.
7. The filter icon is shown in green when the filter is active. Click the icon and then click **Clear** to reset the column data by removing any filters. The filter icon returns to normal.

12.7 Real-Time Statistics Monitoring

A measure of an operational or performance characteristic of a network element can be obtained from a *statistics report*. Pulse NMS tracks a variety of statistical data, such as line card statistics, satellite link statistics, IP traffic statistics, and QoS statistics. Using the **Statistics Reports** operation of the Monitoring menu, you can generate a real-time statistics report based on one or more metrics for any one or more physical or logical elements.

The **Date Range** of the **Monitoring Statistics** report, is preset to the current date, current time, Stream ON to allow display of new statistics data as it occurs, and a **Resolution** of 30 seconds (data sampled every 30 seconds). With these preset parameters, you only need to use the **Elements** selector to specify one or more elements for which to run the report, and use the **Metrics** selector to specify one or more metrics to gather for the report.

If the report is configured for multiple metrics, multiple elements, or both, the output is based on default settings for Report Preferences. The Configurator **Report Preferences** is only displayed and can be modified in the Configurator **Advanced View**. See Table 12-2.



- From: 2017-03-16 17:39:49
- Stream: On
- Resolution: 30 seconds

- Terminal-0

- Terminal D ... verage SNR

2017-03-16 18:46:30
- Terminal-11 – Terminal Downstream Average SNR: **12.95578**
- Terminal-0 – Terminal Downstream Average SNR: **12.35853**

Figure 12-15. Custom Statistics Report - Set for Group by Metric

To generate the Monitoring Statistics Report:

1. Click **Monitoring** > **Real-Time Operation > Monitoring Statistics.** The **Statistic Reports** dialog opens in the Simple View set to current date and time, and with Streaming ON.
2. If desired, select **Advanced View** to display the **Report Preferences** selector, to allow configuration of the report **Output Type, Grouping**, **Chart Type**, and **Chart Size**.
3. Click **Load Query** to load a saved set of Configurator parameters for the report.

4. Click the **Elements** selector to select one or more elements for which the report should be generated. The elements selected for this report are typically of the same type, but may differ if they share a common metric — for example, Transmit Line Card and Receive Line Card.
5. Click the **Metrics** bar to open the dialog to select one or more metrics. A context list of metrics groupings are displayed based on the elements selected for the report.
6. Use the **Metrics Type** filter field to display a list of **Conventional Stats** or **All Stats**. Conventional Stats are those stats that.
7. Select an entire metrics group or use the adjacent blue icon to expand a group and select one or more individual metrics; click **Done** to close the dialog and add the metrics to the Configurator.
8. If the **Report Preferences** selector is displayed, specify the following parameters:
   a. **Output Type:** choose the output method as **Chart** or **CSV Download.**
   b. **Grouping:** choose how the report objects are grouped **-** select **Group by Metric, Group by Metric of Same Unit**, or **Group by Element.** See **Table 12-2.**
   c. **Graph Type:** choose **Line** or **Area** as how the data should be plotted.
   d. **Chart Size:** choose **Small, Medium, Large,** or **Extra Large.**
9. Click **Save Query** to save the **Statistics Report** configuration as a query.
10. Click **Generate Report** to initiate generation of the report output.
11. With the report displayed, with multiple line or area graphs, click on any one of the chart labels to toggle that chart graph between show graph and hide graph.

Table 12-2. Configurator Report Preferences for Statistics

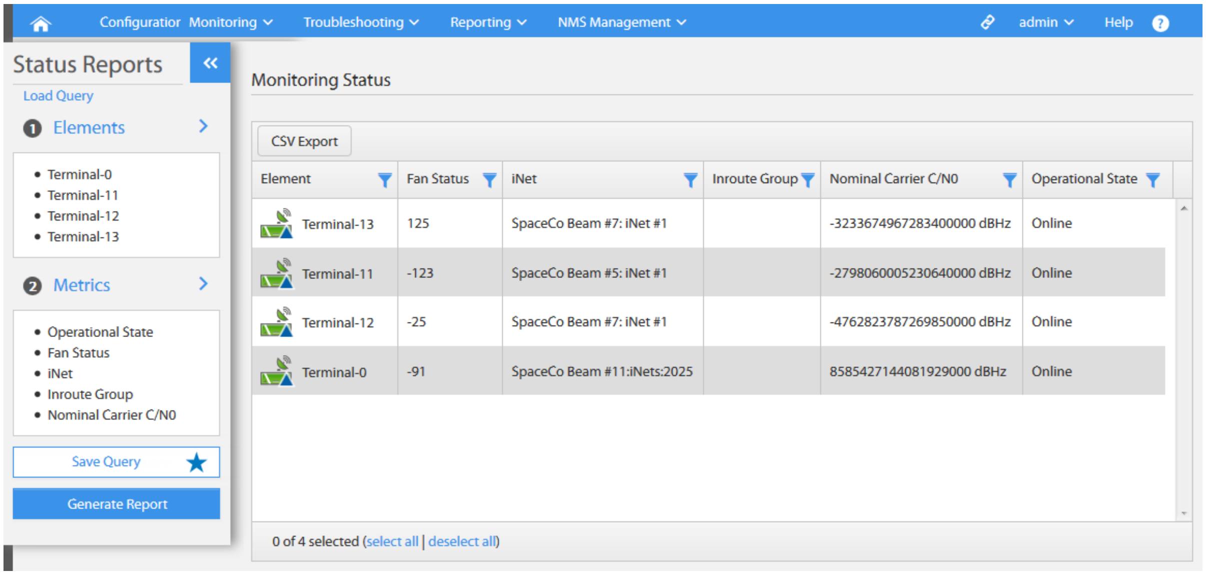
Report Preference Option	Description
Group By: Group By Element	Produces a single chart per element (multiple metrics by color)
Group By: Group By Metric	Produces a single chart per metric (multiple elements by color)
Group By: Group By Metric of Same Type	Produces a single chart per set of shared metric (multiple elements by color)

NOTE: The *Conventional Stats* option represent standard and most commonly used based on the selected element type. The *All Stats* option includes stats used for advanced troubleshooting are not recommended for production use.

12.8 Real-Time Status Monitoring

The Monitoring menu **Monitoring Status** operation generates a real time status report for user-selected network elements, and with respect to user-specified metrics. The report can configured to return the real-time status of one or more elements, for one or more metrics.

Since the report is in real-time, new entries are appended to the report end, if the state of a metric changes or if the value changes.



Elements:
- Terminal-0
- Terminal-11
- Terminal-12
- Terminal-13

Metrics:
- Operational State
- Fan Status
- iNet
- Inroute Group
- Nominal Carrier C/N0

Element	Fan Status	iNet	Inroute Group	Nominal Carrier C/N0	Operational State
Terminal-13	125	SpaceCo Beam #7: iNet #1		-3233674967283400000 dBHz	Online
Terminal-11	-123	SpaceCo Beam #5: iNet #1		-2798060005230640000 dBHz	Online
Terminal-12	-25	SpaceCo Beam #7: iNet #1		-4762823787269850000 dBHz	Online
Terminal-0	-91	SpaceCo Beam #11:iNets:2025		8585427144081929000 dBHz	Online

0 of 4 selected (select all | deselect all)

Figure 12-16. Monitoring Real-Time Status

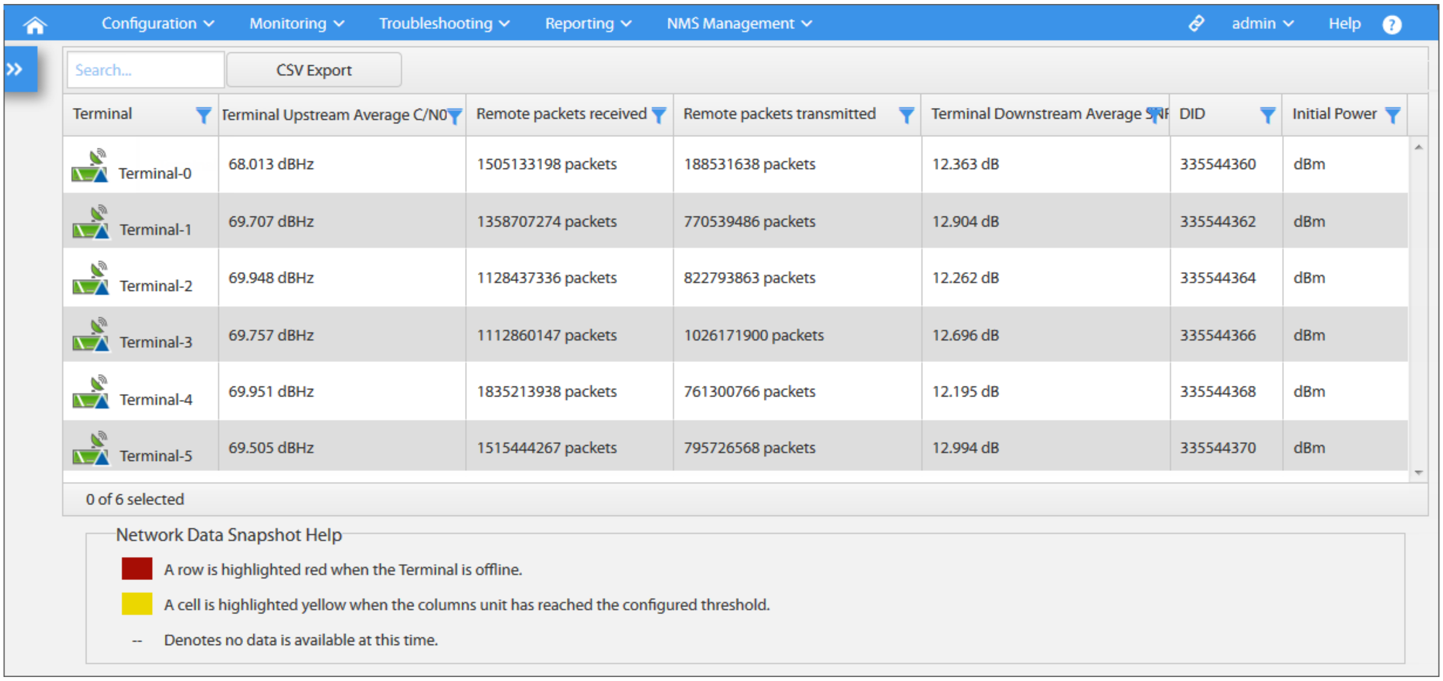
To generate the Monitoring Status Report:

1. Click the **Monitoring** > **Real-Time Operation > Monitoring Status**. The **Status Reports** Configurator dialog opens.
2. Click the **Load Query** button, if applicable, to load a previously saved set of parameters.
3. Click the **Elements** selector to open the Basic Search tool to find and select one or more specific elements to include in the report. The elements should be of the same type.
4. Click the **Metrics** bar to open the dialog to select one or more discrete status metrics. A context list of metrics groupings are displayed based on the selected elements.
5. Use the **Metrics Type** filter field to display a list of **Conventional Stats** or **All Stats**. Conventional Stats are those stats that. Conventional Stats represent standard and most commonly used based on the selected element type. The All Stats option includes stats used for advanced troubleshooting and are not recommended for production use.
6. Select an entire metrics group or use the adjacent blue icon to expand a group and select one or more individual metrics; click **Done** to close the dialog and add the metrics to the Configurator. The list of metrics should be limited to 10 or less.
7. If desired, click **Save Query** to save the **Statistics Report** parameters as a query.
8. Click **Generate Report** to initiate generation of the real-time **Status Report**.

12.9 Real-Time Network Data Snapshot

The Monitoring menu **Network Data Snapshot** operation generates a real time report for one or more selected satellite terminals, based on the user-specified terminals and a user-defined combination of specific metrics and/or configuration data points. The data is polled every 30 seconds.

Since the report is in real-time, if the state of a metric changes or if values change, new entries are inserted to the list according to the sort order and based on the new value.



Terminal	Terminal Upstream Average C/N0	Remote packets received	Remote packets transmitted	Terminal Downstream Average SN	DID	Initial Power
Terminal-0	68.013 dBHz	1505133198 packets	188531638 packets	12.363 dB	335544360	dBm
Terminal-1	69.707 dBHz	1358707274 packets	770539486 packets	12.904 dB	335544362	dBm
Terminal-2	69.948 dBHz	1128437336 packets	822793863 packets	12.262 dB	335544364	dBm
Terminal-3	69.757 dBHz	1112860147 packets	1026171900 packets	12.696 dB	335544366	dBm
Terminal-4	69.951 dBHz	1835213938 packets	761300766 packets	12.195 dB	335544368	dBm
Terminal-5	69.505 dBHz	1515444267 packets	795726568 packets	12.994 dB	335544370	dBm

0 of 6 selected

Network Data Snapshot Help

🟥 A row is highlighted red when the Terminal is offline.

🟨 A cell is highlighted yellow when the columns unit has reached the configured threshold.

-- Denotes no data is available at this time.

Figure 12-17. Monitoring Real-Time Status

To generate the Monitoring Status Report:

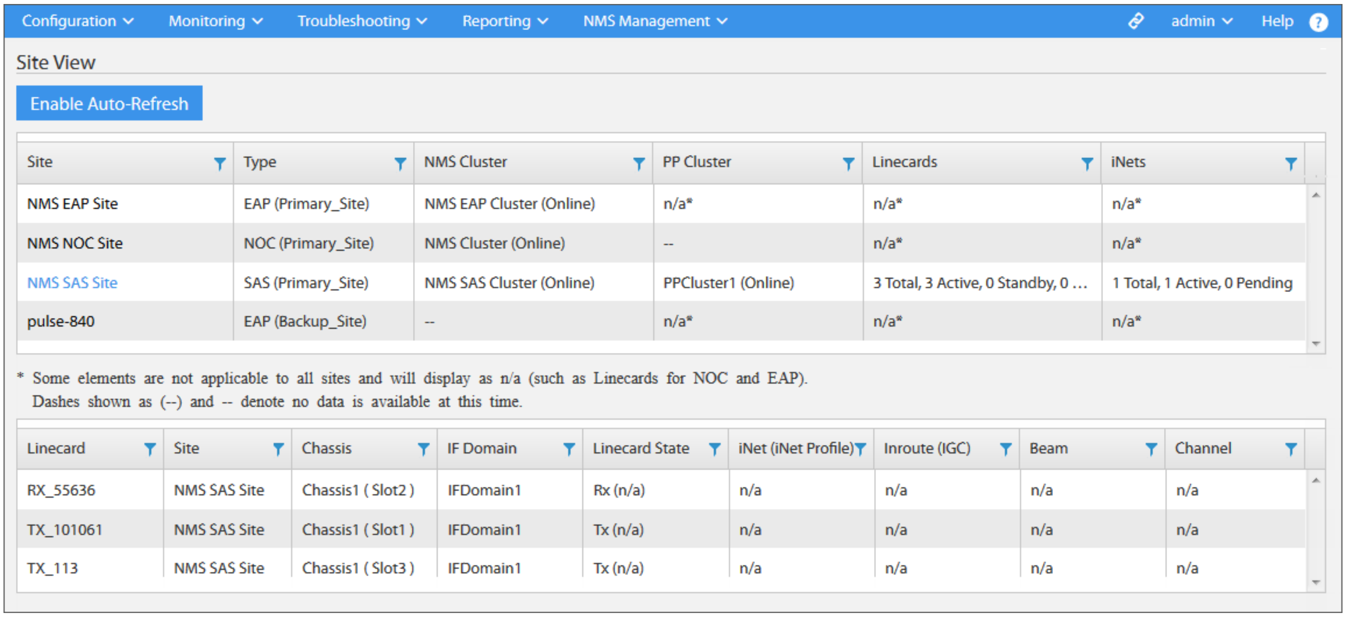
1. Click the **Monitoring** > **Real-Time Operation > Network Data Snapshot**. The **Network Data Snapshot** Configurator dialog opens.
2. Click the **Load Query** button, if applicable, to load a previously saved set of parameters.
3. Click the **Elements** selector to open the Basic Search tool to find and select one or more Terminals to include in the report.
4. Click the **Metrics** bar to open the dialog to select one or more discrete status metrics. Select an entire metrics group or use the adjacent blue icon to expand a group and select one or more individual metrics; click **Done** to close the dialog and add the metrics to the Configurator. The list of selected metrics should be limited to 10 or less.
5. Use the **Metrics Type** filter field to display a list of **Conventional Stats** or **All Stats**. Conventional Stats represent standard and most commonly used based on the element type. The All Stats option includes stats used for advanced troubleshooting and are not recommended for production use.

6. Click the **Configuration** bar to open the dialog to select one or more of the terminal configuration data points to include in the report.
7. If desired, click **Save Query** to save the **Statistics Report** parameters as a query.
8. Click **Generate Report** to initiate generation of the **Network Data Snapshot** report.

12.10 Monitoring At a Glance — Using Site View

The “At-a-Glance” **Site View** report is a manual report operation that produces a quick view of the configured network sites and the associated infrastructure elements, from the view point of the site. The report gives the **Site**, **Type** of site (primary, backup), and shows the associated infrastructure elements such as NMS Cluster, PP Cluster, ASC, Linecards, and iNets.

For each site, listed under **Site**, the **Type** column shows whether the site is a primary or backup EAP, NOC or SAS site; the **PP Cluster** column, where applicable, shows the site PP cluster status. The **Line Card** column, where applicable, shows the status of the line cards associated with the site; and under the **iNets** column, where applicable, the status of iNets associated with a site is given. Some elements are not applicable (n/a) to all sites and will display as such. For example, linecards are not applicable to the NOC and EAP sites.



Site	Type	NMS Cluster	PP Cluster	Linecards	iNets
NMS EAP Site	EAP (Primary_Site)	NMS EAP Cluster (Online)	n/a*	n/a*	n/a*
NMS NOC Site	NOC (Primary_Site)	NMS Cluster (Online)	--	n/a*	n/a*
NMS SAS Site	SAS (Primary_Site)	NMS SAS Cluster (Online)	PPCluster1 (Online)	3 Total, 3 Active, 0 Standby, 0 ...	1 Total, 1 Active, 0 Pending
pulse-840	EAP (Backup_Site)	--	n/a*	n/a*	n/a*

* Some elements are not applicable to all sites and will display as n/a (such as Linecards for NOC and EAP).
Dashes shown as (--) and -- denote no data is available at this time.

Linecard	Site	Chassis	IF Domain	Linecard State	iNet (iNet Profile)	Inroute (IGC)	Beam	Channel
RX_55636	NMS SAS Site	Chassis1 (Slot2)	IFDomain1	Rx (n/a)	n/a	n/a	n/a	n/a
TX_101061	NMS SAS Site	Chassis1 (Slot1)	IFDomain1	Tx (n/a)	n/a	n/a	n/a	n/a
TX_113	NMS SAS Site	Chassis1 (Slot3)	IFDomain1	Tx (n/a)	n/a	n/a	n/a	n/a

Figure 12-18. NMS At-A-Glance Site View Report.

To get an at-a-glance site view:

1. Click the **Monitoring** tab, and under **At A Glance**, select **Site View**.
2. Click on a specific Site link, for example in **NMS SAS Site**, to view real-time details of site elements and information, in the lower half of the page.
3. Click **Enable Auto-Refresh** to allow automatic refresh of the report as changes occur.
4. Click the **Disable Auto-Refresh** button to stop automatic refresh of the report.

12.11 Monitoring at a Glance — Network Overview

The Network Overview page, opened from the **Monitoring** menu, under **At a Glance**, provides network operators with a dashboard overview of hub infrastructure components of an entire network. For each Site, and by each satellite, all critical and major network alarms that have been raised over the last 24 hours are immediately brought into focus.

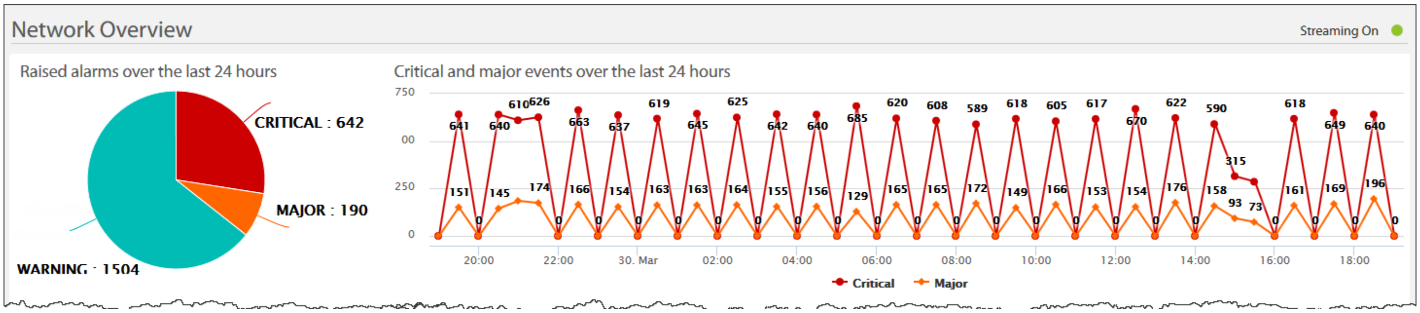


Figure 12-19. Network Overview

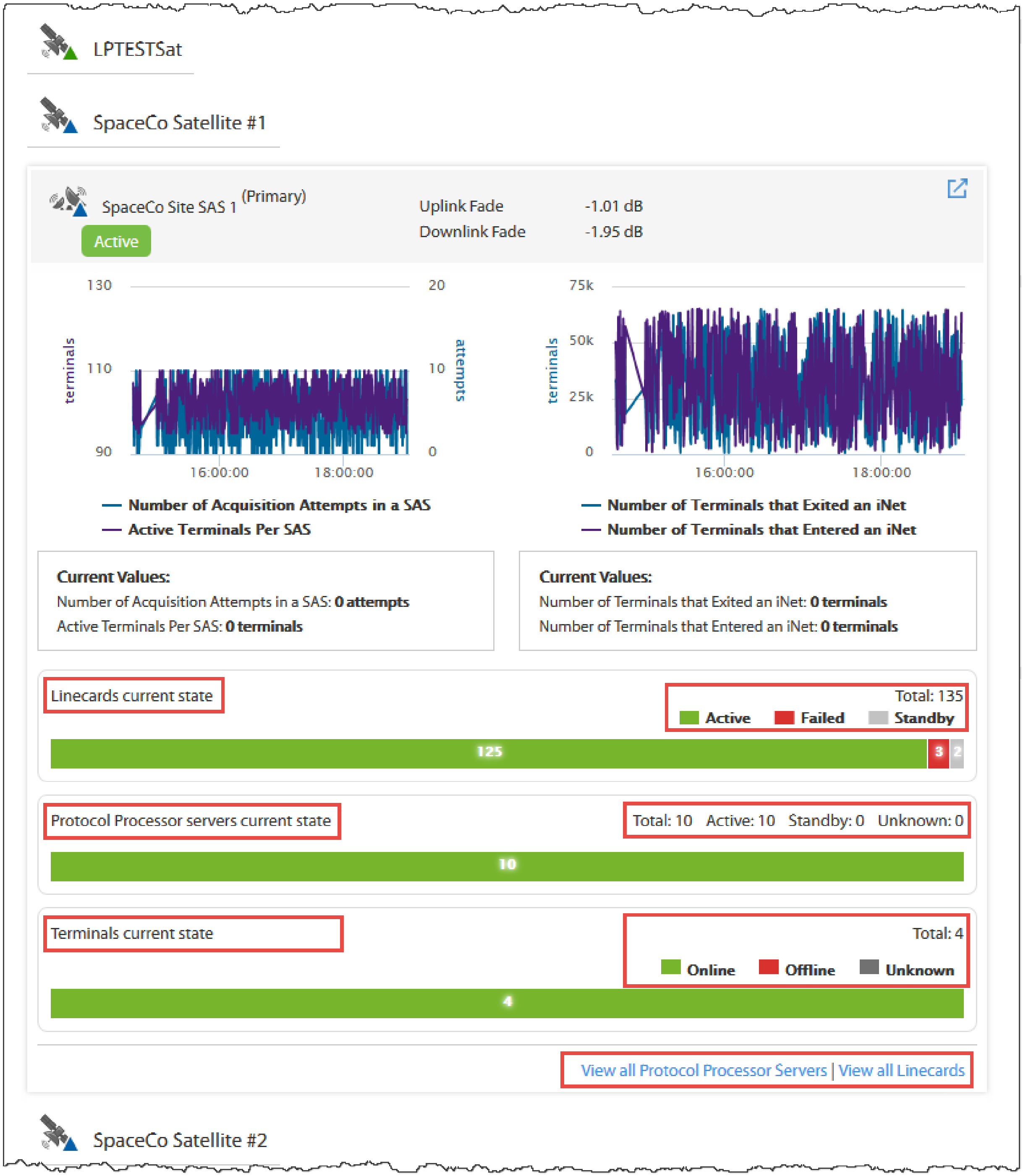
The following list provides brief overview of the Network Overview page report:

- **Essential Information in One Place**: The Network Overview brings together, in one place, vital hub infrastructure components and commonly used metrics to allow the NOC Operator to quickly gain a clear understanding of the overall network health.
- **Single Tool Shared by Everyone**: Provides an at-a-glance view to anyone in the NOC, and overview of relevant network information, which is accessible without manual effort and can confirm whether the network is operating as expected.
- **Instant View of Critical Data and Issues**: Provides easy access to needed data and instant ability to see critical issues and where they are emerging from, thereby allowing NOC operators to be proactive in minimizing the time required to recognize critical issues, and to prevent those issues from causing more severe problems in the network.
- **Line Graph and Chart View of Critical & Major Alarms**: Provides visual charts and graphs to show all critical and major alarms that have occurred during the last 24-hours. NOC Operators can quickly spot and manage a spike in network alarms based on the severity.
- **Full Overview of Each SAS Site**: Provides SAS information and performance such as Rain Diversity Switches, Uplink Fade & Downlink Fade, Total Active Terminals, and Terminals Entering/Exiting an iNet all on a single page — regardless of the number of SAS Sites.
- **Quick Access View of Line Card & Protocol Processors**: Provides a current operational status view of all Line Cards and Protocol Processors, in a few aggregated charts as well as a quick access link to drill down to **View All Linecards** or **View all PP Servers**.

To retrieve the network overview page:

1. Click **Monitoring > At a Glance > Network Overview**. The Network Overview opens to a focus on the critical and major alarms that have occurred in the last 24-hours.
2. Click on any data point in the critical and major alarms line charts to view additional information.

3. Click **View All Protocol Processors** or **View All Line Cards** respectively to open a Browse window to view all P or Line Cards in the Site. The element states are indicated as: **Online** = Green, **Offline** = Red, **Disabled** = Light Gray, and Not Available = Dark Gray.



LPTESTSat
SpaceCo Satellite #1
SpaceCo Site SAS 1 (Primary)
Active
130
110
90
terminals
20
10
0
attempts
16:00:00
18:00:00
Number of Acquisition Attempts in a SAS
Active Terminals Per SAS
75k
50k
25k
0
terminals
16:00:00
18:00:00
Number of Terminals that Exited an iNet
Number of Terminals that Entered an iNet
Linecards current state
🟩 Active 🟥 Failed ▨ Standby
125
3
2
Protocol Processor servers current state
10
Terminals current state
🟩 Online 🟥 Offline ▨ Unknown
4
View all Protocol Processor Servers | View all Linecards
SpaceCo Satellite #2

Uplink Fade -1.01 dB
Downlink Fade -1.95 dB

Current Values:
Number of Acquisition Attempts in a SAS: **0 attempts**
Active Terminals Per SAS: **0 terminals**

Current Values:
Number of Terminals that Exited an iNet: **0 terminals**
Number of Terminals that Entered an iNet: **0 terminals**

Total: 135

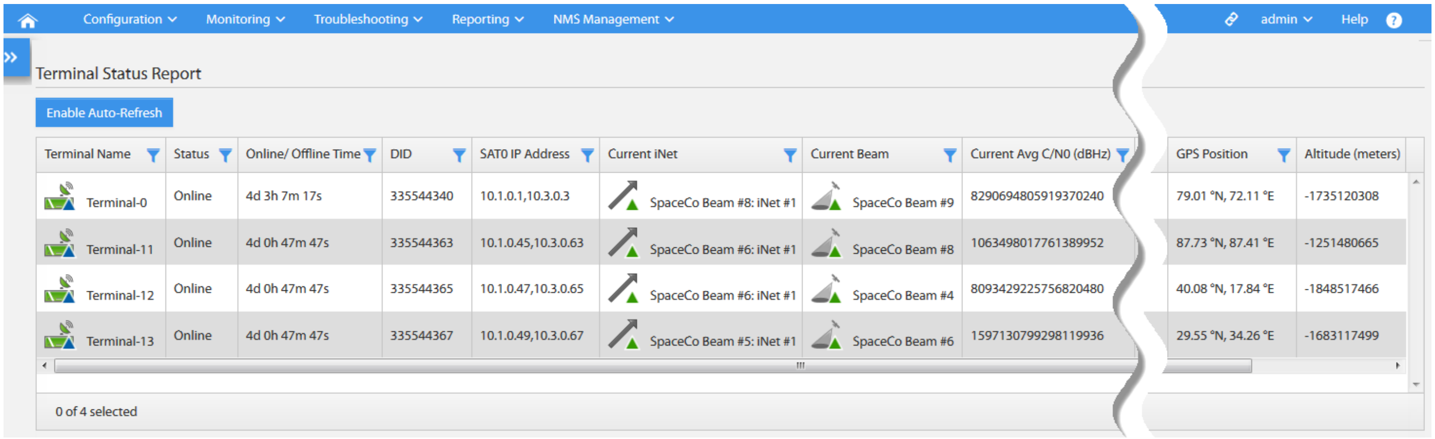
Total: 10 Active: 10 Standby: 0 Unknown: 0

Total: 4

Figure 12-20. Network Overview

12.12 Monitoring At a Glance — Terminal Status Report

The “At-a-Glance” Terminal Status Report is a manual report operation that can produces a snapshot view of one or more configured network terminals and the associated infrastructure elements, from the view point of the terminal. The report gives the Terminal Name, Status, Online/Offline Time, DID, SAT 0 IP Address, Current iNet, Current Average C/N$_0$, Current Average SNR, Failed ACQ Attempts, GPS Location, and Altitude.



Terminal Status Report

Terminal Name	Status	Online/ Offline Time	DID	SAT0 IP Address	Current iNet	Current Beam	Current Avg C/N0 (dBHz)	GPS Position	Altitude (meters)
Terminal-0	Online	4d 3h 7m 17s	335544340	10.1.0.1,10.3.0.3	SpaceCo Beam #8: iNet #1	SpaceCo Beam #9	8290694805919370240	79.01 °N, 72.11 °E	-1735120308
Terminal-11	Online	4d 0h 47m 47s	335544363	10.1.0.45,10.3.0.63	SpaceCo Beam #6: iNet #1	SpaceCo Beam #8	1063498017761389952	87.73 °N, 87.41 °E	-1251480665
Terminal-12	Online	4d 0h 47m 47s	335544365	10.1.0.47,10.3.0.65	SpaceCo Beam #6: iNet #1	SpaceCo Beam #4	8093429225756820480	40.08 °N, 17.84 °E	-1848517466
Terminal-13	Online	4d 0h 47m 47s	335544367	10.1.0.49,10.3.0.67	SpaceCo Beam #5: iNet #1	SpaceCo Beam #6	1597130799298119936	29.55 °N, 34.26 °E	-1683117499

0 of 4 selected

Figure 12-21. NMS At-A-Glance Terminal Status Report.

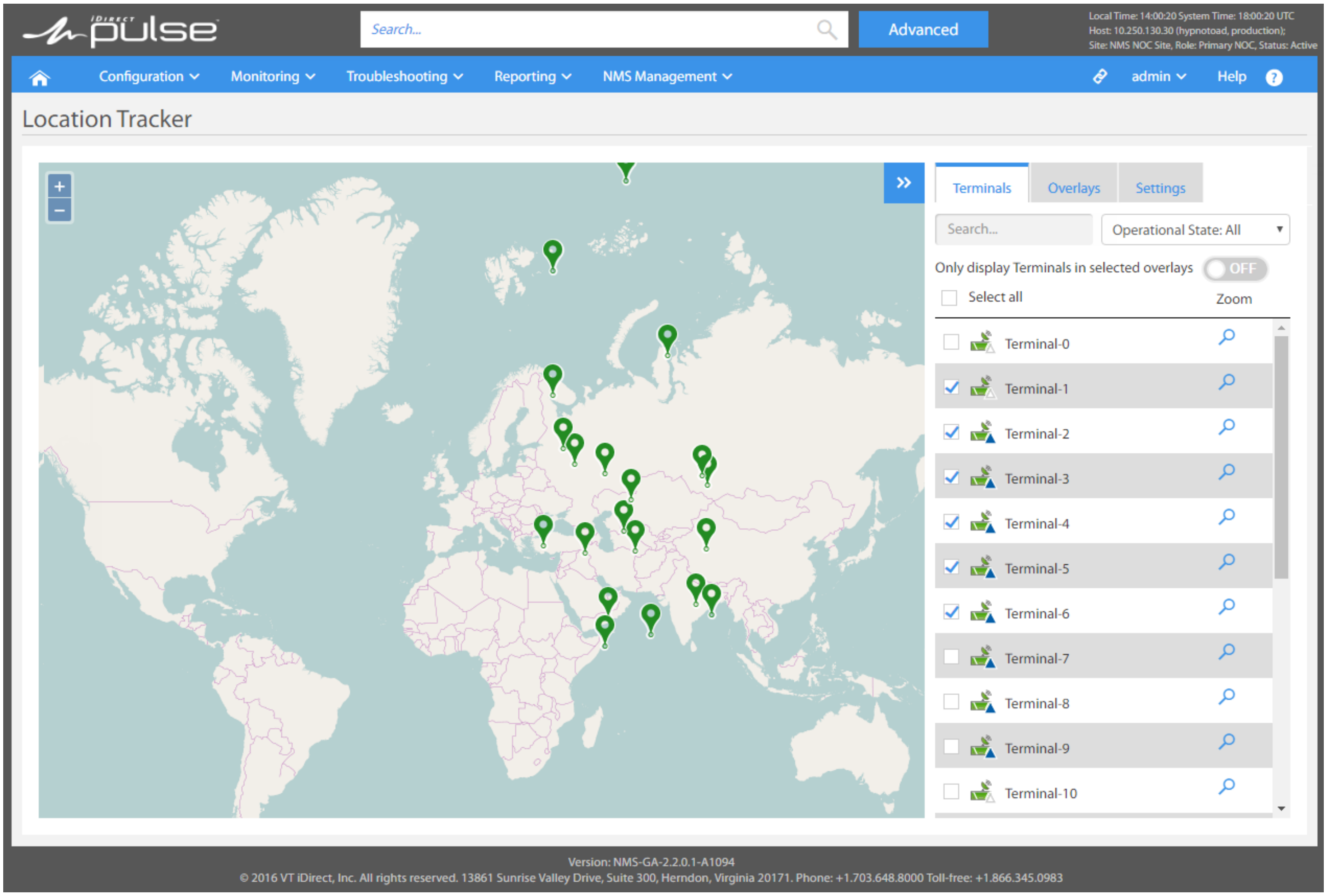
To get an at-a-glance view using terminal status report:

1. Click the **Monitoring** tab, and under **At A Glance**, select **Terminal Status**.
2. Click the **Enable Auto-Refresh** button to allow automatic refresh of the report as changes occur.
3. Click the **Disable Auto-Refresh** button to stop automatic refresh of the report.
4. Click on any element icon to open the element KIP report.

12.13 Monitoring at a Glance — Location Tracker

The *Location Tracker* tool, accessed under the At-a-Glance menu of the Pulse Monitoring tab, allows users to access a mapped view of mobile and fixed satellite terminals for a given network. The 2D Google Map-based system shows a real-time view of where all sites are located and the precise location of individual terminals or an entire group of terminals. With a single click on any terminal, the terminal Key Information Panel (KIP) provides Service Providers with on the spot summary data for each terminal.

In addition to providing summary data, Location Tracker allows users to track the location of mobile network terminals, and to view the environmental conditions that the terminal may be experiencing. The map-based system features current satellite imagery, satellite footprints, real-time weather radar, and mapping tools using overlays.



Local Time: 14:00:20 System Time: 18:00:20 UTC
Host: 10.250.130.30 (hypnotoad, production);
Site: NMS NOC Site, Role: Primary NOC, Status: Active

Operational State: All

Only display Terminals in selected overlays OFF

☐ Select all

☐ Terminal-0
☑ Terminal-1
☑ Terminal-2
☑ Terminal-3
☑ Terminal-4
☑ Terminal-5
☑ Terminal-6
☐ Terminal-7
☐ Terminal-8
☐ Terminal-9
☐ Terminal-10

Version: NMS-GA-2.2.0.1-A1094
© 2016 VT iDirect, Inc. All rights reserved. 13861 Sunrise Valley Drive, Suite 300, Herndon, Virginia 20171. Phone: +1.703.648.8000 Toll-free: +1.866.345.0983

Figure 12-22. Location Tracker

- Shows 2D map/satellite real-time view of terminals and their geolocations
- Immediately view current position of a given set of terminals (fixed and mobile)
- Shows Beams, Service Areas, and/or Regulatory Area where terminals are located.
- Weather overlays for existing Clouds and Precipitation.
- Ability to zoom in/out of the map to a specific location and terminal
- All data can be continuously streamed without need for refresh or switched off
- Toggle overlays to show additional information about weather, beams, SA, and RAs
- Clustering to group terminals within a certain radius of each other
- Users only see the terminals they have permissions to view
- Click terminal name to open the associated Key Information Panel (KIP)
- Show/Hide location Tracker configurator tabs section to view the entire map

12.13.1 The Terminal Tab

From the Terminal tab, all network terminals can be selected to display on the map, or terminals may be individually selected to display. The actions that are possible from the terminal tab, are described using the numbered elements shown on the tab:

1. **Search Field**: Start typing any part of the terminal name to filter the list of terminals to only show the elements whose name includes the typed characters.
2. **Operational State**: Display only those terminals that are currently in the selected state — for example, All, Online, Unknown, Offline:Initializing; Offline:Failed
3. **Select All**: Click the check box to enable the display of all network terminals.
4. **ON/OFF**: Select **ON** to display on the map, only the terminals that are located in any of the currently selected overlays — for example, Beams 1, Beam 2, SA1, SA2. Only those terminals located in any of these overlays are displayed on the map.
5. **Terminal Icon/Name**: Hover on terminal name/icon to show the terminal map location.
6. **Magnifier Icon**: Click on magnifier icon for a terminal to zoom in on the terminal exact location, in the world.

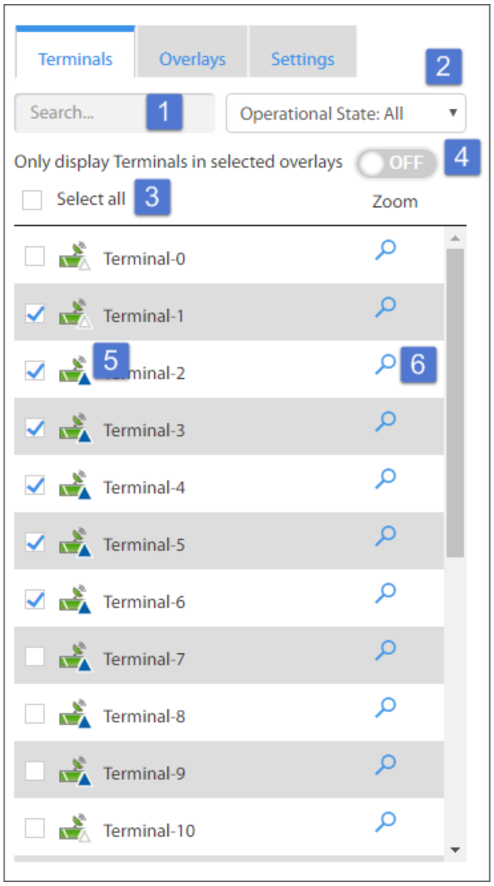


Figure 12-23. Location Tracker - Terminal Tab

12.13.2 Overlays Tab

A Location Tracker *overlay* is a graphical image that is superimposed onto the map, to provide an additional layer of information — for example, weather patterns, satellite footprints, or other information. From the **Overlay** tab, any one or more overlays or overlay sub-components may be selected to be superimposed on the map.

The overlay tab components are described, below, using the numbered elements on the tab:

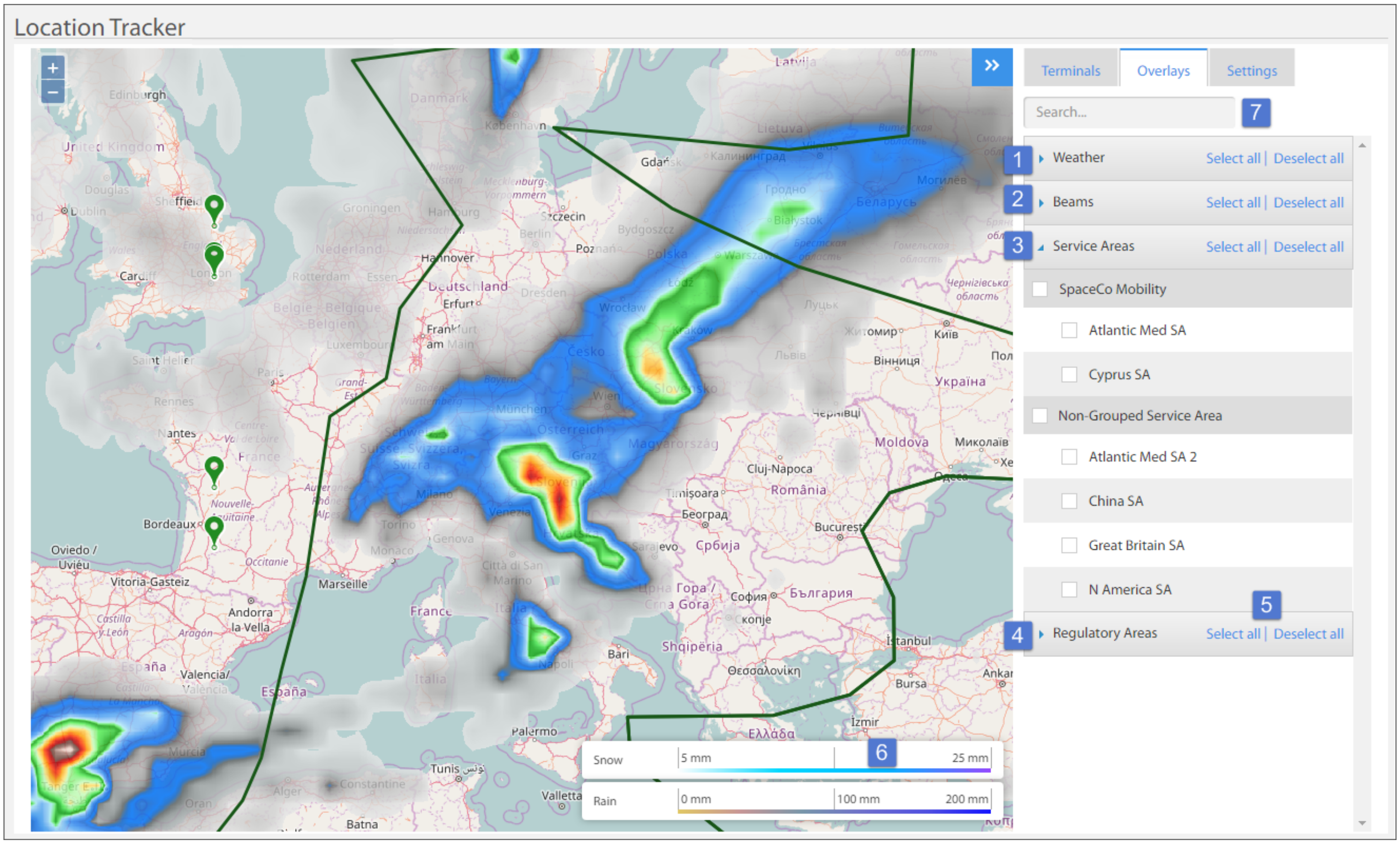


Figure 12-24. Location Tracker - Overlay Tab

1. **Weather**: A set of overlays that show the nearby conditions in which a terminal is located and may be currently experiencing. Weather overlays, for example — include Clouds and Precipitation (rain, snow, or sleet). Using these overlays the NOC Operator can quickly gain a picture of weather conditions that may be affecting the terminals.

   For example: an operator has received a call from a remote site noting a slow link, and believes that the cause is due to some sort of weather effect. By selecting the site in Location Tracker, and enabling a weather overlay for that site's region, the operator can confirm that there is a severe storm moving through that area.

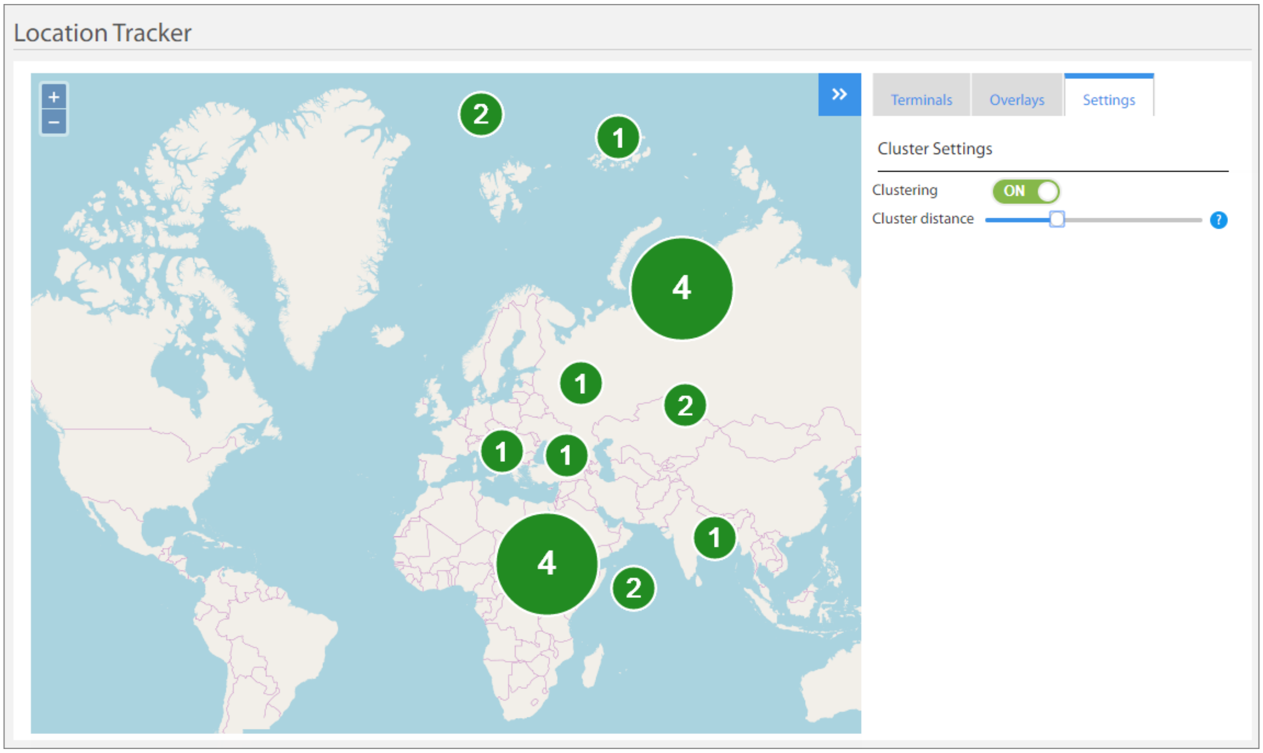
2. **Beams**: Provides a list of beams that are in the network, and that can be overlayed onto the map. If a beam is selected, it is outlined on the map and only the terminals located within the selected beams are shown on the map. Multiple beams may be selected.

3. **Service Areas**: Provides a list of all service areas (SAs) of the network. If an SA is selected, that SA is outlined on the map and only the terminals located within the selected SAs are shown on the map. Multiple SA elements may be selected.
4. **Regulatory Areas**: Provides a list of all regulatory areas (RAs) of the network. If an RA is selected, that RA is outlined on the map and only the terminals currently located within the selected RAs are shown on the map. Multiple RA elements may be selected.
5. **Select All |Deselect All**: Click to select all or deselect all of the overlay components.
6. **Precipitation: Rain | Snow**: Precipitation level indicators.
7. **Search Field**: Start typing any part of the terminal name to filter the list of terminals to only show the elements whose name includes the typed characters.

12.13.3 Settings Tab

Using the Location Tracker **Settings** tab, the map *Clustering* feature can be enabled or disabled. When enabled, terminals within near proximity of one another are grouped into clusters that are displayed as circles that contain a numeric value of the number of terminals in the cluster.

By moving the Cluster Distance slider, to the left or right, you can decrease or increase the distance between clusters. Increasing the distance between clusters causes the circles to be larger and to include more terminals within the cluster. Conversely, decreasing the distance between clusters causes the circles to be smaller and to include fewer terminals.



Cluster Settings

Clustering ON

Cluster distance

Figure 12-25. Location Tracker - Overlay Tab

13 Reporting Operations

Pulse NMS Reporting provides operator access to a variety of customizable history reports based on archived iDirect Network data. These operations include historical reports of network events, alarms, and incidents, as well as a variety of historical reports of network element status and operational and performance statistics of satellite terminals, and other physical and logical network elements.

Pulse Reporting operations are covered in the following topics:

13.1 About Pulse Network Report Builder Operations

iDirect Pulse® **Reporting** operations are partitioned into two sub-menus. The **Report Builder** operations, which are described in this chapter, and **Pre-Defined Reports** operations, which are described in the following chapter.

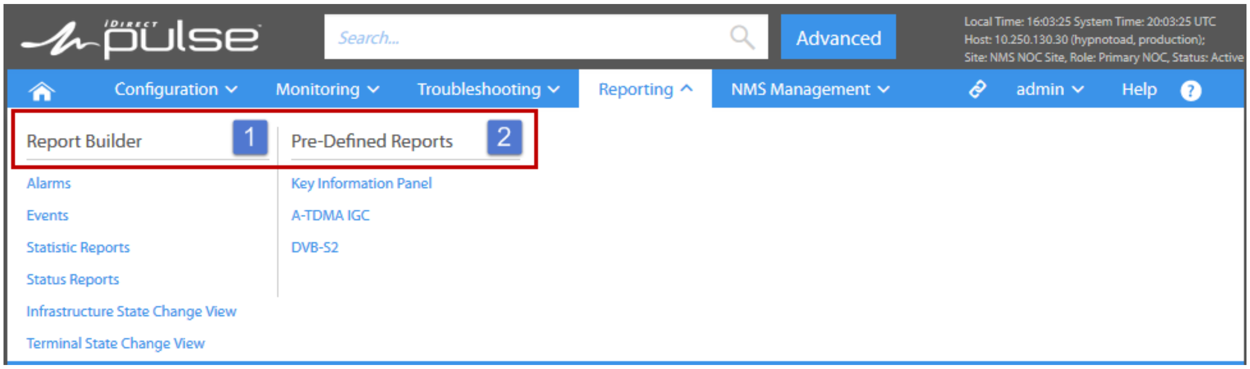


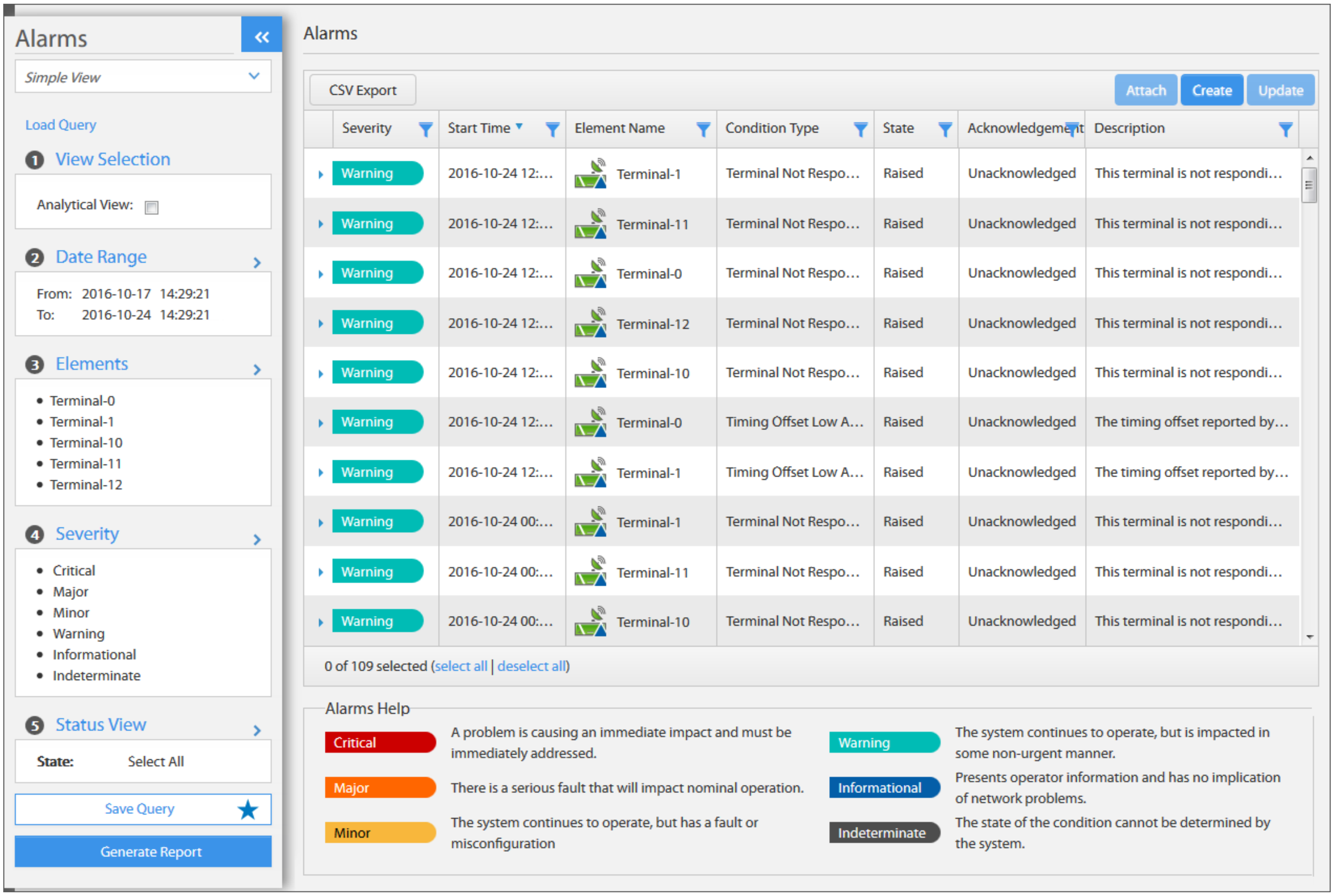
Figure 13-1. Pulse Reporting Menu - Report Builder Operations

Pulse NMS **Reporting** operations support the following types of historical report requests:

- **Alarms** — Use this operation to manually specify Configurator settings such as Date Range, Elements, and Severity to return a customized history report of network alarms.
- **Events** — Use this operation to manually specify settings such as Date Range, Elements, and Severity to return a customized history report of network events.
- **Statistics Reports** — Manually specify settings to generate an historical statistics report for one or more elements based on specific metrics. For example, report IP traffic statistics for one or more terminals over a given period.
- **Status Reports** — Use this operation to manually specify settings to generate an historical Status report for one or more elements, based on specific metrics. For example, report Falcon State or FLL Lock, for one or more line cards during a period.
- **Infrastructure State Change View** — Obtain a change-of-state history report for one or more infrastructure elements over a specified period. These elements include hub-side components PP Cluster, PP Server, NMS Cluster, NMS Server, Line Card, and Chassis; and RF components, Satellite, Beam, Channel, iNet, Inroute Group, Downstream and Upstream Carrier.
- **Terminal State Change View** — Use this operation to obtain a change-of-state history report for any one or more satellite terminals during a specified period.

13.2 Generating an Alarms History Report

Using the **Report Builder** menu under the main **Reporting** menu, users can access the **Configurator** to manually configure an **Alarm History** report of network Alarms that have occurred during a user-specified period, for all elements or for a designated set of elements. An historical Alarms report can go back for as far as 90 days.



Analytical View: ☐

From: 2016-10-17 14:29:21
To: 2016-10-24 14:29:21

- Terminal-0
- Terminal-1
- Terminal-10
- Terminal-11
- Terminal-12

- Critical
- Major
- Minor
- Warning
- Informational
- Indeterminate

State: Select All

Severity	Start Time	Element Name	Condition Type	State	Acknowledgement	Description
Warning	2016-10-24 12:...	Terminal-1	Terminal Not Respo...	Raised	Unacknowledged	This terminal is not respondi...
Warning	2016-10-24 12:...	Terminal-11	Terminal Not Respo...	Raised	Unacknowledged	This terminal is not respondi...
Warning	2016-10-24 12:...	Terminal-0	Terminal Not Respo...	Raised	Unacknowledged	This terminal is not respondi...
Warning	2016-10-24 12:...	Terminal-12	Terminal Not Respo...	Raised	Unacknowledged	This terminal is not respondi...
Warning	2016-10-24 12:...	Terminal-10	Terminal Not Respo...	Raised	Unacknowledged	This terminal is not respondi...
Warning	2016-10-24 12:...	Terminal-0	Timing Offset Low A...	Raised	Unacknowledged	The timing offset reported by...
Warning	2016-10-24 12:...	Terminal-1	Timing Offset Low A...	Raised	Unacknowledged	The timing offset reported by...
Warning	2016-10-24 00:...	Terminal-1	Terminal Not Respo...	Raised	Unacknowledged	This terminal is not respondi...
Warning	2016-10-24 00:...	Terminal-11	Terminal Not Respo...	Raised	Unacknowledged	This terminal is not respondi...
Warning	2016-10-24 00:...	Terminal-10	Terminal Not Respo...	Raised	Unacknowledged	This terminal is not respondi...

0 of 109 selected (select all | deselect all)

Alarms Help

Critical	A problem is causing an immediate impact and must be immediately addressed.	Warning	The system continues to operate, but is impacted in some non-urgent manner.
Major	There is a serious fault that will impact nominal operation.	Informational	Presents operator information and has no implication of network problems.
Minor	The system continues to operate, but has a fault or misconfiguration	Indeterminate	The state of the condition cannot be determined by the system.

Figure 13-2. NMS Alarms History Report

To manually generate an alarm history report for one or more elements:

1. Click the **Reporting** tab, and under **Report Builder**, select **Alarms**.
2. If desired, select the **Advanced View** option to display an extended set of parameters.
3. If applicable, click **Load Query** to load a saved set of parameters for this report.
4. Under **View Selection**, select **Analytical View** to enable this section in order to configure an analytical view of the report. The **Analytical View** renders the **Alarms History** report in a graphical format, in which a visual correlation of the data is presented using line, area, bar, and pie charts.

5. Click the **Date Range** bar and specify a range or select any one of the pre-defined periods — for example **Last 7 Days**, for which the report should be generated; enable **Stream** to report new alarm data as it arrives; and click **Add Date Range** to close the dialog.
6. Click the **Element Selector** to open the Basic Search tool or click **Advanced Search**, to find and specify one or more specific elements or element types to be included.
7. Click the **Severity** bar, to specify one or more severity levels to be included in the alarms report. By default all severity levels are included, but may be unselected as required.
8. Click the **Status View** selector bar if the default settings, for displaying the alarms report, are to be modified. See *Modifying the Default Status View* on page 56.
9. Click **Generate Report** to generate and view the **Alarm History** report. The default display of the **Alarm History** report is opened.
10. To view the details of an alarm, see *Expanding the Status View*.
11. Use **Save Query**, to save the report configuration for future use.

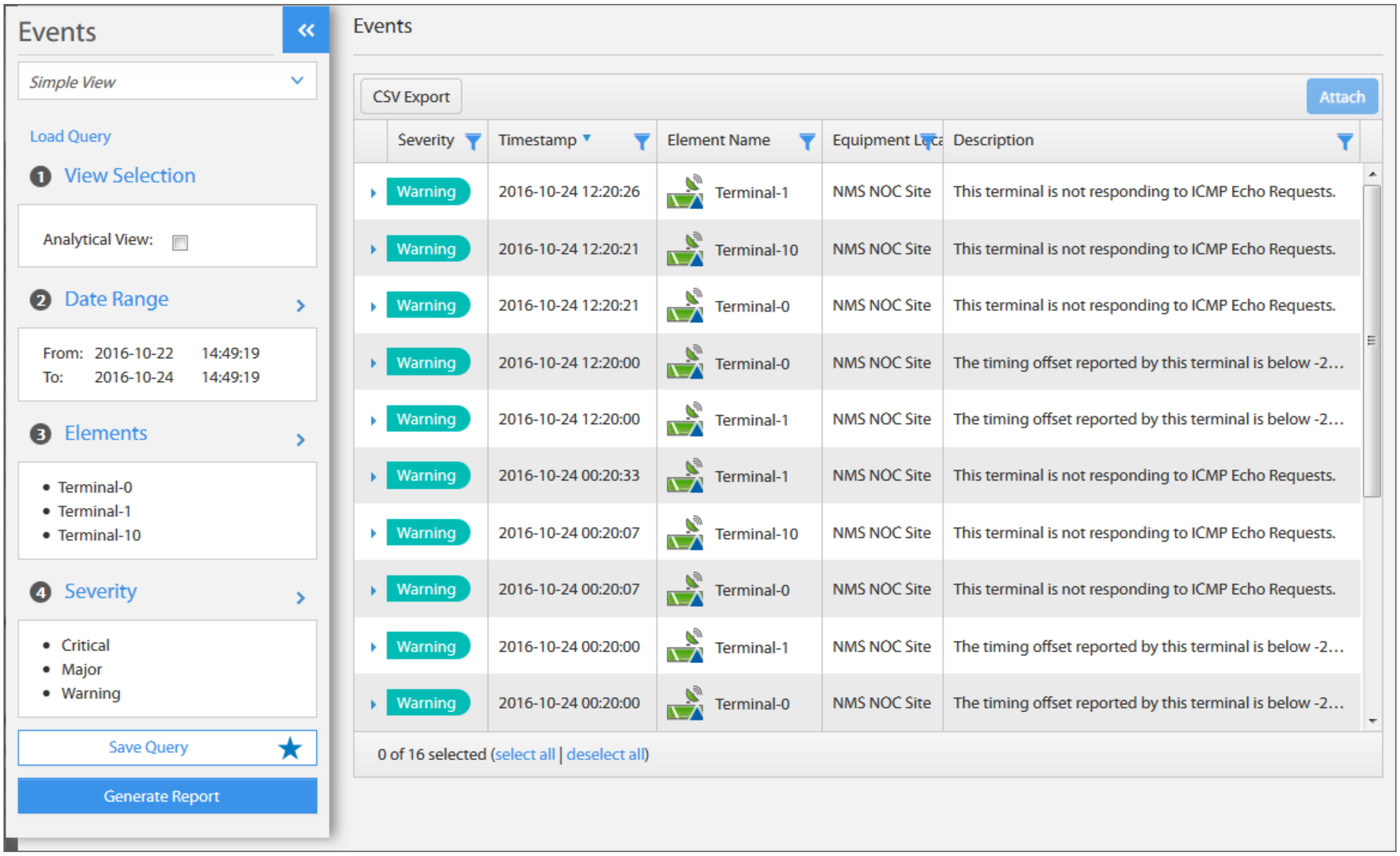
13.3 Generating an Events History Report

Using the **Report Builder** menu under the main **Reporting** menu, users can use the **Report Configurator** to manually configure an **Event History** report of network Events that have occurred during a user-specified period, and associated with all elements or for a selected set of elements.

To manually generate an event history report for one or more elements:

1. Click the **Reporting** tab > **Report Builder > Events**. By default, the **Report Configurator** opens, with the **Simple View** option selected.
2. Select **Advanced Configurator Fields** to display an extended set of parameter fields.
3. If applicable, click **Load Query** to load a previously saved Configurator parameter set.
4. Under **View Selection**, select **Analytical View** to enable this section to configure an analytical view of the report. The **Analytical View** renders the **Events, Alarms,** and **Incidents** report in a graphical format, in which a visual correlation of the data is presented using line, area, bar, and pie charts.
5. Click **Date Range** and specify a range or select any one of the pre-defined periods — for example **Last 7 Days**, for which the report should be generated; enable **Stream** to report new event data as it arrives; and click **Add Date Range** to close the dialog.
6. Click the **Element Selector** to open the Basic Search tool or click **Advanced Search**, to find and specify one or more specific elements or element types to be included.
7. Click the **Severity** bar, to specify one or more severity levels to be included in the events report. By default all severity levels are included, but may be unselected as required.
8. If the Configurator **Advanced View** was selected, the **Log View** selector will be shown. Click the **Log View** selector bar if the default settings for displaying the events report is to be modified. See *Modifying the Default Log View* on page 59.

9. If the Configurator **Advanced View** was selected, the **Report Preferences** selector will be shown. Use the Output Type drop-down list to select whether the report should be rendered in a **Grid** format or as a **CSV Download** file.
10. Click **Generate Report** to generate and view the **Event History** report. The default display of the **Event History** report is opened.
11. To view the details of an event, see *Expanding the Log View*.
12. Use **Save Query**, to save the report configuration for future use.



Analytical View: ☐

From: 2016-10-22 14:49:19
To: 2016-10-24 14:49:19

- Terminal-0
- Terminal-1
- Terminal-10

- Critical
- Major
- Warning

Severity	Timestamp	Element Name	Equipment Loca	Description
Warning	2016-10-24 12:20:26	Terminal-1	NMS NOC Site	This terminal is not responding to ICMP Echo Requests.
Warning	2016-10-24 12:20:21	Terminal-10	NMS NOC Site	This terminal is not responding to ICMP Echo Requests.
Warning	2016-10-24 12:20:21	Terminal-0	NMS NOC Site	This terminal is not responding to ICMP Echo Requests.
Warning	2016-10-24 12:20:00	Terminal-0	NMS NOC Site	The timing offset reported by this terminal is below -2…
Warning	2016-10-24 12:20:00	Terminal-1	NMS NOC Site	The timing offset reported by this terminal is below -2…
Warning	2016-10-24 00:20:33	Terminal-1	NMS NOC Site	This terminal is not responding to ICMP Echo Requests.
Warning	2016-10-24 00:20:07	Terminal-10	NMS NOC Site	This terminal is not responding to ICMP Echo Requests.
Warning	2016-10-24 00:20:07	Terminal-0	NMS NOC Site	This terminal is not responding to ICMP Echo Requests.
Warning	2016-10-24 00:20:00	Terminal-1	NMS NOC Site	The timing offset reported by this terminal is below -2…
Warning	2016-10-24 00:20:00	Terminal-0	NMS NOC Site	The timing offset reported by this terminal is below -2…

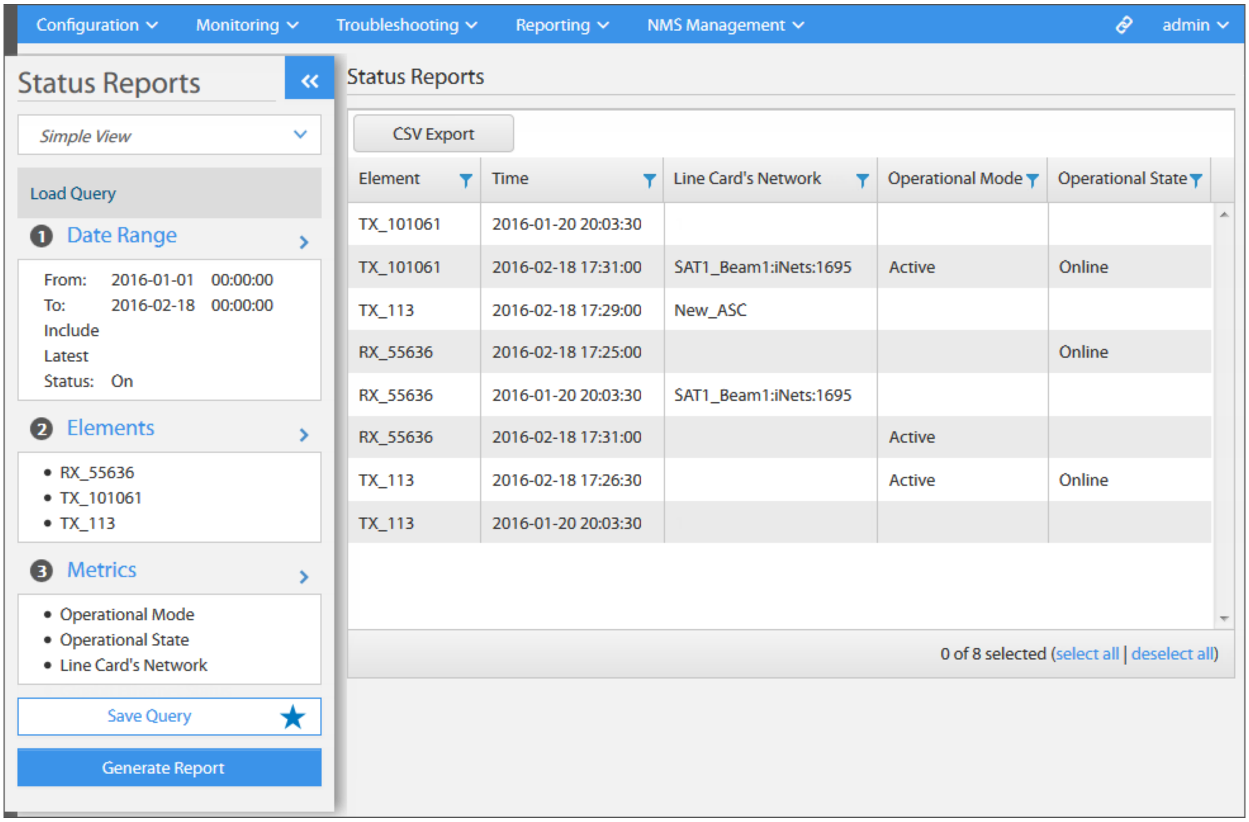
0 of 16 selected (select all | deselect all)

Figure 13-3. NMS Events History Report

13.4 Generating a Status History Report

Having a history of the status of a network element can help diagnose and resolve problems that may have been occurring over time. The Configurator **Status Report** is used to generate a report of the various statuses of a network element over a given period. Various statuses of a terminal, for example, can include items like its geographic location, altitude, iNet, Inroute Group, PP server, service area, satellite, and beam.

A status report can be configured to report against the status of one or more elements of the same type, and use one or more metrics. The best results are achieved, however, when 5 or fewer metrics are specified.



From: 2016-01-01 00:00:00
To: 2016-02-18 00:00:00
Include Latest Status: On

- RX_55636
- TX_101061
- TX_113

- Operational Mode
- Operational State
- Line Card's Network

Element	Time	Line Card's Network	Operational Mode	Operational State
TX_101061	2016-01-20 20:03:30			
TX_101061	2016-02-18 17:31:00	SAT1_Beam1:iNets:1695	Active	Online
TX_113	2016-02-18 17:29:00	New_ASC		
RX_55636	2016-02-18 17:25:00			Online
RX_55636	2016-01-20 20:03:30	SAT1_Beam1:iNets:1695		
RX_55636	2016-02-18 17:31:00		Active	
TX_113	2016-02-18 17:26:30		Active	Online
TX_113	2016-01-20 20:03:30			

Figure 13-4. Historic Status Report

To configure and generate a Status History report:

1. Click the **Reporting** tab > **Report Builder > Report Status**.
2. If applicable, click **Load Query** to load a previously saved Configurator parameter set.
3. Click **Date Range** and enter a report period or use one of the pre-defined periods.
4. Click the **Elements** selector to open the **Basic Search** window. All elements for which status data is collected are listed. The elements selected for this report should be of the same type, but may differ if they share a common metric.
5. With the Basic Search dialog open, do one of the following as required:

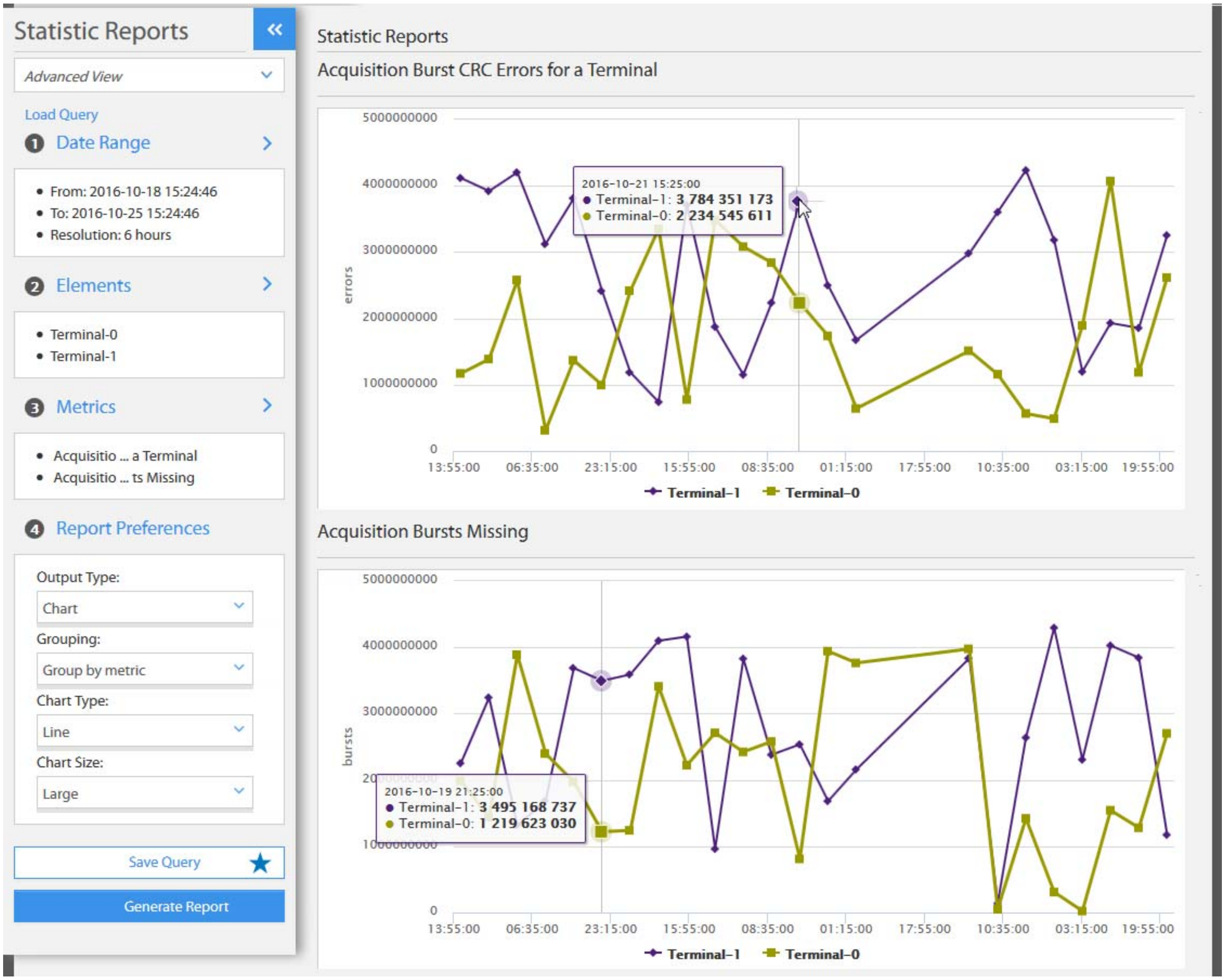
   a. From the displayed list of network elements, specify one or more elements for which an historical status report should be generated.
   b. Use the **Element Type** filter to display a single element type - for example **iNets** or **Terminals**, and select one or more of the elements to return to the Configurator.
   c. Click **Advanced Search** to open the **Custom Query** dialog to compose an extended query; and select one or more of the listed results to return to the Configurator.
6. Click the **Metrics** bar, to open the **Basic Search** window to select one or more metrics from the context-sensitive list of metrics. If elements of different types are configured in the report, only those metrics that the selected elements have in common are listed.
7. Click **Done** to add the metrics to the dialog.
8. If desired, click **Save Query** to save the **Status Report** configuration as a query.
9. Click **Generate Report.**

13.5 Generating a Statistics History Report

The Pulse **Statistics Report** is used to produce a statistics history report on specific operational metrics of a network element, captured over time. For example the report might capture data such as TCP traffic transmitted, total data volume transmitted or received. The statistics report is manually configured using the Configurator, and, based on user selections.

An element statistics report can be based on one or more metrics for any one or more physical elements, such as Line Cards, Terminals, Chassis; or logical elements such as Beam, iNet, Inroute Group Composition, Group Service Plan, or Subscriber Service Plan Component.

If the report is configured for multiple metrics, multiple elements, or both, the report output is based on the user settings in the Report Preferences dialog. The Configurator **Report Preferences** section is only displayed if the **Advanced View** Configurator option is selected.



Statistic Reports

Advanced View

Load Query

1 Date Range

- From: 2016-10-18 15:24:46
- To: 2016-10-25 15:24:46
- Resolution: 6 hours

2 Elements

- Terminal-0
- Terminal-1

3 Metrics

- Acquisitio ... a Terminal
- Acquisitio ... ts Missing

4 Report Preferences

Output Type: Chart

Grouping: Group by metric

Chart Type: Line

Chart Size: Large

Statistic Reports

Acquisition Burst CRC Errors for a Terminal

2016-10-21 15:25:00
- Terminal-1: 3 784 351 173
- Terminal-0: 2 234 545 611

Acquisition Bursts Missing

2016-10-19 21:25:00
- Terminal-1: 3 495 168 737
- Terminal-0: 1 219 623 030

Figure 13-5. Historic Statistics Report

To configure and generate a Statistics History report:

1. Click the **Reporting** tab > **Report Builder > Report Statistics**. The Configurator opens, with the default option of **Simple View** selected.
2. Select **Advanced View** to display the Configurator **Report Preferences** selector.
3. If applicable, click **Load Query** to load a previously saved Configurator parameter set.
4. Click the **Date Range** bar and specify a report period or one of the pre-defined periods.
5. Click the **Elements** selector to open the **Basic Search** window. The elements selected for this report should be of the same type, but may differ if they share a common metric.
6. With the Basic Search dialog open, do one of the following as required:
   a. From the displayed list of network elements, specify one or more elements for which the report should be generated.
   b. Use the **Element Type** filter to display a single element type - for example **iNets** or **Terminals**, and select one or more of the elements to return to the Configurator.
   c. Click **Advanced Search** to open the **Custom Query** dialog to compose an extended query; and select one or more of the listed results to return to the Configurator.
7. Click the **Metrics** bar, to open the **Basic Search** window to select one or more metrics from the context-sensitive list of metrics.
8. Click the blue icon adjacent to a metric group to show the available metrics.
9. Select one or more metrics for the report.
10. Click **Done** to add the metrics to the dialog.
11. If the **Report Preferences** selector is displayed, use the drop-down lists as follows:
    a. **Object Type:** select **Chart** or **CSV Download.**
    b. **Grouping:** select **Group by Element, Group by Metric**, or **Group by Metric of Same Type.**
    c. **Graph Type:** select **Line** or **Area.**
    d. **Chart Size:** select **Small**, **Medium**, **Large**, or **Extra Large**.
12. Click **Generate Report.**

Table 13-1. Configurator Report Preferences Options for Statistics

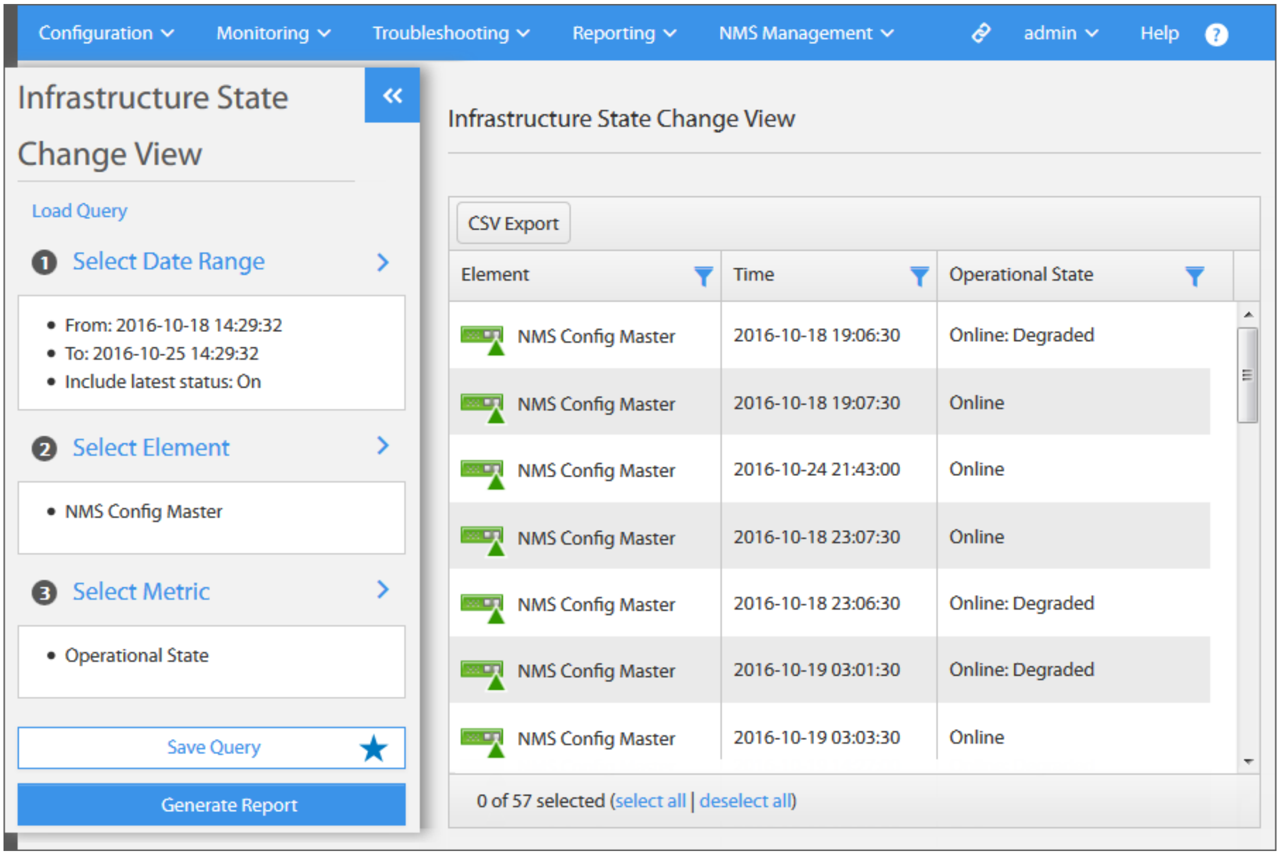
Report Preference Option	Description
Group By: Group By Element	Produces a single chart per element (multiple metrics by color)
Group By: Group By Metric	Produces a single chart per metric (multiple elements by a color)
Group By: Group By Metric of Same Type	Produces a single chart per set of shared metric (multiple elements by a color)

13.6 Infrastructure State Change Report

The **Infrastructure State Change Report** is used to capture a history report of the operational state changes of one or more selected network infrastructure elements, over a specified period of up to 90 days.

Network infrastructure elements include physical elements including PP Cluster, PP Server, NMS Cluster, NMS Server, Line Card, and Chassis; and logical elements including Satellite, Beam, Channel, Downstream Carrier, Upstream Carrier, IF Domain, iNet, and Inroute Group.

If the report is configured for multiple infrastructure elements, then the report will display the results of the elements, interleaved based on the time of the state-change occurrence.



Infrastructure State Change View

1. Select Date Range
- From: 2016-10-18 14:29:32
- To: 2016-10-25 14:29:32
- Include latest status: On

2. Select Element
- NMS Config Master

3. Select Metric
- Operational State

Infrastructure State Change View

Element	Time	Operational State
NMS Config Master	2016-10-18 19:06:30	Online: Degraded
NMS Config Master	2016-10-18 19:07:30	Online
NMS Config Master	2016-10-24 21:43:00	Online
NMS Config Master	2016-10-18 23:07:30	Online
NMS Config Master	2016-10-18 23:06:30	Online: Degraded
NMS Config Master	2016-10-19 03:01:30	Online: Degraded
NMS Config Master	2016-10-19 03:03:30	Online

0 of 57 selected (select all | deselect all)

Figure 13-6. Infrastructure State Change Report

To configure and generate an Infrastructure State Change View report:

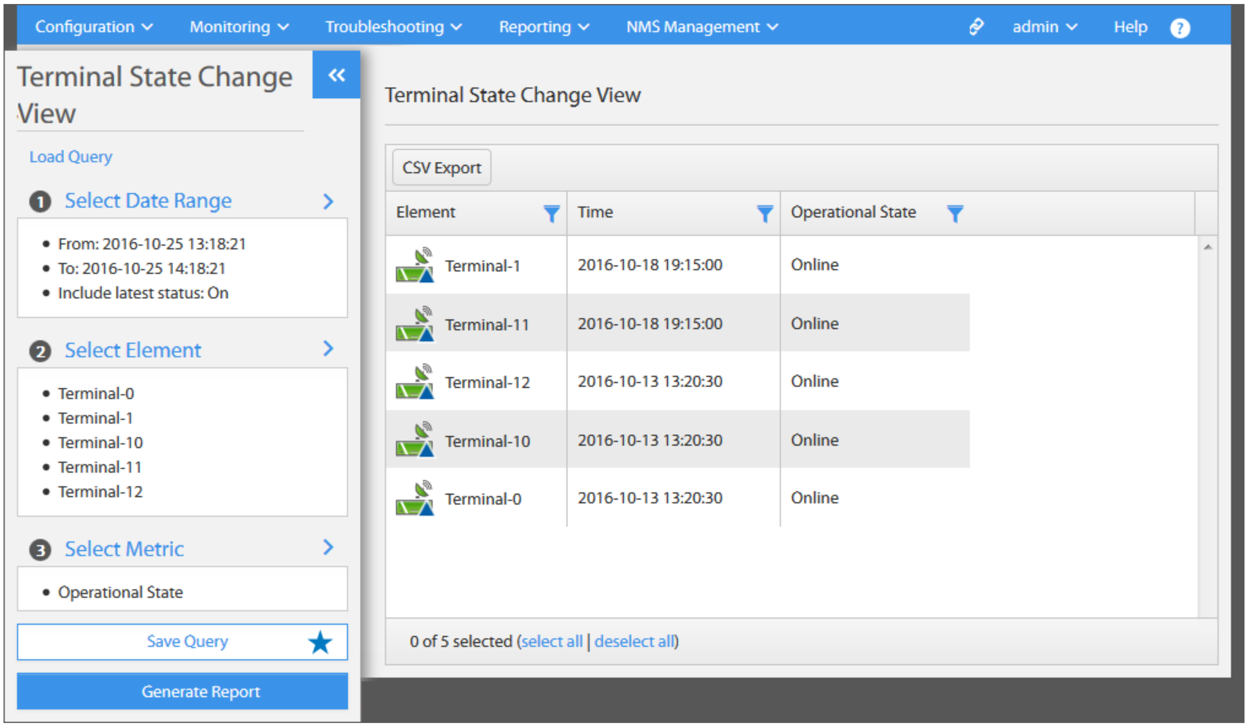
1. Click the **Reporting** tab > **Report Builder > Infrastructure State Change View**.
2. If applicable, click **Load Query** to load a previously saved Configurator parameter set.
3. Click the **Date Range** bar and specify a report period one of the pre-defined periods.
4. Click the **Elements** selector to open the **Basic Search** window.

5. With the Basic Search dialog open, do one of the following as required:
    a. From the displayed list of network infrastructure elements, specify one or more elements for which the report should be generated.
    b. Use the **Element Type** filter to display a single element type - for example **iNets**, and select one or more of the listed elements to return to the Configurator.
    c. Click **Advanced Search** to open the **Custom Query** dialog to compose an extended query; and select one or more of the listed results to return to the Configurator.
6. Click the **Metrics** bar to open the **Basic Search** window.
7. Click the blue icon adjacent to a metric group to show the available metrics.
8. Select **Operational State** as the metric, and click **Done** to add the metrics to the dialog.
9. If desired, click **Save Query** to save the **Infrastructure State Change** report configuration as a query.
10. Click **Generate Report.**

13.7 Terminal State Change Report

The **Terminal State Change Report** is used to capture a history report of the operational state changes of one or more selected Satellite Terminals, over a specified period. The report period can be up to a maximum of 90 days.

If the report is configured for multiple terminals, then the report will display the results for all of the terminals, interleaved based on the time of the state-change occurrence.



Terminal State Change View

1 Select Date Range
- From: 2016-10-25 13:18:21
- To: 2016-10-25 14:18:21
- Include latest status: On

2 Select Element
- Terminal-0
- Terminal-1
- Terminal-10
- Terminal-11
- Terminal-12

3 Select Metric
- Operational State

Terminal State Change View

Element	Time	Operational State
Terminal-1	2016-10-18 19:15:00	Online
Terminal-11	2016-10-18 19:15:00	Online
Terminal-12	2016-10-13 13:20:30	Online
Terminal-10	2016-10-13 13:20:30	Online
Terminal-0	2016-10-13 13:20:30	Online

0 of 5 selected (select all | deselect all)

Figure 13-7. Terminal State Change Report

To configure and generate a Terminal State Change report:

1. Click the **Reporting** tab, and under **Report Builder**, select **Terminal State Change View**. The Configurator opens, with the default option of **Simple View** selected.
2. If applicable, click the **Load Query** to load a previously saved set of Configurator parameters for this report.
3. Click the **Date Range** bar and enter a report period or use one of the pre-defined periods.
4. Click the **Elements** selector open the **Basic Search** window.
5. With the Basic Search dialog open, do one of the following as required:
    a. From the displayed list of Satellite Terminal elements, specify one or more elements for which the report should be generated.
    b. Click **Advanced Search** to open the **Custom Query** dialog to compose an extended query; and select one or more of the listed results to return to the Configurator.

6. Click the **Metrics** bar to open the **Basic Search** window.
7. Click the blue icon adjacent to a metric group to show the available metrics.
8. Select **Operational State** as the metric, and click **Done** to add the metrics to the dialog.
9. If desired, click **Save Query** to save the **Terminal State Change View** report configuration as a query.
10. Click **Generate Report**

14 Pre-Defined Reports

In addition to the standard Reporting operations, Pulse provides a variety of pre-defined reports that include the A-TDMA IGC, DVB-S2, and Adaptive Coding and Modulation (ACM).

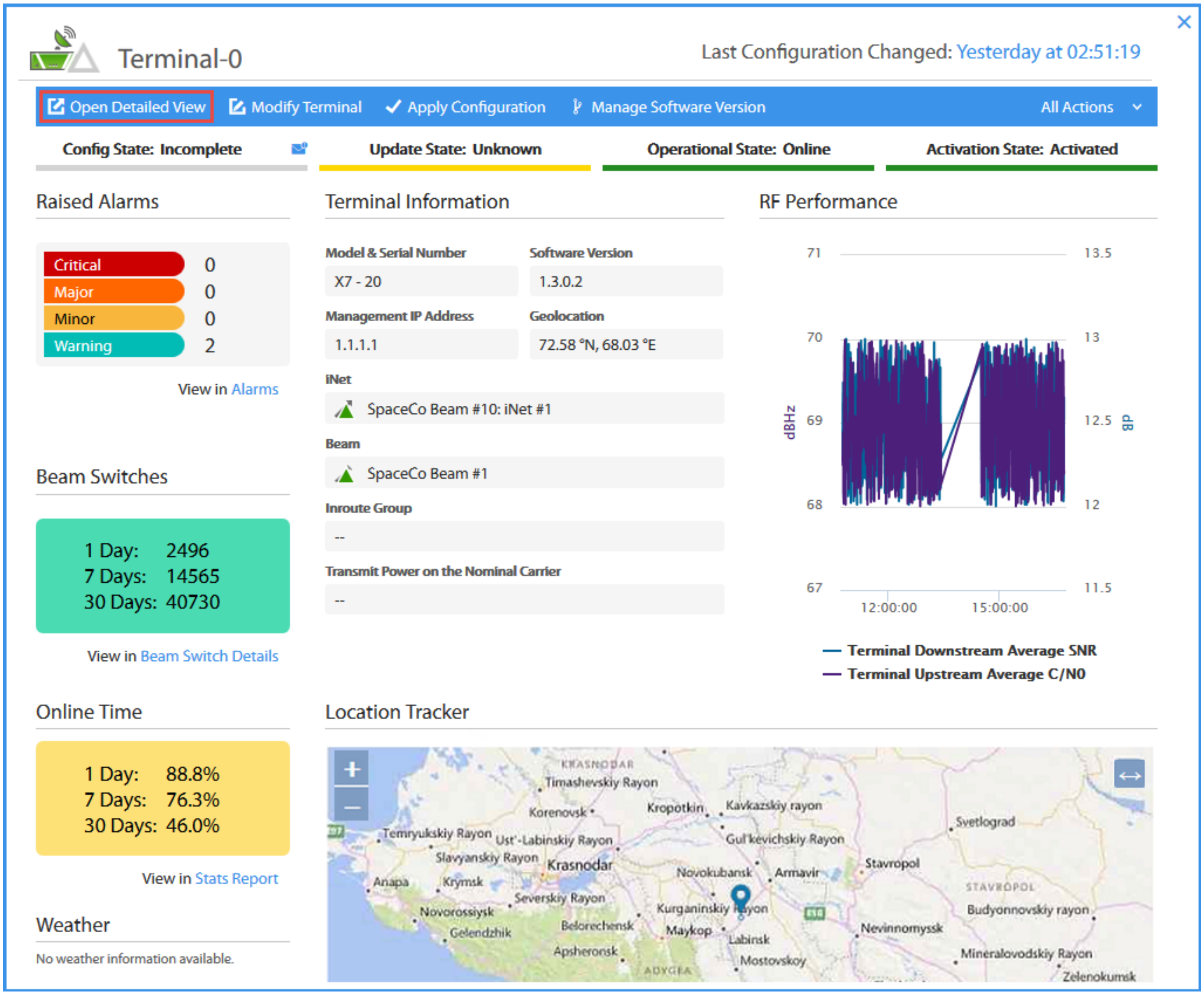
Pulse Pre-Defined Reporting operations are covered in the following topics:

- *Key Information Panel* on page 206
- *Generating an A-TDMA IGC Report* on page 211
- *Generating a DVB-S2 Report* on page 213

14.1 Key Information Panel

Using the **Key Information Panel** (KIP), Network Operators can access a collection of vital and applicable information about any single network element—all in one view. The KIP can be used to access at-a-glance information on any physical or logical network element—for example, a Site, Terminal, Line Card, PP Server; or a GSP, SSPC, or an iNet. Once the KIP is opened, each information widget provides access to drill further down in order to learn more.

The KIP page has two levels of detail — Tier 1 and Tier-2. Tier-1, which is opened when the icon of a particular element is clicked from the search, browse, or report window, presents an at-a-glance view using widgets as shown in Figure 14-1. Tier-2, a more detailed view, is opened by clicking the "**Open Detailed View**" option on the Tier-1 menu bar.



Terminal-0

Last Configuration Changed: Yesterday at 02:51:19

Config State: Incomplete

Update State: Unknown

Operational State: Online

Activation State: Activated

Raised Alarms

Critical	0
Major	0
Minor	0
Warning	2

View in Alarms

Terminal Information

Model & Serial Number: X7 - 20

Software Version: 1.3.0.2

Management IP Address: 1.1.1.1

Geolocation: 72.58 °N, 68.03 °E

iNet: SpaceCo Beam #10: iNet #1

Beam: SpaceCo Beam #1

Inroute Group: --

Transmit Power on the Nominal Carrier: --

Beam Switches

1 Day:	2496
7 Days:	14565
30 Days:	40730

View in Beam Switch Details

Online Time

1 Day:	88.8%
7 Days:	76.3%
30 Days:	46.0%

View in Stats Report

Weather

No weather information available.

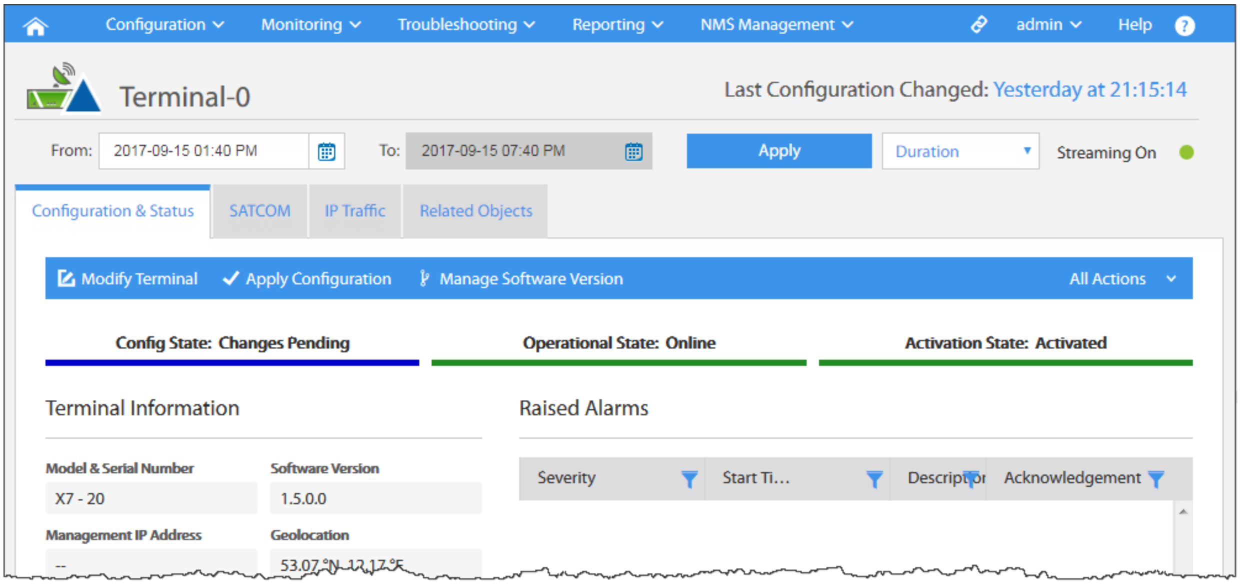
Figure 14-1. Key Information Panel (Tier-1) for Terminal Element

To retrieve the KIP for an element from the Browse or Search window (preferred):

1. From the NMS **Browse** or **Search** window, click the icon of the element in question. The Tier-1 (first level) KIP report for the element is opened.
2. After viewing the KIP Tier-1 information, click the **Open Detailed View** to drill down to additional element details (fastest way to get information) — for a terminal for example:
   a. **Raised Alarms**, **Events**, and **Configuration History**.
   b. Click on a tab to view the analytical graphs of key metrics statistics - for example **SATCOM** or **IP Traffic.**
   c. Click one of the **Action** commands, for example **Modify**, to perform the element action; or click the **All Actions** button to access any of the element actions.

To retrieve the KIP for an element using the Pre-Defined Reports menu (secondary way):

1. Click the NMS **Reporting** tab > **Pre-Defined Reports > Key Information Panel**.
2. If applicable, click the **Load Query** to access a previously saved set of Configurator parameters for the Key Information Panel.
3. Use the **Select Date Range** dialog to specify a date rage or choose a pre-defined period for which the KIP report should be generated.
4. Click the **Select Element** dialog, to open the basic search tool.
5. Use any of the filter fields to narrow the list of displayed elements.
6. Select the element for which a KIP report should be generated.
7. If applicable, click **Save Query**, to save the Configurator settings for the KIP.
8. Click **Generate Report**, to open the Key Information Panel for the selected element. The Tier-2 (secondary level) KIP report for the element is opened.



Terminal-0

Last Configuration Changed: Yesterday at 21:15:14

From: 2017-09-15 01:40 PM To: 2017-09-15 07:40 PM

Streaming On

Config State: Changes Pending

Operational State: Online

Activation State: Activated

Terminal Information

Model & Serial Number: X7 - 20

Software Version: 1.5.0.0

Management IP Address: --

Geolocation: 53.07 °N, 12.17 °E

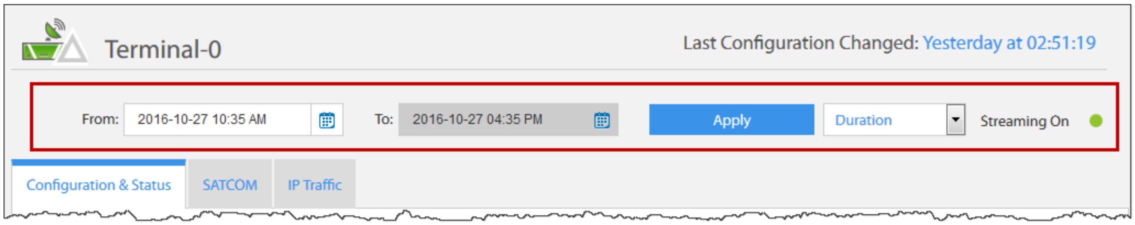
Raised Alarms

Figure 14-2. Key Information Panel (Tier-2) for Terminal Element

14.1.1 KIP Widgets

The Key Information Panel provides a number of associated tools and widgets that provide one-click navigation, quicker access to various tools, and instant visibility of the most vital information for a given element. The following is a list of KIP components and widgets:

- **Date and Time**: which appears in the KIP detailed view, allows easy generation of KIP reports based on a **Date** and **Time** range, using a date/time picker. Alternatively, a pre-defined **Duration** can be selected — for example the **Last 24 hours**. Finally, **Streaming** can be turned ON/Off with a single click to stream KIP data from a specified date and time, and only reloading the data every 30 seconds. Click **Apply** after your selection.



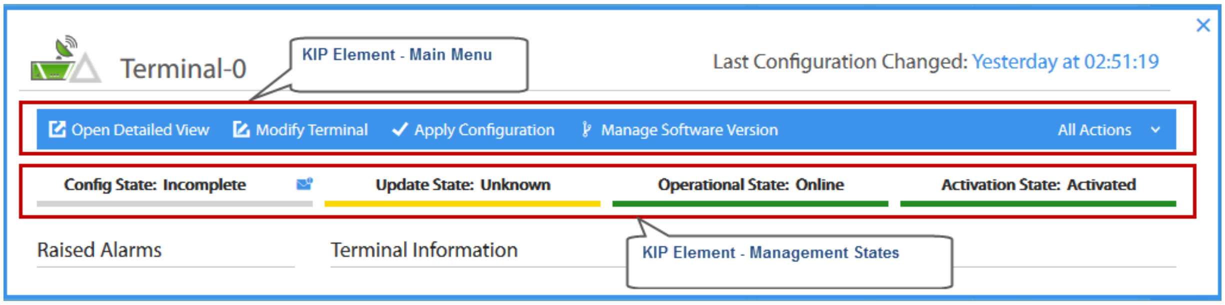
Last Configuration Changed: Yesterday at 02:51:19

From: 2016-10-27 10:35 AM

To: 2016-10-27 04:35 PM

Figure 14-3. KIP Date and Time Bar

- **KIP Main Menu**: the KIP main menu provides quick access to commonly used element actions — for example, Modify Element, Apply Configuration, Manage Software Version, as well as access to **All Actions**. If the KIP was opened by clicking the element icon in the Search, Browse, or Report window, an **Open Detailed View** link to KIP Tier-2 is displayed.
- **Management States**: shows a color-coded view of the current management states for the element. For example, the **Config State**, **Operational State**, and **Activation State**. If an element is **Incomplete**, first click the white triangular overlay icon, then when the status pop-up is presented, click the blue message envelope icon, to the right of the Config State status to determine why the element is incomplete.



Last Configuration Changed: Yesterday at 02:51:19

Config State: Incomplete

Update State: Unknown

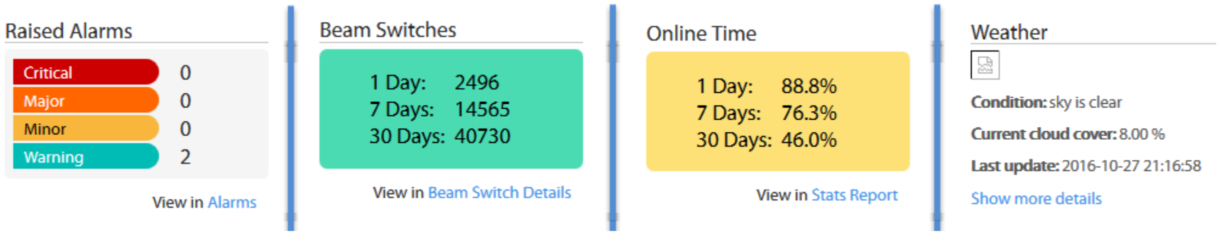
Operational State: Online

Activation State: Activated

Figure 14-4. KIP Main Menu and Management States Bar

- **Configuration History**: this widget, which appears on the KIP detailed view, queries the Activity Log for any changes or updates that have been made for the element. The log is updated to reflect what was shown in the history. Access to the Activity Log is also available from this widget, to drill down to further detail. The widget lists each configuration action, along with the user and date the change was made.

- **Raised Alarms:** reports the number of alarms raised, by severity (**Critical**, **Major**, **Minor**, and **Warning**), in the last 6-hours for the element. Clicking on a non-zero severity category presents a pop-up with a list of the alarms, without leaving the main KIP page. From this widget, click **View in Alarms** to drill down to further alarm details.
- **Beam Switches**: shows the total number of beam switches from the past **1 Day**, **7 Days**, and **30 Days**. Click **Beam Switch Details** to see additional information.
- **Online Time:** shows the percentage of the total time an element has been Online for the past **1 Day**, **7 Days**, or **30 Days**. Click **View Stats Report** to see additional information.
- **Online Weather**: shows the **Condition**, **Current Cloud Cover**, and **Last update** date. Click **Show more details** to see additional information.



Raised Alarms

Critical	0
Major	0
Minor	0
Warning	2

View in Alarms

Beam Switches

1 Day: 2496
7 Days: 14565
30 Days: 40730

View in Beam Switch Details

Online Time

1 Day: 88.8%
7 Days: 76.3%
30 Days: 46.0%

View in Stats Report

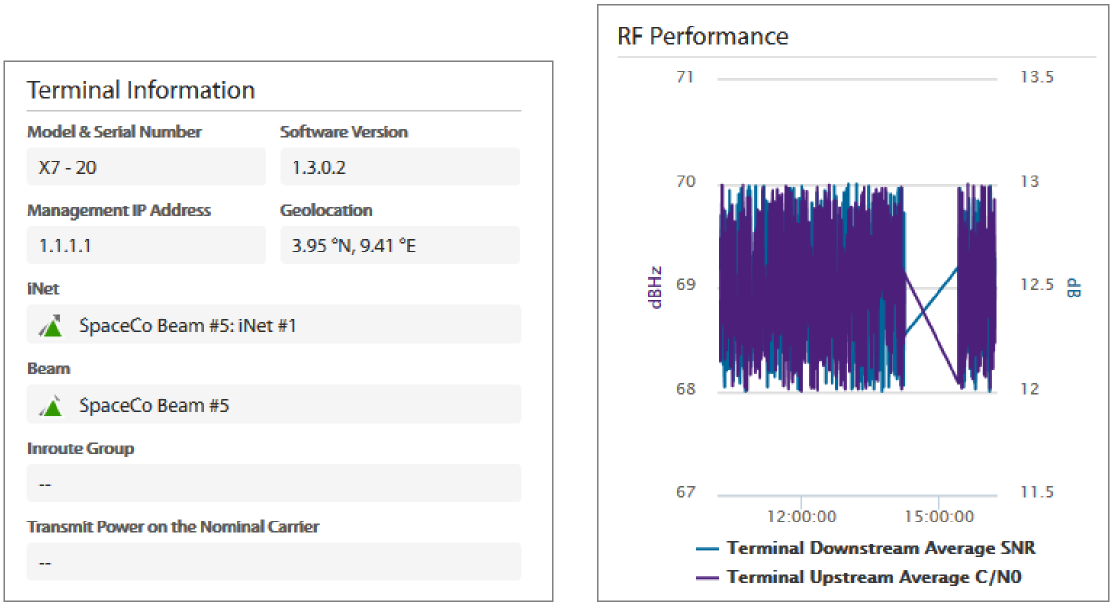
Weather

Condition: sky is clear
Current cloud cover: 8.00 %
Last update: 2016-10-27 21:16:58

Show more details

Figure 14-5. KIP Widgets — Raised Alarms, Beam Switches, Online Time, Weather

- **Element Information**: provides vital element information like Model & Serial Number**,** Software Version, Management IP Address, Geo-location, current iNet & Beam, Inroute Group. In addition to this, an analytical view of a Key Element metric is shown — for example, RF performance is shown for a terminal.



Terminal Information

Model & Serial Number: X7 - 20
Software Version: 1.3.0.2
Management IP Address: 1.1.1.1
Geolocation: 3.95 °N, 9.41 °E
iNet: SpaceCo Beam #5: iNet #1
Beam: SpaceCo Beam #5
Inroute Group: --
Transmit Power on the Nominal Carrier: --

RF Performance

71
70
69
68
67
dBHz
13.5
13
12.5
12
11.5
dB
12:00:00
15:00:00
Terminal Downstream Average SNR
Terminal Upstream Average C/N0

Figure 14-6. KIP Element Information and Key Metric Widgets

14.1.2 KIP Related Objects Tab for Terminal

The **Related Objects** tab, also known as “**Triage View**”, in the terminal KIP **Detailed View,** displays the network objects related to the terminal in the Terminal, Transport, and Service domains, and in the Hub. From the terminal KIP Detailed View, click the **Related Objects** tab.

For objects to which the user has access, the object icon is displayed and can be clicked to open the KIP. If the user does not have permissions for an object, only the name of the object is displayed — for example, iNet, Inroute Group, or Beam.

If any alarms are active for an object for which the user has access, an alarms icon and counter is displayed below the object icon. The alarms icon and counter can be clicked to display a pop-over box, which shows the number of alarms in each category for that object and the details of each alarm.

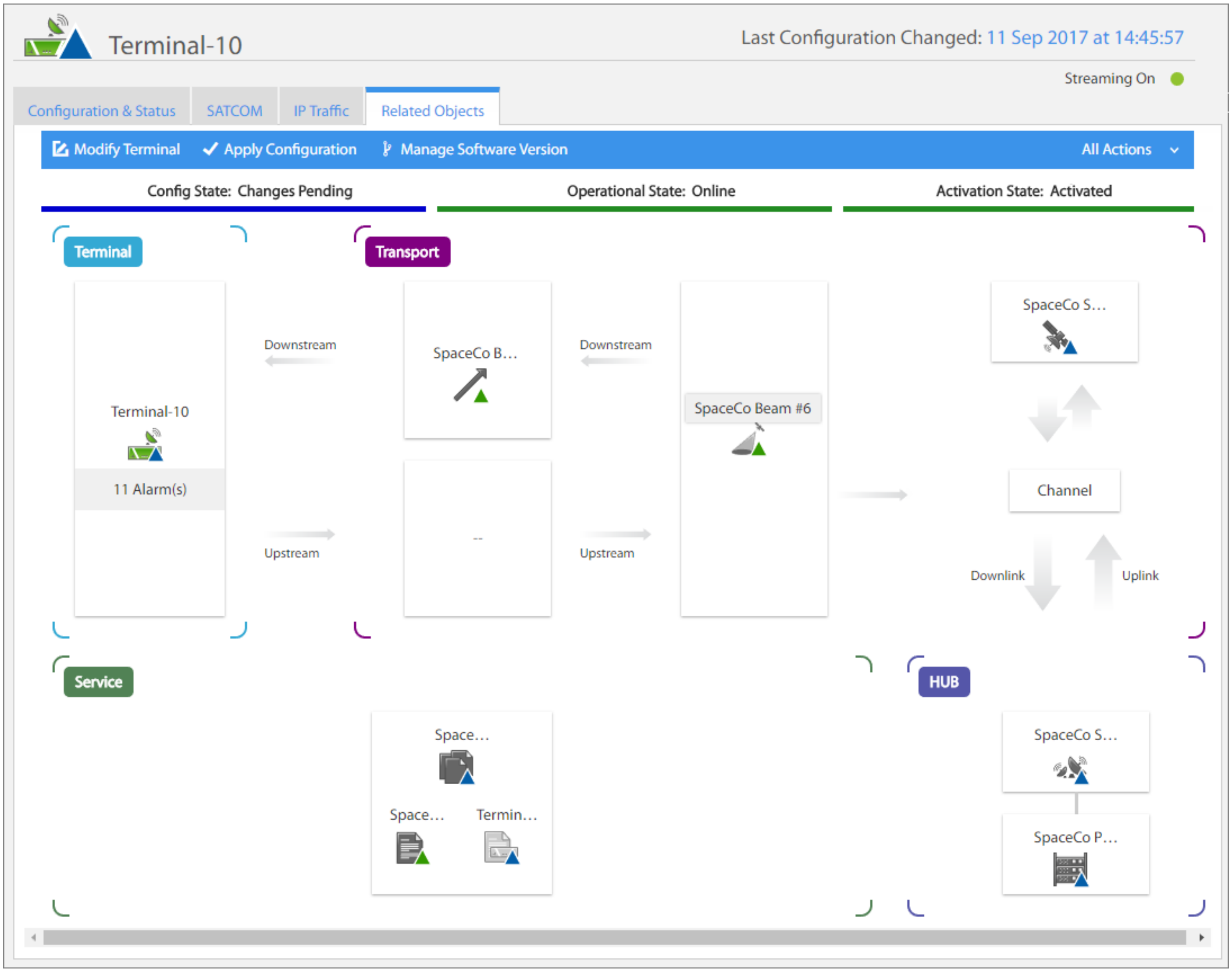


Figure 14-7. KIP Rel;ated Objects tab for a Terminal

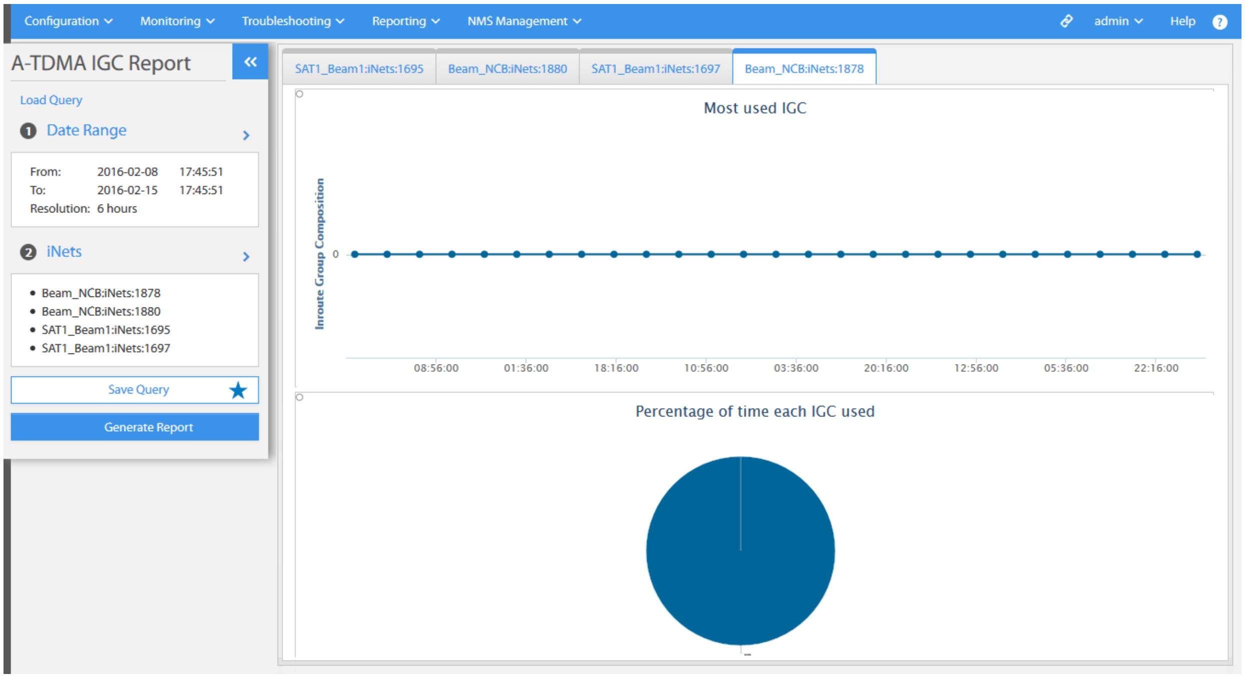
14.2 Generating an A-TDMA IGC Report

An IGC selection algorithm executes periodically, in the protocol processor, to determine the best suited IGC for an inroute group given current network conditions. Each execution of the algorithm results in a new *figure of merit (FOM)* factor for each IGC. These FOMs are relative values used to compare the IGCs. An IGC with a higher FOM is better suited for current network conditions than an IGC with a lower FOM. On each execution pass of the selection algorithm, the IGC with the highest FOM is chosen as the next IGC.

The A-TDMA IGC (*Inroute Group Composition)* Report generates a report on the actual usage of the configured IGCs assigned to an Inroute Group Profile.

By examining the report, users can see the IGC usage over time, as a percentage for each IGC. The most active IGC can be identified, as well any discrepancies between actual and expected usage of the IGCs configured in an inroute group. The report includes the following panes per IGC, which can be selected by the labeled iNet tab:

- A time line showing the Most Used IGC selections over the specified period
- A pie chart of the percentage of in-use time of each IGC over the specified period



From: 2016-02-08 17:45:51
To: 2016-02-15 17:45:51
Resolution: 6 hours

- Beam_NCB:iNets:1878
- Beam_NCB:iNets:1880
- SAT1_Beam1:iNets:1695
- SAT1_Beam1:iNets:1697

Figure 14-8. A-TDMA IGC Usage Report

To generate the ATDMA IGC usage report:

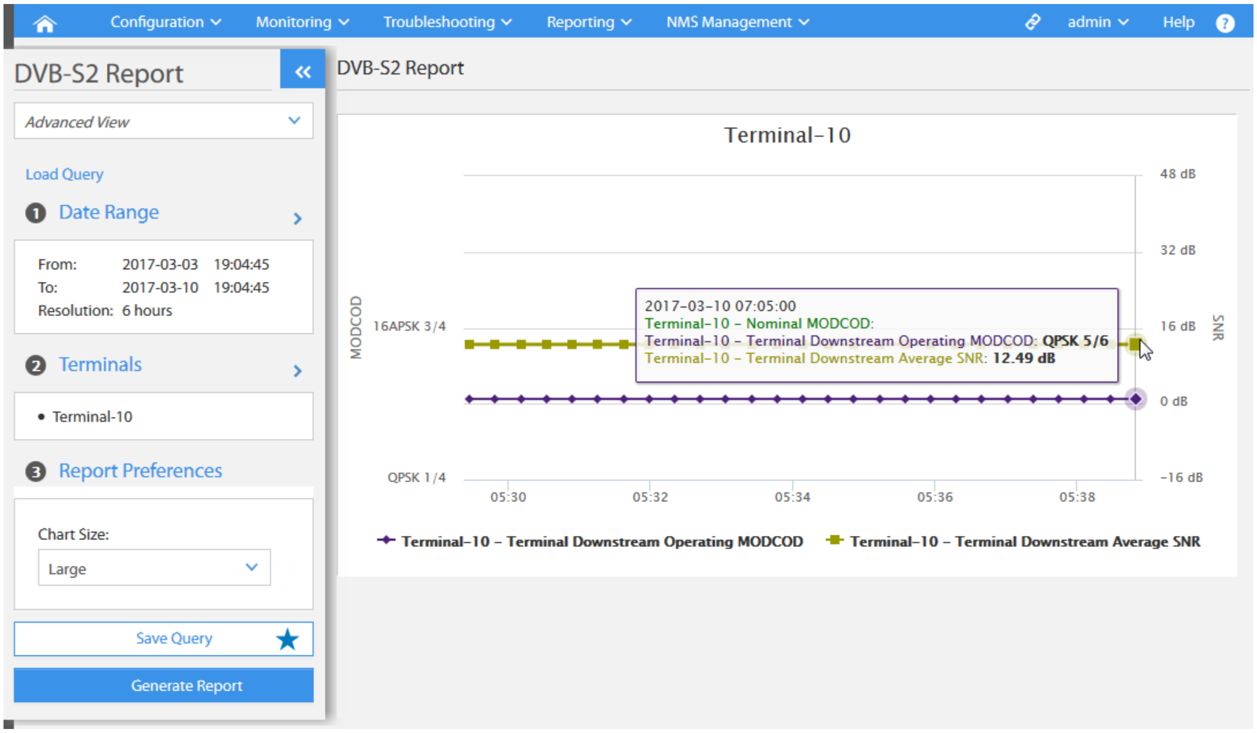
1. Click the **Reporting** tab, and under **Pre-Defined Reports**, select **A-TDMA IGC**. The Configurator opens to the **A-TDMA IGC Report** Configurator dialog.
2. If applicable, click **Load Query** to load a previously saved set of Configurator parameters for an **A-TDMA IGC Report**.

3. Click the **Date Range** bar, to open the **Date Range** dialog and enter a period or specify one of the pre-defined periods for which the report should be generated.
4. Click the **iNets** bar, to open the **Basic Search** window to specify one or more iNets to be included in the report; and click **Done** to select the iNets and return to the Configurator.
5. If applicable, click **Save Query** to save the **A-TDMA IGC Report** configuration as a query.
6. Click **Generate Report** to initiate generation of the A-TDMA IGC report.

14.3 Generating a DVB-S2 Report

During normal operation, each remote terminal regularly sends its SNR to the protocol processor (PP), and based on this SNR, the PP adjusts the MODCOD that it uses to transmit to the remote. The DVB-S2 report, which is manually configured using the Configurator, displays a correlation between the MODCODs used by a terminal on the Downstream carrier, to the Downstream Average SNR for each of the MODCODs.

This report can be used to identify the average SNR for each MODCOD, on which a terminal operates on the downstream DVB-S2 carrier.



Advanced View

From: 2017-03-03 19:04:45
To: 2017-03-10 19:04:45
Resolution: 6 hours

- Terminal-10

Chart Size: Large

2017-03-10 07:05:00
Terminal-10 – Nominal MODCOD:
Terminal-10 – Terminal Downstream Operating MODCOD: **QPSK 5/6**
Terminal-10 – Terminal Downstream Average SNR: **12.49 dB**

Figure 14-9. DVB-S2 Report

To generate the DVB-S2 report:

1. Click the **Reporting** tab > **Pre-Defined Reports > DVB-S2**.
2. Select the **Advanced View** option to enable the **Report Preferences** section.
3. If applicable, click **Load Query** to load a saved set of Configurator parameters.
4. Click the **Date Range** bar, to open the **Date Range** dialog and enter a period or specify any one of the pre-defined periods for which the report should be generated.
5. Click the **Terminals** bar, to open the Basic Search tool to select one or more terminals to be included in the report. Click **Done** to select the terminals and close the dialog.
6. Click the **Report Preferences** bar, and choose the Chart Size to use in the report.
7. Click **Generate Report** to initiate generation of the DVB-S2 report.

15 Troubleshooting Operations

Pulse Troubleshooting operations include a variety of tools that support detailed investigation of network issues. Diagnostic probes are available for troubleshooting infrastructure elements — including line cards, clusters, and terminals. Probes are also available for diagnosing problems with group service plan and subscriber service plan components.

Pulse Troubleshooting operations are covered in the following topics.

15.1 About Pulse Troubleshooting

Pulse NMS troubleshooting operations, which are accessed from the **Troubleshooting** tab, include the following operations categories:

- Probe Commands
- Engineering Debug Console

The *probe commands* support real-time interaction with the operating system of iDirect Satellite Terminal, Line Card, and Cluster infrastructure elements; as well as with service elements including Group Service Plans (GSPs), and Subscriber Service Plan Components (SSPCs). Each of these network elements support a set of commands that allow users with permission to access and manipulate specific operations.

Probe operations use the Pulse Configurator panel. When setting the configurator parameters, the **Command** section of the dialog changes to reflect the selected element type. Each executed command provides feedback to indicate whether the operation was completed.

The *engineering debug console* operations, which also use the Pulse Configurator panel, supports direct access to a selected terminal, line card, or cluster server, using a shell window for debugging purposes.

15.2 Terminal Probe Commands

From the **Probe Commands** Configurator tool, terminal probe commands can be issued to perform specific tests, or to affect a specific behavior or operation of a selected terminal.

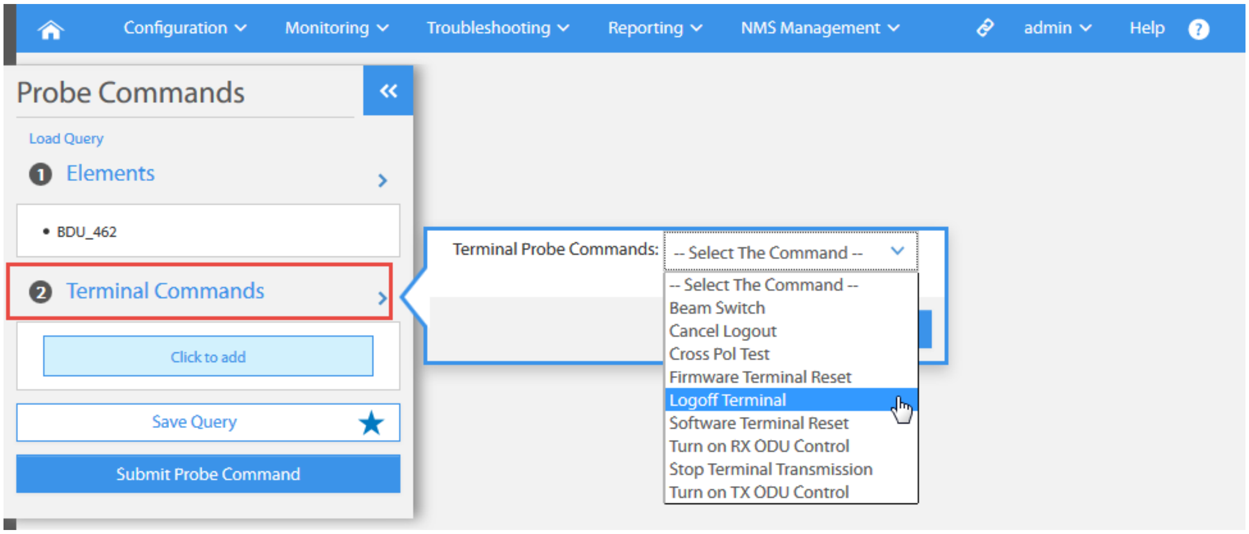


Figure 15-1. Probe Command Configurator - Terminal Commands

To issue terminal probe commands using the Configurator:

1. Click the **Troubleshooting** tab > **Probe Commands**.
2. Click **Load Query**, if applicable, to load a saved set of Configurator parameters.

3. Click **Elements** to open the Basic Search tool.
4. Click the **Element Type** drop-down and select **Terminal** to list terminals found in NMS.
5. If necessary, use the **Operational** or **Config/Update** filter to narrow the list of terminals.
6. Select one or more terminals to which a probe command will be applied.
7. Click the **Terminal Commands** bar; use the **Terminal Probe Commands** drop-down list to select a command to issue; and click **Done** to add the command to the Configurator.
8. Depending on the command, a **Command Fields** section is displayed with one or more parameters that can be specified. Specify the parameters to be applied to the command.
9. Click **Submit Probe Command**, to issue the command on the selected terminals.

Table 15-1. Terminal Probe Commands

Probe Command	Brief Description
Beam Switch	Issue command to the terminal, to switch beams based on the specified **IF Domain** and **iNet ID**.
Logoff Terminal	Issue command to the terminal to logoff for a specified duration (0-3600 sec.)
Cancel Logoff	Cancel previously issued “logoff terminal” command.
Stop Terminal Transmission	Initiate command to terminal to stop transmitting (Mute Tx).
Turn On Tx ODU Control	Turn Tx ODU control (DC power) ON to BUC.
Turn On Rx ODU Control	Turn Rx ODU control (DC power) ON to LNB.
Software Terminal Reset	Initiate a terminal reset at the iDirect application level.
Firmware Terminal Reset	Initiate a terminal reset at the terminal firmware level.
Cross Pol Test	Supports user in performing the cross-polarization test. Allows transmission of a modulated or un-modulated CW as part of the test.

NOTE: See Terminal Probe command field descriptions in the following table.

Table 15-2. Terminal Probe Command - Command Field Descriptions

Probe Command	Command Field	Brief Description (Valid Values)
Beam Switch	IF Domain	IF Domain for terminal beam switch.
	iNet	iNet to which terminal should switch. Terminal may switch back immediately based on current network conditions.
Logoff Terminal	Logoff	Specify a terminal logoff duration (0-3600 seconds).
CrosPol Test (This command set tells the terminal to start transmitting a CW tone or PN signal at the specified power and frequency)	Frequency at RF	Specify the RF frequency at which the terminal should transmit for test. The value must be in the valid range supported by terminal.
	Data Source	B_PN = BPSK PN sequence; 8_PN = 8PSK PN sequence; Q_PN = QPSK PN sequence; CW= CW Tone; CANCEL = cancel.
	Power Level	Power for test signal at the L-band output, in units of 0.1 dbm. For example, -100 = -10 dbm.
	Symbol Rate	Symbol rate of modulated carrier, in Ksym/s. This message is ignored if the rate is below that which is supported by the terminals.
Stop Terminal Transmission	Stop Tx	Select/unselect to mute/unmute the terminal transmitter.
Turn On Tx ODU Control	Request Params	Choose ODU DC power or reference; 10 MHz, 50 MHz, DC Power, None
	Enable	Select/unselect **Enable** to enable/disable Tx ODU DC power or reference to BUC.
Turn On Rx ODU Control	Request Params	10 MHz, 50 MHz, DC Power, or None
	Enable	Select/unselect **Enable** to enable/disable Rx ODU DC power or reference to LNB.

15.3 Line Card Probe Commands

From the Probe Commands Configurator tool, users are able to issue commands to either perform specific tests, or to affect a specific behavior or operation of a network line card.

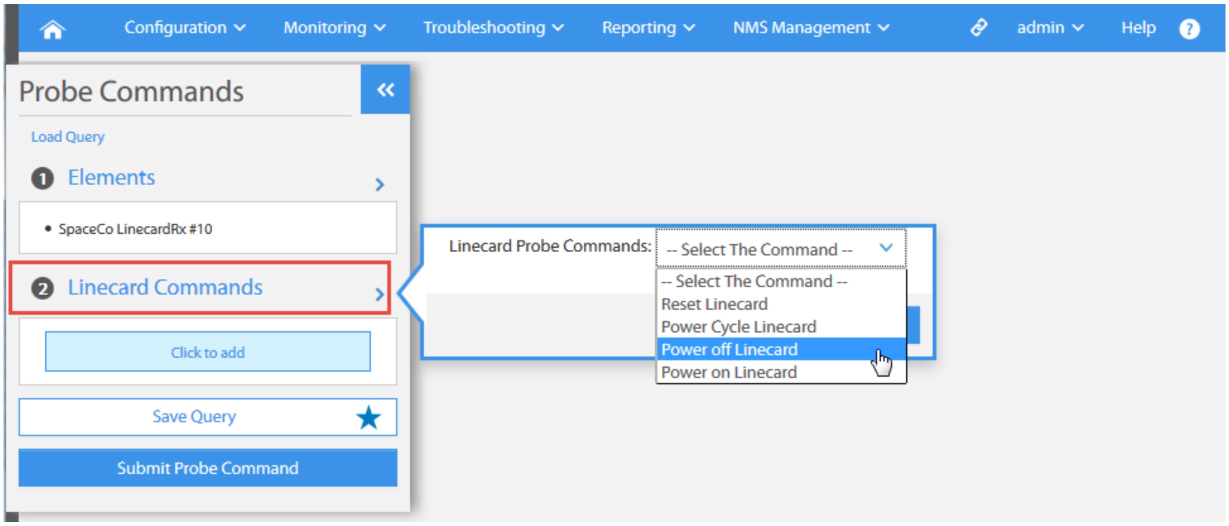


Figure 15-2. Probe Command Configurator - Line Card Commands

To issue line card probe commands using the Configurator:

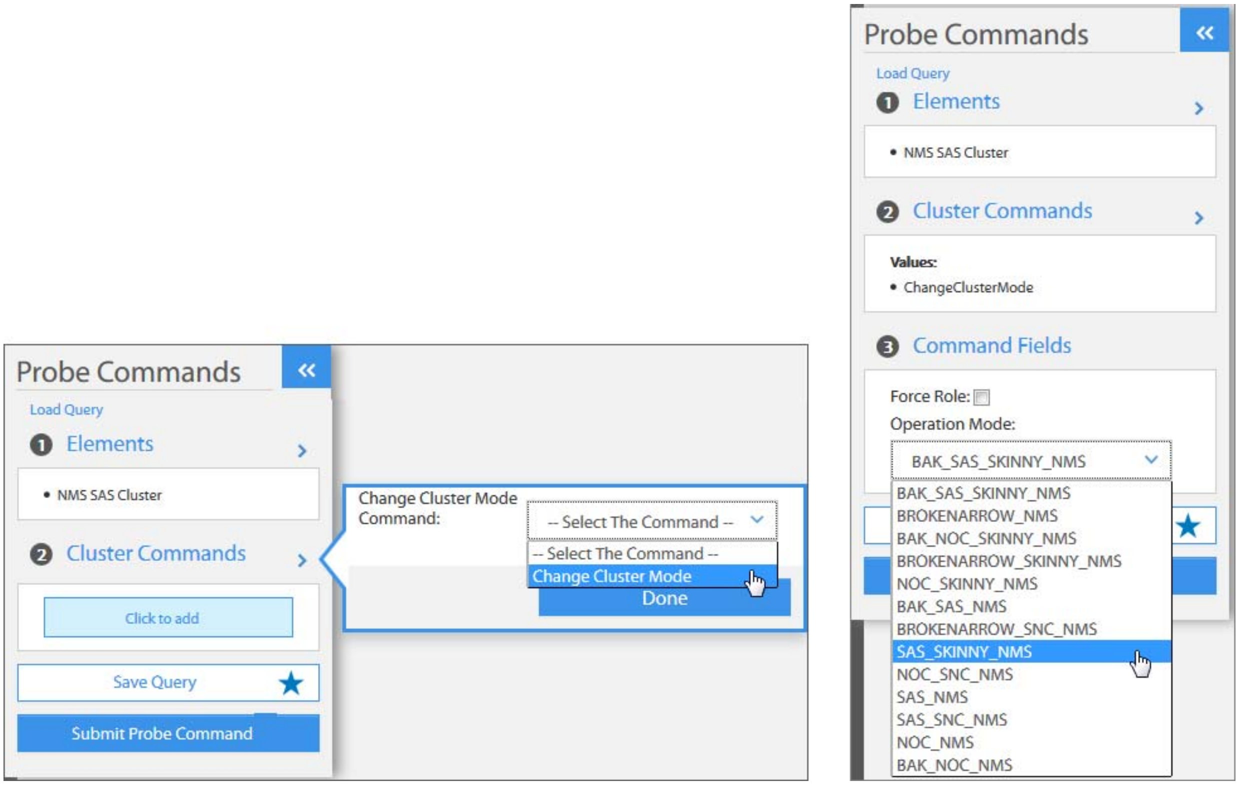
1. Click the **Troubleshooting** tab > **Probe Commands**.
2. Click **Load Query**, if applicable, to load a saved set of Configurator parameters.
3. Click **Elements** to open the Basic Search tool.
4. Click the **Element Type** drop-down list and select **Line Card** to list the line cards found in the NMS. Both transmit and receive line cards are listed.
5. If required, use the **Operational** or **Config/Update** filters to narrow the list of line cards.
6. Select one or more line cards to which a command will be applied and click **Done**.
7. Click the **Linecard Commands** bar; use the **Linecard Probe Commands** drop-down list to select a command to issue; and click **Done** to add the command to the Configurator.
8. With the selected command shown in the **Linecard Commands** section, click **Submit Probe Command**, to issue the command on the selected line cards.

Table 15-3. Line Card Probe Commands

Probe Command	Brief Description
Reset Line Card	Initiate software reset at the iDirect application level of the selected line card(s).
Power Cycle Line Card	Initiate command to chassis manager to cycle power for the selected line card (s).
Power On Line Card	Initiate command to chassis manager to apply power to slot of a selected linecard.
Power Off Line Card	Initiate command to chassis manager to remove power to slot of a selected linecard.

15.4 Cluster Probe Commands

From the Probe Commands Configurator tool, users are able to issue commands to change the mode of a selected cluster. The probe commands may be applied to affect the mode of an NMS Cluster, located at any primary/backup SAS or NOC Site.



Change Cluster Mode Command: -- Select The Command --

Force Role: ☐

Operation Mode: BAK_SAS_SKINNY_NMS

Figure 15-3. Probe Command Configurator - Cluster Commands

To issue cluster probe commands using the Configurator:

1. Click the **Troubleshooting** tab > **Probe Commands**.
2. Click **Load Query**, if applicable, to load a saved set of Configurator parameters.
3. Click **Elements** to open the Basic Search tool.
4. Click the **Element Type** drop-down list and select **NMS Cluster** or **Protocol Processor Cluster** to display a list of configured NMS or PP clusters.
5. Select a cluster to which a command will be applied, and click **Done**.
6. Click the **Cluster Commands** > **Change Cluster Mode Command** > select **Change Cluster Mode >** click **Done**.
7. The **Command Fields** section displays a set of parameters appropriate to the selected command. Specify the parameters to be applied to the selected Cluster command. The **Force Role** option is only required where there is no backup cluster available and it is necessary to move the current selected cluster into primary mode.

8. Under **Command Fields**, select **Force Role** to enable the command, and use the **Operation Mode** drop-down list to select the operational mode to which the cluster should be switched.
9. Click **Submit Probe Command**, to issue the command on the selected Cluster.

Table 15-4. Cluster Probe Command Operational Mode Options

Operational Modes	Brief Description
Change Cluster Mode to:	
• BAK_SAS_SKINNY_NMS	5-node SAS NMS Cluster - No Slave nodes for Regular and Fat Master Nodes
• BROKENARROW_NMS	7-node SAS NMS Cluster temporarily resumes the authoritative role of NOC NMS Cluster (during NOC to SAS connection failure)
• BAK_NOC_SKINNY_NMS	5-node Backup NOC NMS Cluster - No Slave nodes for Regular and Fat Master Nodes
• BROKENARROW_SKINNY_NMS	5-node SAS NMS Cluster resumes the authoritative role of NOC NMS Cluster (during NOC to SAS connection failure)
• NOC_SKINNY_NMS	5-node NOC NMS Cluster - No Slave nodes for Regular and Fat Master Nodes
• BAK_SAS_NMS	7-node complete operational Backup SAS NMS Cluster
• BROKENARROW_SNC_NMS	Single node NMS Cluster temporarily resumes the authoritative role of NOC NMS Cluster (during connection failure to NOC)
• SAS_SKINNY_NMS	5-node SAS NMS Cluster - No Slave nodes for Regular and Fat Master Nodes
• NOC_SNC_NMS	Single Node NOC NMS Cluster
• SAS_NMS	Node complete operational Primary SAS NMS Cluster
• SAS_SNC_NMS	Single-node SAS NMS Cluster
• NOC_NMS	7-node complete operational NOC NMS Cluster
• BAK_NOC-NMS	7-node complete operational Backup NOC NMS Cluster

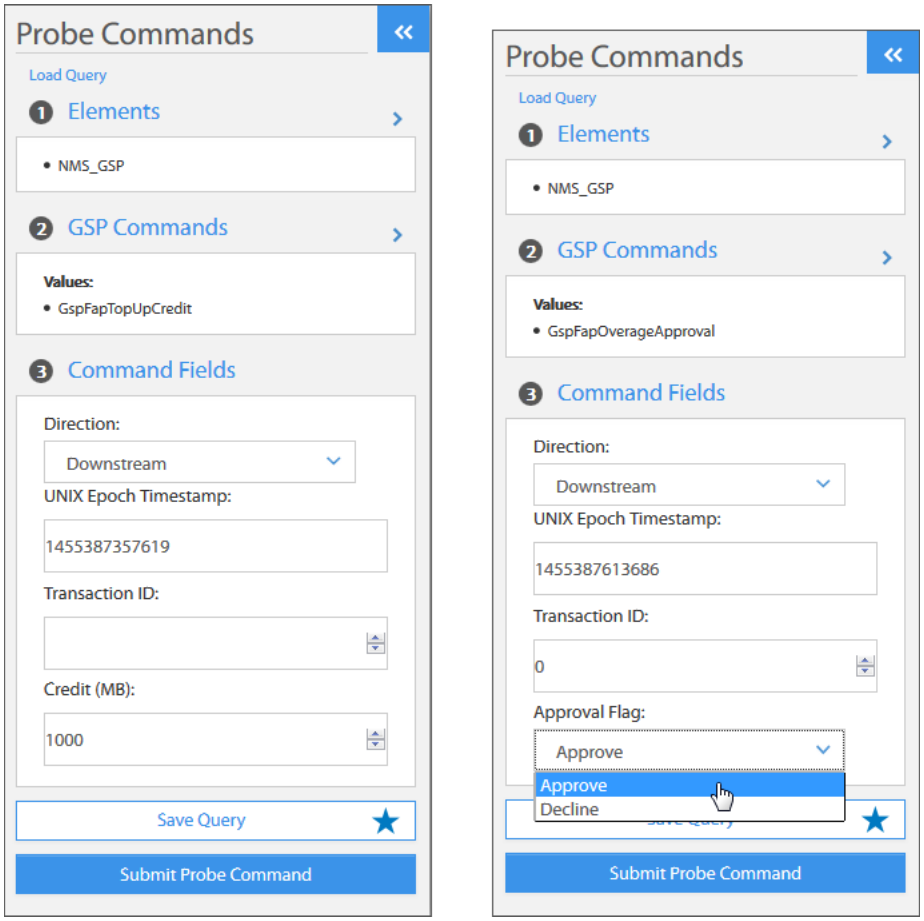
NOTE: When gaps in communication between the SAS NMS and the primary NOC NMS occur, the SAS NMS enters Broken Arrow mode. In Broken Arrow mode, the SAS allows local users to access the SAS NMS to view data, including stats and configuration data.

Although the regular communication may be temporarily interrupted, once communication is re-established, the NMS resumes SAS-to-NOC communication. See the *Velocity Technical Reference Guide*, for additional details on broken-arrow mode.

15.5 Group Service Plan (GSP) Probe Commands

GSP probe commands can be issued to issue a top-up credit, or to approve or decline a FAP overage allowance request. These probe commands may be applied specifically to the upstream or downstream, and performed for both GSP (Group Service Plan) and SSPC (Subscriber Service Plan Component) elements.

The SSPC Probe Command procedure is identical to the GSP Probe Command procedure.



Elements: NMS_GSP

Values: GspFapTopUpCredit

Direction: Downstream

UNIX Epoch Timestamp: 1455387357619

Transaction ID:

Credit (MB): 1000

Elements: NMS_GSP

Values: GspFapOverageApproval

Direction: Downstream

UNIX Epoch Timestamp: 1455387613686

Transaction ID: 0

Approval Flag: Approve

Figure 15-4. GSP Probe Command- FAP Top Up Credit and FAP Overage Approval

To issue group service plan probe commands using the Configurator:

1. Click the **Troubleshooting** tab > **Probe Commands**.
2. Click **Load Query**, if applicable, to access a saved set of Configurator parameters.
3. Click **Elements** to open the Basic Search tool.
4. Click the **Element Type** drop-down list and select **Group Service Plan** to display a list of configured GSPs.
5. Select one or more GSP elements from the list, and click **Done** to add the element to the Configurator.

6. Click the **GSP Commands** bar > **Probe Commands** drop-down list > **GSP FAP Top Up** or **GSP FAP Overage Approval**; click **Done** to add the command to the Configurator.
7. Depending on the selected command, a **Command Fields** section is displayed with one or more parameters that can be specified.
8. Specify the parameters to be applied to the selected GSP or SSPC command.
9. Click **Submit Probe Command**, to issue the command.

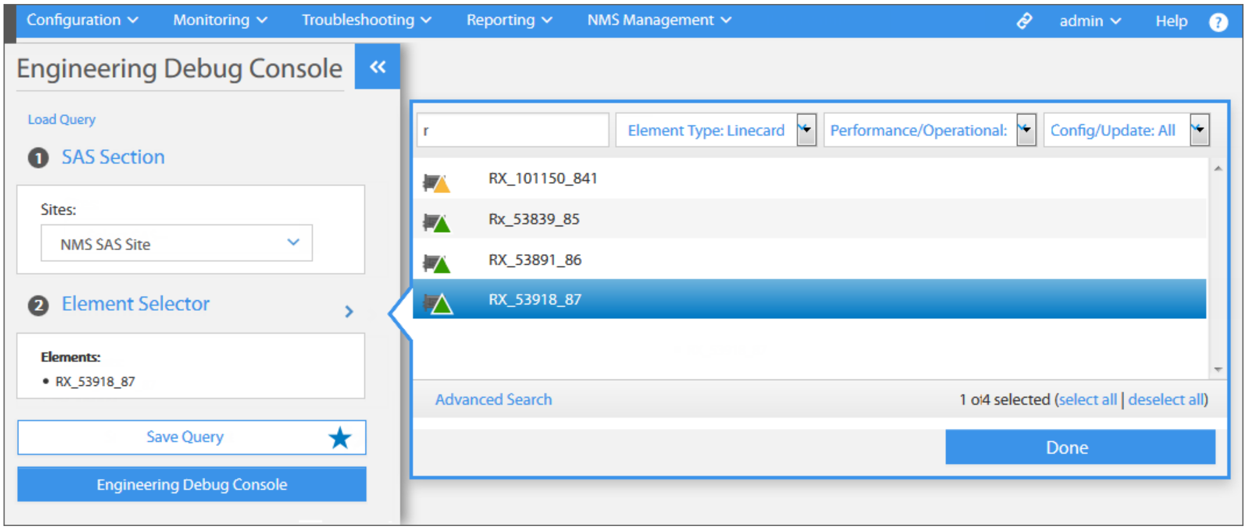
Table 15-5. GSP/SSPC Probe Commands FAP Top Up and FAP Overage Approval

Probe Commands	Brief Description
GSP FAP Top-Up of SSPC FAP Top-Up	FAP top-up is the process of adding to the current allowance balance, a top-up credit allowance, specified in MBytes. This is a one-time allowance that may be purchased separately at any time. It is typically purchased to avoid service interruption when the periodic volume allowance is depleted. If this command is selected, a FAP Top-up **Credit** can be specified, in MBytes, for the **Upstream** or **Downstream** Allowance.
GSP FAP Overage Approval or SSPC FAP Overage Approval	Overage charges are per MB charges that are applied when the volume allowance is exceeded during the allowance period. Unless pre-approved, the defined volume allowance, if exceeded, will result in the overage charge. If this command is selected, users may individually **Approve** or **Decline** the **Upstream** or **Downstream** overage allowance.
GSP/SSPP Probe Command Fields	**Brief Description**
Direction	Indicates the Upstream or Downstream direction
Credit	Credit amount in Mbytes (negative values supported)
Transaction ID	Unique value to each credit amount added to top-up/ or each overage approval
Approval/Decline	Indicates whether overage was approved/declined

15.6 Engineering Debug Console

The *engineering debug console* provides direct access to a selected element, using a shell window for debugging purposes. Access to this debug console is via the Configurator tool.

Network infrastructure elements accessible using this tool include line cards, terminals, NMS and PP servers, and the chassis controller.



Sites: NMS SAS Site

Elements:
- RX_53918_87

r

Element Type: Linecard

Performance/Operational:

Config/Update: All

RX_101150_841
Rx_53839_85
RX_53891_86
RX_53918_87

1 o 4 selected (select all | deselect all)

Figure 15-5. Engineering Debug Console

To use the engineering debug console:

1. Click the **Troubleshooting** tab > **Engineering Debug Console.** The **Engineering Debug Console** dialog is opened.
2. Click **Load Query**, if applicable, to access a saved set of Configurator parameters.
3. Under the **SAS Section**, use the **Sites** drop-down list to select the appropriate site.
4. Click **Element Selector** to open the Basic Search tool.
5. Use the **Element Type** filter to limit the list to Terminals, Line Cards, NMS Servers or PP Servers.
6. Find and select a specific Terminal, Line Card, or Cluster Server element to which a debug command will be issued.
7. Click **Done** to add a selected element to the Configurator tool.
8. If applicable, click **Save Query**, to save the configuration for future use.
9. Click **Engineering Debug Console**, to open a shell command session directly with the selected element.

Glossary

2D 16-State	A type of Forward Error Correction coding, available on inbound carriers, in DVB-S2 networks. Provides link margins, improved IP throughput and faster acquisition when compared to Turbo Product Coding.
Access Class Value	On the channel side, a bit mask value that is logically combined, using the AND operation, with the terminal access class value when the terminal attempts to join the channel. If the logical result is non-zero, the terminal is allowed into the sub-channel — otherwise it is not.
Adaptive Coding and Modulation (ACM) *Gain*	The increase in performance achieved on a DVB-S2 outbound carrier when the MODCOD used to transmit data is higher than the minimum MODCOD configured for the carrier.
Acquisition	The process whereby the satellite router synchronizes its bursts with the upstream TDMA frame timing and joins the network.
Acquisition Signaling Carrier (ASC)	Used to broadcast the current satellite beam configuration information to the terminals within a network.
Action Plan	A list of update commands to be applied by the update manager, against a configuration item.
Active Configuration	The element configuration that is resident on the network element.
Activity Log	An NMS record of date/time and details of each activity, whether performed by a human or machine user.
Adaptive Coding and Modulation (ACM)	A method of applying coding to a data stream in DVB-S2 networks in which every BBFrame can be transmitted on a different MODCOD.

Adaptive Coding and Modulation (ACM) Gain	The increase in performance achieved on a DVB-S2 outbound carrier when the Modulation and Coding (MODCOD) used to transmit data is higher than the minimum Modulation and Coding (MODCOD) configured for the carrier.
Admin SVN	The iDirect administrative data VLAN.
Alarm	A condition that is important enough to bring to the attention of an operator, and generally needs some corrective action or further investigation.
Allocation Fairness Relative to **Committed Information Rate (CIR)**	1) When enabled causes bandwidth to be allocated in proportion to the configured CIR of the Group QoS node or virtual remote. 2) When not enabled, bandwidth is allocated equally to competing nodes until available bandwidth is exhausted. A Group QoS (GQoS) configuration option.
Allocation Fairness Relative to **Modulation and Coding (MODCOD)**	Applies only to DVB-S2 outbound carriers using Adaptive Coding and Modulation (ACM), also for this option, bandwidth allocation is based on information rate (Mb) rather than the whole spectrum satellite bandwidth (MHz). A Group QoS (GQoS) configuration option. *NOTE: This favors remotes at lower MODCODs as bandwidth allocations must increase to achieve the same information rate as remotes at higher MODCODs.*
Alternate **Downstream Carrier**	Allows a second downstream carrier definition to be associated with a network in order to facilitate moving the network to a new downstream carrier.
Antenna Control Unit	A control device that monitors and controls the position of a Very Small Aperture Terminal (VSAT) antenna.
Application	An Application defines a specific type of service (such as Voice over IP or TCP) as defined in a Service Group. An Application is created from an Application Profile. An instance of an Application running on a remote is called a Virtual Remote. A Group QoS (GQoS) feature.
Application-Based GQoS	Visible and configurable GQoS parameters, per Service Level.
Automatic Beam Selection (ABS)	Allows roaming remotes to select which network to join and automatically lock on to the associated outbound carrier. Also known as Automatic Beam Switching.
Available Tokens	The number of tokens still open for use by a user group or other associated element.

Backup Site	The backup (or secondary) operational site of any one of the Velocity network site pairs, to which operations can be switched if a failure occurs at the primary site. Each site and its optional backup/diversity site can operate as the primary or backup (secondary) site.
Bandwidth Group	A Bandwidth Pool contains one or more Bandwidth Groups. Each Bandwidth Group contains one or more service groups. An intermediary Group QoS (GQoS) node.
Bandwidth Pool	Either a Network (in which case the network defines the QoS properties of the Downstream Carrier) or an Inroute Group (in which case the network defines the QoS properties of the Upstream Carrier). The root (or top-level node) of a Group QoS (GQoS) tree.
Beam	The physical footprint from a satellite antenna onto the ground.
Binary Large Object File (BLOB)	A collection of binary data files stored as a single entity.
Blade	An alternate name for a Protocol Processor server machine.
Block Up Converter (BUC)	A device used in the transmission of Very Small Aperture Terminal (VSAT) uplink signals.
Board Support Package (BSP)	Also known as Cumulative Update Package. Support package downloaded to remotes before loading remote image files.
Border Gateway Protocol (BGP)	A standardized exterior gateway protocol designed to exchange routing and reachability information among autonomous systems (AS) on the Internet. BGP is often classified as a path vector protocol but is sometimes classed as a distance-vector routing protocol. BGP makes routing decisions based on paths, network policies, or rule-sets configured by a network administrator and is involved in making core routing decisions.
Border Gateway Protocol (BGP) *Peer Group*	A group composed of member BGP peers that share common update policies, in order to simplify routing configuration and management.
Border Gateway Protocol (BGP) *Peers*	Two or more routers that maintain a TCP connection, through BGP, for the purpose of exchanging BGP route table information.

Border Gateway Protocol (BGP) *IP Prefix List*	A filter list, which may be applied to a specific route map.
Bose-Chaudhuri-Hocquenghem (BCH)	In coding theory, the BCH codes form a class of cyclic error-correcting codes that are constructed using finite fields. BCH codes were invented in 1959 by French mathematician Alexis Hocquenghem, and independently in 1960 by Raj Bose and D. K. Ray-Chaudhuri.
Burst Time Plan (BTP)	Slot allocation message sent to remote modems to indicate when each remote can transmit on the TDMA upstream carriers.
Carrier	A single modulated RF signal carrying information.
Certificate	A certificate, created by the CA Foundry, is required by all in Network elements in the Public Key Infrastructure (PKI) Data File system, in order to communicate with one another.
Certificate Authority (CA)	An authority in a network that issues and manages security credentials and public keys for message encryption.
Certificate Authority (CA) *Foundry Service*	The Certificate Authority (CA) utility that issues the X.509 public key certificates that allow “hosts” to join a TRANSEC network.
Channel	A fixed section of bandwidth on the feeder link mapped to beam. Channels are bidirectional, with equal inbound and outbound bandwidths; in Velocity, a channel is also dynamically mapped onto a beam.
Chassis Group	A group of chassis physically linked, allowing a single network to span multiple chassis.
Chassis License	A license, purchased from iDirect, required to activate slots in a chassis.
Classification Rules	Rules and actions that determine how packets are filtered and prioritized.
Committed Information Rate (CIR)	Provides a node with guaranteed network bandwidth availability and specifies bandwidth allocation to a node before additional (non-CIR) bandwidth is allocated to that node for traffic with the same priority. A Group QoS (GQoS) feature.

Comms-on-the-MOVE (COTM)	A fully integrated communication system based on the L3 high-performance, multiband random antenna system. A mobile remote feature.
Compare Configuration	A Pulse operation that supports side-by-side viewing of the active and pending options file of an element; also view manifest and configuration inventory.
Configuration Inventory	A list of software items that are currently installed on the element.
Configuration Rollback	The process of undoing previously made additions, deletions, or modifications to the configuration of an element.
Configurator Panel	A Pulse tool that assists operators with the tasks of generating real-time and historical reports of network elements.
Constant Coding and Modulation (CCM)	A method of applying coding in a DVB-S2 data stream in which every BBFrame is transmitted at the same Modulation and Coding (MODCOD) rate.
Cumulative Update Package	See Board Support Package (BSP).
Custom Key	A method by which the functionality of a specific network feature or element is added or modified without adding fields to or modifying the NMS GUI. Also referred to as the “Engineering Debug Key,” is also an options file parameter configured in the NMS. Custom keys allow options to be configured on a remote or network that are not available on the GUI.
Customer	An NMS data record of an individual or business entity, which is not necessarily an NMS user. The record contains contact information, including name, phone number, and an e-mail address.
Customer SVN	A Global SVN that connects customer equipment, located in the terminal network, behind a terminal, through the SAS and across the DCN to a customer network. Also called Data SVN.
Daisy Chain	See Chassis Group.
Dedicated **Acquisition Signaling Carrier (ASC)**	A DVB-S2 signaling carrier in which the hub broadcasts current satellite network configuration information, to terminals, on a single uplink and a single downlink.

Dedicated **Acquisition Signaling Carrier (ASC)** *with fan-out*	A single DVB-S2 signaling carrier, in network, by which the hub broadcasts the current satellite configuration, on a single up-link that is replicated on multiple downlinks in different beams.
Default Value	A value that is preset for various NMS element configuration pages, data fields, check boxes, and drop-down selections.
Derived ID (DID)	The unique identifier of a remote satellite router derived from the model type and serial number.
Deterministic TDMA (DTDMA)	A technique used to prevent collisions of remotes transmitting simultaneously in which synchronized burst time plan provides the network timing.
Digital Video Broadcasting - Satellite - Second Generation (DVB-S2)	A set of open standards for satellite digital broadcasting. DVB-S2 is an extension to the widely-used DVB-S standard and was introduced in March 2005.
Download Certificate	An action that results in the actual transfer of a certificate from the NMS element to a local PC or laptop device.
Downstream Carrier	1) The satellite carrier transmitted from the hub to the remote satellite router. 2) A DVB-S2 carrier from the SAS to a satellite terminal. Same as Outbound Carrier or Outroute.
Dynamic Configuration	The terminal configuration information that is passed over the RF interface from the SAS to the remote, using an over-the-air dynamic configuration exchange protocol.
Dynamic Features and Options Exchange (DFOE)	A protocol used by the NMS to allow some remote-side configuration changes to be dynamically applied. Hub-side options groups beginning with 'RMT_' are sent from the Protocol Processor to the remote using the DFOE protocol.
Dynamic Multicast Stream	Velocity multicast option: When enabled, terminal software accepts dynamic configuration of static streams and configures IGMPv3 or MLD on a per terminal, per SVN basis. Dynamic multicast is the default option on all SVNs, but can be disabled.
EDAS Controller Board	Type of controller board used with older Chassis. See also MIDAS Controller Board.

Eight-Port Switch	Configurable LAN switch available on some remote satellite router model types.
Element Domains	A hierarchical object model in Pulse, in which configurable network elements are grouped into logically related collections called Element Domains.
Engineering Debug Console	A Pulse tool that provides direct access to a selected network infrastructure element, using a shell window for debugging purposes.
Enhanced Information Rate (EIR)	Allows system configuration to maintain Committed Information Rate (CIR) or Maximum Information Rate (MIR) during rain fade; for the physical remote (Remote-Based Group QoS (GQoS)) or critical applications (Application-Based Group QoS). Option only applies to networks that use DVB-S2 with Adaptive Coding and Modulation (ACM). A Group QoS (GQoS) feature.
External Access Portal (EAP)	An external instantiation of the Pulse NMS that provides limited access to NMS configuration, statistics, and reporting functionality for any users external to the Satellite Operator. The EAP also supports configuration capabilities that allow an EAP user with appropriate permissions to create, modify, and delete network elements.
Fast Fade Margin	For Digital Video Broadcasting - Satellite - Second Generation (DVB-S2) outbound carriers, the additional margin added to the SNR thresholds measured at hardware qualification to arrive at the operational threshold during a “fast fade” condition.
Feature License	A license purchased from iDirect allowing NMS operators to configure a license-controlled feature.
Filter Profile	A traffic profile configurable in the NMS and assigned to remotes to filter out unwanted packets.
Free Slots	Slots left in the dynamic sub-frame after all stream, guaranteed (Committed Information Rate (CIR) and preemptive bandwidth requests are satisfied.
Frequency Hopping	The ability of remotes to switch between Time Division Multiple Access (TDMA) carriers within an Inroute Group when transmitting to the hub.
Full-Trigger CIR	Committed Information Rate (CIR) that is always fully-allocated, even if demand is less than the configured Committed Information Rate (CIR).
Geographic Region	A geographic region that defined as a combination of satellites/beams, and/or service areas that constitutes an area of coverage.

Global SVN	A high level synthetic virtual network structure that represents an extensive virtual private network across the core network (the data communications network) to another Site.
Group QoS (GQoS)	1) An iDirect Quality of Service (QoS) solution based on a hierarchical tree structure (Group QoS is built on a 'Group QoS tree') by which bandwidth allocation flows downward through the 'tree' from the 'root' node to the 'leaf' nodes. GQoS allows high flexibility; creation of subnetworks, and groups of remotes, with various levels of service tailored to the characteristics of supported user applications. 2) Alternate description - hierarchical construct within which containership and inheritance rules allow the iterative application of basic allocation methods across groups and subgroups. QoS properties configured at each level of the Group QoS tree determine how bandwidth is distributed when demand exceeds availability.
Group Service Plan (GSP)	A plan of service that represents an acquisition of satellite bandwidth capacity on the Velocity Network. *Note: May be defined by the Network Service Provider*.
Header Compression	A network optimization option that enables the compression of the IP header of each data packet prior to transmission. Two types of header compression are supported in Velocity — RTP header compression (used for RTP packets) and TCP header compression (used for TCP packets).
Hub Line Card (HLC)	A modem deployed at the hub to transmit and/or receive outroutes and inroutes.
Hub Network Operator (HNO)	An NMS operator with privilege to act as an administrator to Virtual Network Operators. An HNO can configure VNO users and networks and set VNO permissions such as visibility and read/write access.
iDirect Tunnel SVN	A Global SVN that connects Protocol Processors and Line Cards in a Velocity network.
Inbound Carrier	1) The carrier transmitted from the remote satellite router to the hub. 2) An adaptive Time Division Multiple Access (TDMA) carrier from the satellite terminal to the Satellite Access Station (SAS). Same as Upstream Carrier.
Inbound Group	A set of inbounds associated with an outbound.
Incident	A super alarm that is normally internal in the NMS, and is based on the linking of multiple specific alarm conditions.

Indoor Unit (IDU)	The satellite modem and indoor devices (in contrast to Outdoor Unit or ODU).
iNet	An individual DVB-S2/ACM outbound and inbound group. In Velocity, one or more iNets may be assigned to a channel.
Information Rate	The rate of transmission of user data over an upstream or downstream carrier including IP headers and overhead.
Inroute	A Time Division Multiple Access (TDMA), Upstream Carrier.
Inroute Group	A group of inroutes shared by a set of remotes in a network. Typically, a remote can frequency hop among the Time Division Multiple Access (TDMA) carriers within its inroute group.
Inroute Group Composition (IGC)	A set of defined carriers assigned to an inroute group.
Intermediate Frequency (IF) Domain	Represents a specific group of line cards and IF frequency ranges at which these line cards operate.
Inventory Data	A list of the various files and data associated with a network element.
Lightweight Encapsulation for Generic Streams (LEGS)	An iDirect proprietary protocol for encapsulating data in DVB-S2 networks which maximizes the efficiency of data packing into BBFrames.
Low Density Parity Coding (LDCP)	The error correction coding scheme used in DVB-S2 networks.
Low-noise Block (LNB) Converter	A receiving device that is integrated in the Very Small Aperture Terminal (VSAT) terminal to convert the signal gathered by the antenna feed circuit.
Management Profiles	It is a standardized method of defining the duration, in days, for which various types of historical data are collected and stored.
Maximum Information Rate (MIR)	A configuration parameter that specifies maximum bandwidth allocated to a node, regardless of demand generated by the node. A node with MIR set will never be granted more bandwidth than the configured MIR bit rate. A Group QoS (GQoS) feature.

Maximum MODCOD	Modulation and Coding (MODCOD) scheme, used in Digital Video Broadcasting - Satellite - Second Generation (DVB-S2) networks.
MIDAS Controller Board	a type of controller board used on newer chassis.
Minimum Information Rate (MIN)	A Group QoS feature: A configuration parameter that specifies maximum bandwidth allocated to a node, regardless of demand generated by the node.
Modulation and Coding (MODCOD)	The combinations of Modulation Types and Error Coding schemes supported on a satellite channel. The higher the modulation the greater the number of bits per symbol (or bits per Hz).
Monitor	An operation that can be executed on a specific server to track a specific performance metric.
Multicast Group Service Plan (MGSP)	A service plan that provides a data transmission service in which the data stream is simultaneously transmitted to multiple recipients, rather than sending separately to each recipient.
Multicast Subscriber Service Plan Profile (MSSPP)	Like the unicast SSPP, the MSSPP is configured in Pulse by authorized VNOs and used in creating a Terminal Service Plan - particularly, a multicast component of a TSP, to which individual terminals or a group of terminals may subscribe.
MUSiC Box	A hardware device that allows a common antenna/electronics platform to be shared across multiple remotes that are in the same physical location.
Network Accelerator	a hardware device that maximizes the speed of encrypted traffic over secure networks.
Network Address/Port Translation (NAT/PAT or NAPT)	A process of modifying IP addresses as well as TCP/UDP port numbers so that nodes residing on a private network can share a public IP address for communication with the outside world.
Network Domain	The network domain immediately above the transport element domain — it consists of logical infrastructure elements.
Network Management Center (NOC)	One or more locations from which network monitoring and control, or network management, is exercised over a computer, telecommunication or satellite network.

Network Management System (NMS)	Software used by network operators to configure and manage their networks.
Network Management System (NMS) *Server Cluster*	A group of servers that act as a single system to provide the resources required by the Pulse NMS for managing network configuration and control, software version management and updates, as well as for monitoring and reporting on network events and alarms. The NMS server cluster is implemented at both the primary SAS, and optional backup SAS sites where applicable, and at the NOC site.
Nominal MODCOD	The reference operating point for a remote receiving a downstream Digital Video Broadcasting - Satellite - Second Generation (DVB-S2) carrier with ACM.
Options File	A configuration file generated by the NMS, used to manage download configuration settings to protocol processors, hub line cards and satellite terminals.
Outbound Carrier	Same as Downstream Carrier.
Outroute	See Outbound Carrier.
Package	A package, in the NMS, represents various software files and images required to upgrade a Protocol Processor Server, Line Card, or Satellite Terminal to a particular software version.
Payload Compression	A mechanism whereby a datagram is compressed with the intent of reducing the size of data transmitted over congested or slow network connections, thereby increasing the speed of such networks without losing data.
Pending Configuration	The pending configuration of an element is the last saved or the configuration that is currently stored in the NMS database.
Physical Domain	The hardware infrastructure network elements; i.e. sites, virtual networks, hub chassis components, system management software and other ancillary servers.
Primary Site	The main operational site of network Site pairs. Each site and its optional backup/diversity site may operate as primary or backup (secondary) site.
Probe Command Configurator	A Configurator operation that supports real-time interaction with the operating system of Satellite Terminal, Line Card, and Cluster infrastructure elements; as well as support for accessing network service elements including Group Service Plan (GSP), and Subscriber Service Plan Component (SSPC).

Protocol Processor (PP)	The Protocol Processor is a high performing, highly scalable core part of the hub, providing many critical functions. The protocol processor software is designed to scale and provide load balancing and automatic redundancy.
Public Key Infrastructure (PKI) Data File	The chain of trust required by network elements to facilitate inter-communication.
Pulse Banner	The dark gray area across the top of each Pulse page; also the global header.
Quality of Service (QoS)	System traffic flow, classification, filter and priority: The classification and prioritization of IP traffic in order to optimize the delivery of packets as it flows through the network. (Attributes of a connection that affect QoS include throughput, latency, jitter and packet loss and others).
Reference Clock Module (RCM)	Hardware component required for frequency hopping.
Remote-Based **Group QoS (GQoS)**	Provides ability to configure all upstream and downstream rate shaping parameters on QoS user interface, for each remote. This setting establishes pre-GQoS compatibility and is the default QoS Mode for Group QoS Settings.
Remote Locking	A feature that allows individual remotes to be locked to a particular network. Once a remote is locked with a key, it only functions in a network with the same key.
Return Material Authorization (RMA)	Issued by iDirect TAC, for equipment that must be returned for repair or replacement.
Revoke Certificate	Retraction of a security certificate that was previously assigned to a network element.
Roaming Remote	Mobile remotes that use the Global NMS feature to “roam” from network to network around the globe. Roaming remotes are not constrained to a single location or limited to any geographic region.
Roll Vault	A Pulse operation used to increase security of the network by requesting that the vault table cease using the existing keys and generate a new set of keys for data encryption.
Route map	A map that defines the routing policies that are considered before a router examines its forwarding table.

Real-Time Transport Protocol (RTP)	Real-Time Transport Protocol. A protocol designed to provide end-to-end network transport functions for applications that transmit real-time data, such as audio, video, or simulation data, over unicast or multicast network services. RTP provides such services as payload type identification, sequence numbering, time-stamping, and delivery monitoring to real-time applications.
Satellite Access Station (SAS)	The Velocity network terrestrial segment, also referred to as a hub, provides communications between the Service Provider Data Communications Network and the remote Satellite Terminals. A SAS site contains the SAS LAN, Protocol Processor servers, Network Management System (NMS) servers, Web Cache servers, Chassis and Line Cards, the Radio Frequency Subsystem, and other ancillary equipment.
Satellite Terminal Domain	The element domain that provides IP connectivity between each remote LAN and the Teleport equipment.
Satellite Terminal Identification Message	A terminal identification feature whereby, on each attempt to acquire the network, a terminal is screened, by the Satellite Access Station (SAS), as to whether it should be allowed to acquire the network.
Satellite Virtual Network OR Synthetic Virtual Network (SVN)	1) An IP VPN that contains a satellite network segment. 2) An SVN is a set of connected elements within the Global Xpress network that uses a common IP address space. It comprises a VPN within both the backbone and satellite networking segments and extends to multiple satellite terminals. The traffic within the SVN on these satellite terminals is managed by a single SVNO and is subject to global GQoS rules.
Scheduling Service	A Pulse service, implemented in a network system, to support the carrying out of various server tasks that must be performed on a routine or other basis.
Server (Blade) SVN	Each Server SVN is generated automatically as a result of creating a Site SVN and its parent Global SVN.
Service Area Group	In Velocity, an SA Group maps to a single active map in the NMS, and represents an identifier pool from which service areas (SA) can be designated when defining geoscopes or regulatory areas (RA).
Site	A Site, within a Velocity™ Network, is a collection of processes and equipment at a designated location — for example a Satellite Access Station (SAS) or a Network Operations Center (NOC), or External Access Portal (EAP).
Site SVN	The second organization level of the Velocity Global SVN hierarchy; represents the segment of an SVN (VPN) located within a Site — for example within a NOC or Satellite Access Station (SAS).

Sleep Mode	A feature that allows remote modems to conserve power consumption during periods of network inactivity.
Spread Spectrum	A transmission technique in which a pseudo-noise (PN) code is employed as a modulation waveform to “spread” the signal energy over a bandwidth much greater than the signal information bandwidth.
Squid proxy	A web proxy cache server application that provides caching services to a variety of network protocols, such as HTTP or FTP.
Static Configuration	The terminal configuration information that is stored in the configuration file, and is the minimum required by the terminal software for the terminal to acquire into a specific iNet.
Static Multicast Stream	When this Velocity multicast option is enabled, the NMS provides the terminal with the static multicast configuration.
Statistics Report	A report that displays the measure of an operational characteristics of a network element.
Stats Threshold Profile	A set of Stats Threshold Rules.
Stats Threshold Rule	A user-defined standard based on a specific network metric, that generates an event when the standard is met.
Steady State Margin	In Digital Video Broadcasting - Satellite - Second Generation (DVB-S2) networks, the margin added to the SNR thresholds measured at hardware qualification to arrive at the operational SNR threshold during steady state operation.
Subscriber Service Plan Component (SSPC)	When an Subscriber Service Plan Profile (SSPP) is selected as part of a Terminal Service Plan (TSP), an instance of the SSPP is created in the NMS. That instance of the SSPP is called a Subscriber Service Plan Component, as it could be one of several components of the Terminal Service Plan (TSP).
Subscriber Service Plan Profile (SSPP)	A set of service plan parameters, configured for use in creating a Terminal Service Plan.
Symbol Rate	The number of symbols that are transmitted in one second. From the symbol rate, calculate the bandwidth (total number of bits per second) by multiplying the bits per symbol by the symbol rate.

System Generated Files	These are elements that are generated in the NMS when some other element is created.erived by the NMS and is a unique numeric value such as a Derived ID (DID) or a text value, such as a name. Also called, "System Generated Value"
System Monitor	A routine that monitors a particular performance metric on a server.
System Monitor Service	A service that supports NMS functionality that allows administrators to monitor the physical health and status of the NMS and Data Path servers, routers, and switches.
Technical Assistance Center (TAC)	iDirect Customer service and technical support center, at http://tac.idirect.net or 703-648-8151. iDirect Government customer service and technical support center, at http://tac.idirectgov.com
Teleport	A Teleport, for example, contains elements hub equipment such as the Protocol Processor servers, line cards, and chassis; and the NMS and associated servers, and connecting SVNs. Also called SAS.
Terminal Domain	In the Pulse hierarchy of network element domains, the element domain that comprises terminals and terminal components.
Terminal Metadata File	A file that consists mainly of terminal model-specific information that is loaded during PP start-up.
Terminal Service Plan (TSP)	It is the configured service plan of an individual terminal.
Terminal SVN	That segment of an SVN that is located in the remote network behind a Satellite Terminal.
Terminal Type	A terminal type is a unique element type in the NMS that has a unique Name, is composed of specific terminal components (LNB, BUC, and ACU), a specific satellite router type, and specific RF parameters. As an NMS element the terminal type defines a set of baseline elements from which multiple terminals may be created.
Time Division Multiple Access (TDMA)	A type of over-the-air multiplexing by which two or more channels of information are transmitted simultaneously over the same link by allocating different time slots within TDMA frames for the transmission of each channel.
Token	In a network system, it is a way of managing the number of times a certain operation can be performed or an object may be created.
Token Number	The number of tokens owned by a user group for a specific operation.

Traffic Filters	Traffic filters are created to classify and manage packets presented on the Upstream or Downstream.
Transmission security (TRANSEC)	The component of communications security that includes the application of measures designed to protect transmissions from interception and exploitation by means other than encryption.
Transmission Rate	A measure of the speed of all over-the-air data. This includes the user data (Information Rate), overhead, and FEC encoding bits.
Transport Domain	In the Pulse hierarchy of network element domains, the element domain that represents a set of logical elements that are associated with the space segment of a Velocity™ Network. For example, satellites, beams, and channels.
Update Profile	A list of one or more update rules.
Upstream Carrier	Same as Inbound Carrier and may be characterized as the carrier transmitted from the remote satellite router to the hub.
Used Tokens	The number of tokens that are already used or given away.
User	An individual or an internal process or external system that has authorized access to the NMS, but only as a member of one or more user groups and with assigned user roles.
User Datagram Protocol (UDP)	A connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols. UDP is defined in RFC 768.
User Group	A collection of users with a common set of permissions and visibility.
User Role	A specific set of defined permissions that can be assigned to a user.
Variable Coding and Modulation (VCM)	A method of applying coding to a DVB-S2 data stream in which MODCODs are assigned according to service type. This method is not currently supported.
Vault Table	A vault table stores a set of AES keys, used to encrypt all Certificate Authority (CA) private keys that are associated with the same chain of trust branch.
Very Small Aperture Terminal (VSAT)	A two-way satellite ground station with a less-than three meter dish antenna.

Virtual Local Area Network (VLAN)	Any broadcast domain, partitioned and isolated in a computer network at the data link layer (OSI layer 2). *Note: To subdivide a network into virtual LANs, configure a network switch or router.*
Virtual Network Operator (VNO)	A member of a VNO User Group. A VNO User Group restricts visibility and access rights of group members based on the permissions granted to the group by the Hub Network Operator (HNO).
Virtual Remote	An instance of a Group QoS Application running on a remote modem. In Application Based QoS mode, a remote has one Virtual Remote for each Application assigned to the remote. In Remote Based QoS mode, all Applications are combined into a single Virtual Remote.

iDirect

13861 Sunrise Valley Drive, Suite 300
Herndon, VA 20171-6126
+1 703.648.8000
+1 866.345.0983

www.idirect.net

Advancing a Connected World