NetVue User Guide
Release 2.5

Part Number MN-NETVUE
Revision 9

IMPORTANT NOTE: The information contained in this document supersedes all previously published information regarding this product. Product specifications are subject to change without prior notice.

Comtech EF Data, 2114 West 7th Street, Tempe, Arizona 85281 USA, 480.333.2200, FAX: 480.333.2161

Revision History

Rev	Date	Description
-	6-2013	Initial Release.
1	10-2013	Released 1.1 updates.
2	12-2013	Internal documentation update.
3	4-2014	Internal documentation update.
4	7-2014	Released 2.1 updates.
5	10-2015	Internal documentation update.
6	12-2015	Bandwidth Manager and Provisioning updates.
7	1-2016	Added section J.2.4, connection with local SLNet error troubleshooting.
8	4-2016	Released 2.2 updates; changes to Chapters 3, 5, and 6.
9	7-2017	Released 2.5 updates; changes to Chapters 3, 4, 5, and Appendix B; added Appendix K and L. Updated document formatting.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

BLANK PAGE

PREFACE

About this User Guide

This user guide contains installation and operation information for the Comtech EF Data (CEFD) NetVue Integrated Management System (IMS).

The user guide is a single resource for information including, but not limited to the set up, operation, management, and troubleshooting of a network that is managed by the NetVue IMS.

Intended Audience

This user guide is intended for persons responsible for the provisioning, day-to-day operation, and performance of a network managed by the NetVue IMS. The information in this user guide is intended for operators, Network and RF technicians, planners, network engineers, managers, as well as IT network professionals.

Conventions and References

Patents and Trademarks

Comtech EF Data's Patents and Patents Pending are available for review http://patents.comtechefdata.com.

Comtech EF Data acknowledges that all trademarks are the property of the trademark owners. DoubleTalk® is licensed from "Raytheon Applied Signal Technology".

DoubleTalk® is a registered trademark of "Raytheon Applied Signal Technology".

Carrier-in-Carrier® is a registered trademark of Comtech EF Data.

Microsoft®, Windows®, Internet Explorer® and Visio® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Google Chrome® is a registered trademark of Google Inc.

Mozilla Firefox® is a registered trademark of the Mozilla Foundation.

Cautions and Warnings

WARNING indicates a potentially hazardous situation that, if not avoided, could result in death or serious injury.

CAUTION indicates a hazardous situation that, if not avoided, may result in minor or moderate injury. CAUTION may also be used to indicate other unsafe practices or risks of property damage.

IMPORTANT or NOTE indicates information critical for proper equipment function, or a statement that is associated with the task being performed.

Regulatory Compliance

Telecommunications Terminal Equipment Directive

In accordance with the Telecommunications Terminal Equipment Directive 91/263/EEC, do not connect this equipment directly to the Public Telecommunications Network.

CE Mark

Comtech EF Data declares that the NetVue unit meets the necessary requirements for the CE Mark.

RoHS Compliancy

This unit satisfies (with exemptions) the requirements specified in the European Union Directive on the Restriction of Hazardous Substances, Directive 2002/95/EC, (EU RoHS).

EMC (Electromagnetic Compatibility)

In accordance with European Directive 89/336/EEC, independent testing showed that the NetVue unit complied with these standards:

Emissions EN 55022 Class B Limits and methods of measurement of radio interference characteristics of Information Technology Equipment
(Also tested to FCC Part 15 Class B)

Immunity EN 50082 Part 1 Generic immunity standard, Part 1: Domestic, commercial and light industrial environment.

Additionally, the NetVue unit complied with these standards:

- EN 61000-3-2 Harmonic Currents Emission
- EN 61000-4-6 RF Conducted Immunity
- EN 61000-3-3 Voltage Fluctuations and Flicker
- EN 61000-4-8 Power frequency Magnetic Field Immunity
- EN 61000-4-2 ESD Immunity
- EN 61000-4-9 Pulse Magnetic Field Immunity
- EN 61000-4-4 EFT Burst Immunity
- EN 61000-4-11 Voltage Dips, Interruptions and Variations Immunity
- EN 61000-4-5 Surge Immunity
- EN 61000-4-13 Immunity to Harmonics

Electrical Safety

The NetVue unit has been shown to comply with the EN 60950 Safety of Information Technology Equipment (including electrical business machines) safety standard.

Fuses

CAUTION: Always replace the fuses with the correct fuse type and rating. Use correct fuses to help prevent damage to the equipment.

Class I Pluggable Equipment Type A-Protective Earthing

The cable distribution system/telecommunication network of this product relies on protective earthing and the integrity of the protective earthing must be insured

In Finland:

"Laite on liitettävä suojakoskettimilla varustettuun pistorasiaan"

In Norway:

“Apparatet må tilkoples jordet stikkontakt”

In Sweden:

“Apparaten skall anslutas till jordat uttag”

In Denmark:

"Apparatets stikprop skal tilsluttes en stikkontakt med jord, som giver forbindelse til stikproppens jord"

Galvanic Isolator Use

Utrustning som är kopplad till skyddsjord via jordat vägguttag och/eller via annan utrustning och samtidigt är kopplad till kabel-TV nät kan i visa fall medföra risk för brand. För att undvika detta skall vid anslutning av utrustningen till kabel-TV nät galvanisk isolator finnas mellan utrustningen och kabel-TV nätet

Restricted Access Location

In Nordic Countries, equipotential bonding should be applied using the permanently connected ground stud by a qualified service person

Battery Warning

CAUTION

Risk of explosion if battery is replaced by an incorrect type. Dispose of used batteries according to the instructions.

Environmental

Maximum storage temperature allowed is -20 to +70°C.

The NetVue must not be operated in an environment where it is exposed to:

- Precipitation
- Condensation
- Humid atmospheres above 95% RH
- Altitudes (unpressurized) greater than 2000 meters
- Excessive dust or vibration
- Flammable gases
- Corrosive or explosive atmospheres
- Extremes of temperature outside the ambient range 0 to +50°C

Operation in vehicles or other transportable installations that are equipped to provide a stable environment is permitted. If such vehicles do not provide a stable environment, safety of the equipment to EN 60950 may not be guaranteed.

Related Documents

- EN300-421 and EN301-210 ETSI
- ETSI EN302-307
- INTELSAT Earth Station Standards IESS-308, -309, -310, and -315
- EUTELSAT SMS

Equipment Drivers

Contact Comtech EF Data about equipment drivers that may be supported by the NetVue IMS.

Product Support

For all product support, please call:

esc@comtechefdata.com

+1.866.472.3963
(Toll Free, U.S. & Canada)

+1.240.243.1880
(Outside U.S. & Canada)

Comtech EF Data Headquarters

http://www.comtechefdata.com

Comtech EF Data Corp.

2114 West 7th Street

Tempe, Arizona USA 85281

+1.480.333.2200

Warranty Policy

Comtech EF Data products are warranted against defects in material and workmanship for a period of two years from the date of shipment. During the warranty period, Comtech EF Data will, at its option, repair or replace products that prove to be defective. Repairs are warranted for the remainder of the original two year warranty, or a 90 day extended warranty, whichever is longer.

For equipment under warranty, the owner is responsible for freight to Comtech EF Data and all related customs, taxes, tariffs, insurance, etc. Comtech EF Data is responsible for the freight charges only for return of the equipment from the factory to the owner. Comtech EF Data will return the equipment by the same method (i.e., Air, Express, Surface) as the equipment was sent to Comtech EF Data.

All equipment returned for warranty repair must have a valid RMA number issued prior to return and be marked clearly on the return packaging. Comtech EF Data strongly recommends all equipment be returned in its original packaging.

Comtech EF Data Corporation's obligations under this warranty are limited to repair or replacement of failed parts, and the return shipment to the buyer of the repaired or replaced parts.

Limitations of Warranty

The warranty does not apply to any part of a product that has been installed, altered, repaired, or misused in any way that, in the opinion of Comtech EF Data Corporation, would affect the reliability or detracts from the performance of any part of the product, or is damaged as the result of use in a way or with equipment that had not been previously approved by Comtech EF Data Corporation.

The warranty does not apply to any product or parts thereof where the serial number or the serial number of any of its parts has been altered, defaced, or removed.

The warranty does not cover damage or loss incurred in transportation of the product.

The warranty does not cover replacement or repair necessitated by loss or damage from any cause beyond the control of Comtech EF Data Corporation, such as lightning or other natural and weather related events or wartime environments.

The warranty does not cover any labor involved in the removal and or reinstallation of warranted equipment or parts on site, or any labor required to diagnose the necessity for repair or replacement.

The warranty excludes any responsibility by Comtech EF Data Corporation for incidental or consequential damages arising from the use of the equipment or products, or for any inability to use them either separate from or in combination with any other equipment or products.

A fixed charge established for each product will be imposed for all equipment returned for warranty repair where Comtech EF Data Corporation cannot identify the cause of the reported failure.

Exclusive Remedies

Comtech EF Data Corporation's warranty, as stated is in lieu of all other warranties, expressed, implied, or statutory, including those of merchantability and fitness for a particular purpose. The buyer shall pass on to any purchaser, lessee, or other user of Comtech EF Data Corporation's products, the aforementioned warranty, and shall indemnify and hold harmless Comtech EF Data Corporation from any claims or liability of such purchaser, lessee, or user based upon allegations that the buyer, its agents, or employees have made additional warranties or representations as to product preference or use.

The remedies provided herein are the buyer's sole and exclusive remedies. Comtech EF Data shall not be liable for any direct, indirect, special, incidental, or consequential damages, whether based on contract, tort, or any other legal theory.

Chapter 1. INTRODUCTION

1.1 Basic Concepts

This section introduces some concepts that you need to understand when you are new to NetVue. These concepts are present throughout the NetVue User Manual. If you are not yet familiar with them, it is advisable to read this section before you go on to the rest of the documentation.

This chapter covers the basics of NetVue, but not the operation of the NetVue system. After reading this chapter, read the Navigation, Operation and Client Configuration chapters to learn about operating the NetVue for Comtech EF Data's Heights, Advance VSAT and Trunking products.

1.1.1 NetVue Server and Client

To use NetVue, you must have at least one NetVue Server and a NetVue Client.

- **NetVue Server or DMA** is a piece of hardware that runs the NetVue software.
- **NetVue Client** is an entity that communicates with the NetVue Server. Typically, the term means a client application that allows users to interact with the NetVue Server.

1.1.2 System Components

On a NetVue Server, you can find different kinds of objects that represent components of your system:

- **An Element** is a device monitored by the NetVue Management System.
- **A Parameter** is a variable that refers to pieces of data in the system. Its value can be detected by NetVue, or can depend on user input. Values can be part of a range limited by a particular minimum and maximum, or part of a limited set of predetermined values.
- **A Service** is a group of elements, combined from the perspective of a particular business aspect. As such, a NetVue service reflects all components required for an actual business service.
- **A View** is a folder that can contain elements, services and other NetVue components. Logically combining components in a view allows users to access quickly all components that belong together in some way.

- **A Redundancy Group** is a group of devices configured in such a way that, if any of them fail, then others can take over automatically.

1.1.3 NetVue Functionalities

The following concepts pertain to the way NetVue gathers and visualizes information about your system:

- **A Protocol or Driver** is an XML file that allows NetVue to communicate with a device in the system.
- **A Visual Overview** is a graphical representation of components and data in the system. The visual overviews in NetVue are created in Microsoft Visio, and can represent information in many different ways. They can be made interactive also, so that the user can interact with the NetVue system by clicking areas in the visual overview.
- **An Alarm** is a notification that a parameter value has crossed a particular threshold, or a parameter has attained a particular value. With alarms, users are notified of any abnormal situation in the system. Alarms can have different severity levels, and can be linked to other alarms.
- **Trending**: NetVue can store measurements of parameter values, taken over time. This data is shown in graphs so that you can see trends in the system.

1.1.4 NetVue Modules

A NetVue system can have several additional modules or apps. Some of these modules are mentioned quite often throughout the documentation. It is useful to know what they are, even if you will not use them yourself.

- **Automation** is a module used to create scripts that can execute certain tasks automatically. Scripts can set parameters, change element states, send notifications, etc.
- **Correlation** is a module that can gather information about parameter values and alarms, and trigger other alarms, notifications or automation scripts based on triggers defined by the user.
- **Dashboards** is a module that allows the creation of dashboards, which are pages containing important information about components of the system. You can see these dashboards separately from the main NetVue client applications.
- **Scheduler** is a module that can schedule certain actions in the NetVue System. It works in close relation with the Automation module.
- **Reporter** is a module you can use to create reports on the NetVue System. The reports use templates that you can fully customize. You can see Reports within the Cube client application, or independently, or you can send them by email.
- **Spectrum Analysis** is a module that allows the integration of spectrum analyzers in a NetVue System.
- **System Center** is a module that contains most of the administrator functionalities in NetVue, such as management of databases and users.

1.2 General Layout of a NetVue System

A NetVue System is a cluster of interconnected NetVue Servers.

As to software, all NetVue Servers in a NetVue System (cluster) are identical. Each of them is a fully functional monitoring system.

In a cluster, there is no central server and there are no dedicated client terminals. NetVue users can log on to any of the NetVue Servers in the cluster, and see the entire NetVue System as a single entity.

1.2.1 NetVue Servers

A NetVue Server is a piece of industry-standard computing hardware running the NetVue Server software on top of a Microsoft Windows 2012 Server operating system.

The NetVue Server software is a collection of services of which the names all start with “SL” (SLNet, SLProtocol, SLLog, etc.).

By default, the startup type of the NetVue services is set to Automatic (Delayed Start). This means that NetVue waits until all Windows services are running before launching its own services.

1.2.2 NetVue Clients

NetVue client applications connect to only one NetVue Server in the NetVue System. Through that single point of contact, they then have access to all information in the cluster.

1.2.3 NetVue Databases

Each of the NetVue Servers has a local database. By default, this is a MySQL database.

Optionally, the data stored in each of the local databases can be offloaded automatically to a central database on a dedicated database server. This is especially useful when you intend to use that data for heavy-duty reporting or billing purposes.

1.2.4 Dual LAN Architecture

Every NetVue Server is equipped with a dual Ethernet interface card.

- Primary port
  - Connected to the corporate IP network
  - Communicates with clients (web browsers, SNMP Managers, etc)
  - Processed data (e.g. alarms, real-time data, reports, etc.)
- Secondary port
  - Connected to the equipment management LAN
  - Collects information from the Elements
  - Raw data

1.2.5 NetVue Peripherals

In some network setups, special interfacing tools (called NetVue peripherals) connect a NetVue Server to third-party devices or serial devices. Typically, the intelligence is in the NetVue Server, while the peripherals do medium interfacing and conversion tasks.

Frequently used peripherals include:

- IP to Serial Gateway (RS-232 and/or RS-485 ports)
- IO Gateway (analog and digital inputs/outputs (interfaces))
- GPIB Gateway (IEEE-488 ports)
- And others

1.3 NetVue Applications

Several applications are available for access to NetVue. In addition to the two main client applications, there are several other applications with more limited functionality.

- **NetVue Cube** is the main client application used to connect to a NetVue Server. It exists as a standalone version, and as a version to be used in Internet Explorer.
- **Reports and Dashboards** are Reports and/or Dashboards that you can consult separately from the main NetVue client applications.
- **Alerter** is the system tray application that notifies the user of alarms in the NetVue system.
- **DataMiner Taskbar Utility** is the system tray application on the NetVue Server that allows some basic functions, like starting, stopping and upgrading the NetVue Server.
- **Web APIs** allow any third-party application to retrieve real-time NetVue data via XML-RPC, SOAP or JSON.

When connecting to a NetVue Server by browsing to the IP address of the server, you are redirected to your default user interface, which is the NetVue Cube. Mobile clients are directed to the mobile interface.

1.4 Licensing

The NetVue System supports a given number of devices per NetVue Server based on the number of devices specified in the license. Licensing also controls the redundancy feature.

A device is an element under management. Examples of managed devices, or elements, are modems, switches, RF devices, etc.

For example, a NetVue Server with a license for 100 devices can manage a maximum of 100 devices collectively. (Please note that SLA Manger and Ping Manager also consume the device count)

To change a license, CEFD Product Support uses Team Viewer to access the NetVue Server. They install a new license file without negatively affecting the NetVue System operation.

1.4.1 License Features

1.4.1.1 Managed Devices

- 50 Devices
- 110 Devices
- 250 Devices
- 500 Devices

1.4.1.2 Redundancy

- Cold Standby Server, powered down until needed
- 1:1 Hot Synched Server, powered on and continuously synchronized

1.4.2 Procedure to Upgrade an Existing NetVue License

1. Contact CEFD Sales with a purchase order for the license upgrade.
2. CEFD contacts the Customer to schedule the license upgrade.
3. CEFD installs the license upgrade.
4. CEFD asks the Customer to reboot the server and check that the NetVue application is running without error(s).

BLANK PAGE

CHAPTER 2. SERVER OPERATIONS AND CLIENT CONFIGURATION

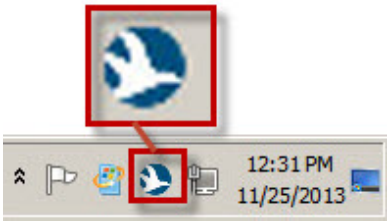
2.1 Verify and Start DataMiner

This section explains how to verify that the DataMiner Service has been started and/or how to start the Dataminer Section.

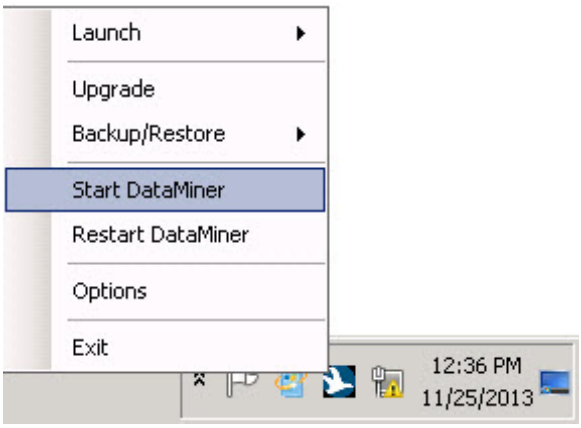
2.1.1 Start the DataMiner Service

1. Go to the system Tray in the lower right corner.

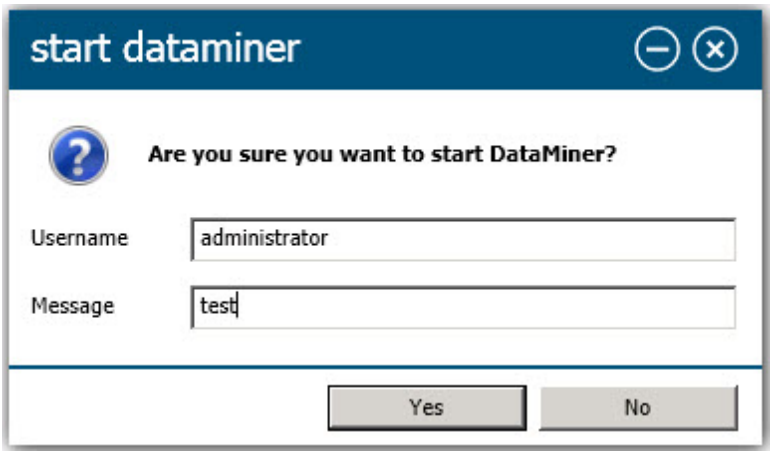
2. Find the DataMiner Icon.



3. Right-click the DataMiner Icon and select *Start DataMiner.*



4. In the *start dataminer* prompt, enter *administrator* and any message.

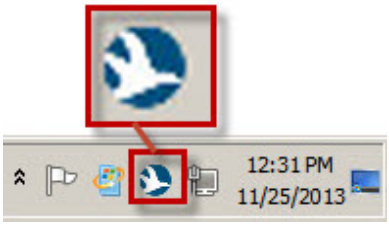


5. Click *Yes* to start the service.

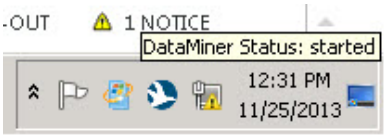
2.1.2 Verify DataMiner Service Started

1. Go to the system Tray in the lower right corner.

2. Find the DataMiner Icon.



3. To see if the service started, hold the mouse cursor over the DataMiner icon.



2.2 UI Installation

NetVue Client is an XAML application/browser object (XBAP). The executable module is downloaded and installed onto the operator/user computer automatically. This installation first occurs when you open the NetVue Cube user interface through an internet browser.

After the initial installation is completed, the version is checked every time you launch the UI and connect to a NetVue server. If a newer version of the XBAP is available, it is downloaded and installed automatically.

2.2.1 Prerequisites for Running XBAPs

The Internet browser must have the ability and permission to run XAML browser applications.

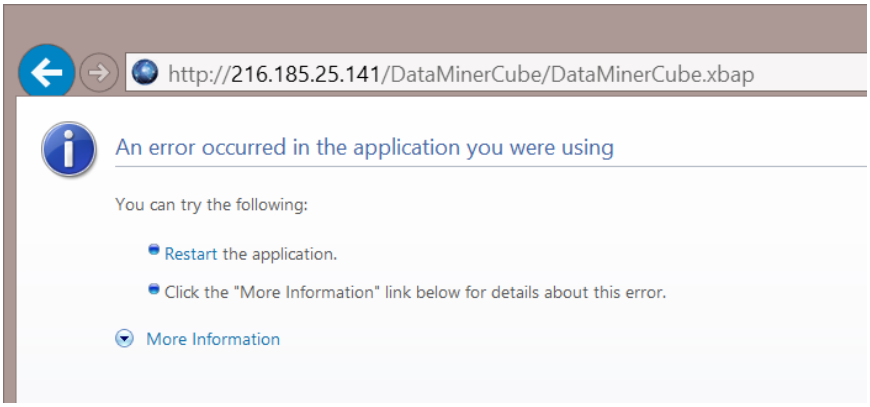


Figure 2-1. Security Certificates

The Skyline certificates must be installed. A *Trust Not Granted* error occurs if the Skyline self-signed Root certificates are not installed when you run NetVue Cube.

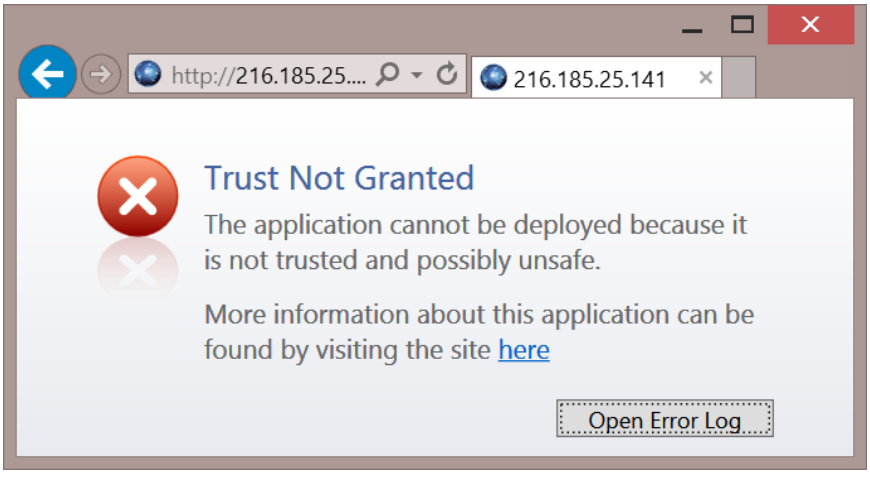


Figure 2-2. Trust Granting

Third-party software is required:

- Microsoft .NET Framework 4.0
- Microsoft Web Services Enhancements 2.0 SP3 (only when using Web Services)

If necessary, install the XBAP offline by running an MSI installation package or a "ClickOnce" web installer.

2.2.1.1 Install the Skyline certificates

1. Open the Internet browser, and go to this address:

   http://[NetVue Server]/Tools

   Replace [NetVue Server] with the IP address or host name of the NetVue Server to which you want to connect.

2. In the *Installing Skyline Root Certificate* section, click the *link*.
3. In the *File Download* dialog box, click *Run*.

2.2.1.2 Configure Microsoft Internet Explorer to run NetVue Cube

Microsoft Internet Explorer must be permitted to run XAML browser applications. To configure the XBAP settings in Microsoft Internet Explorer, perform the following steps:

1. Open Microsoft Internet Explorer.
2. Choose *Tools* > *Internet Options*.
3. In the *Security* tab, select the applicable zone and click *Custom level.*
4. In the *Security Settings* dialog box, go to *.NET Framework*.
5. Set *XAML browser applications* to *Enable*.

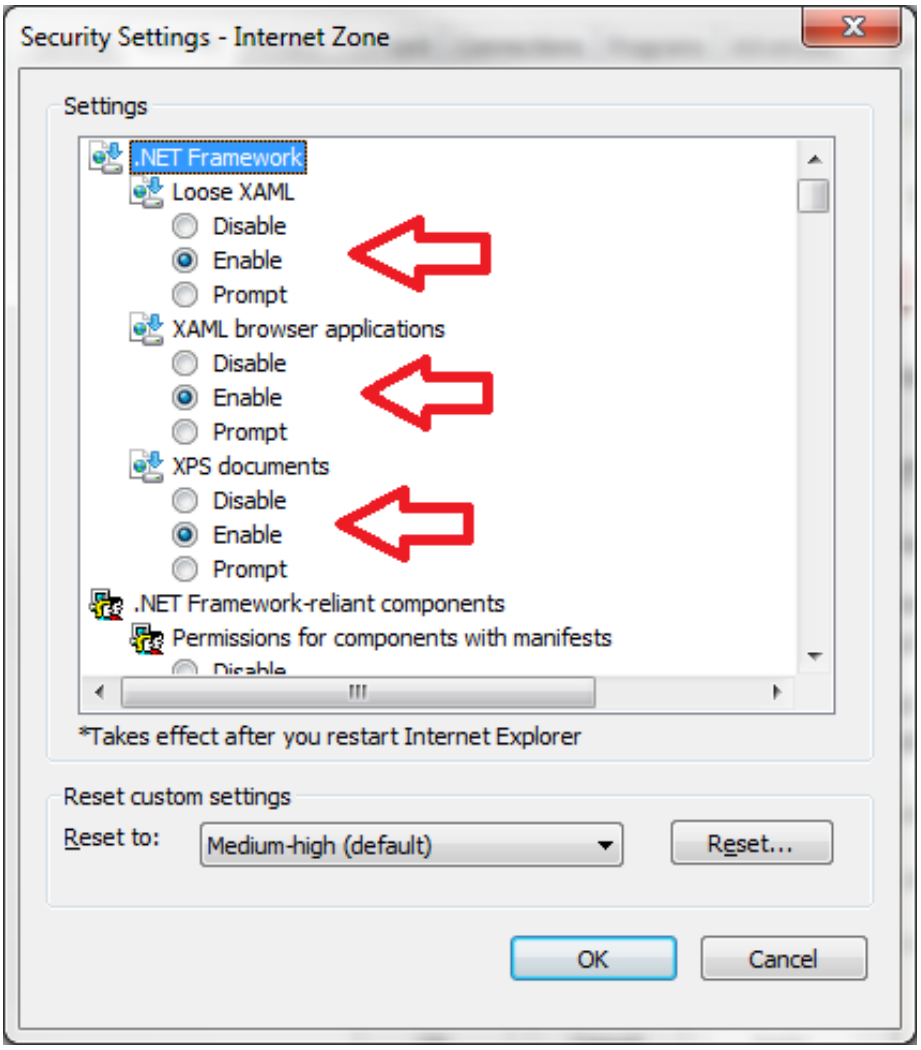


Figure 2-3. Security Settings – Internet Zone

Chapter 3. CUBE NAVIGATION/OPERATIONS/ ADVANCED FUNCTIONS

3.1 Cube Navigation

This chapter describes how to use Internet Explorer to get access to and navigate in NetVue.

3.1.1 Access NetVue User Interface

3.1.1.1 Log on to NetVue Cube

1. Open an Internet browser window.
2. Go to ***http://[IP address of NetVue Server]/***

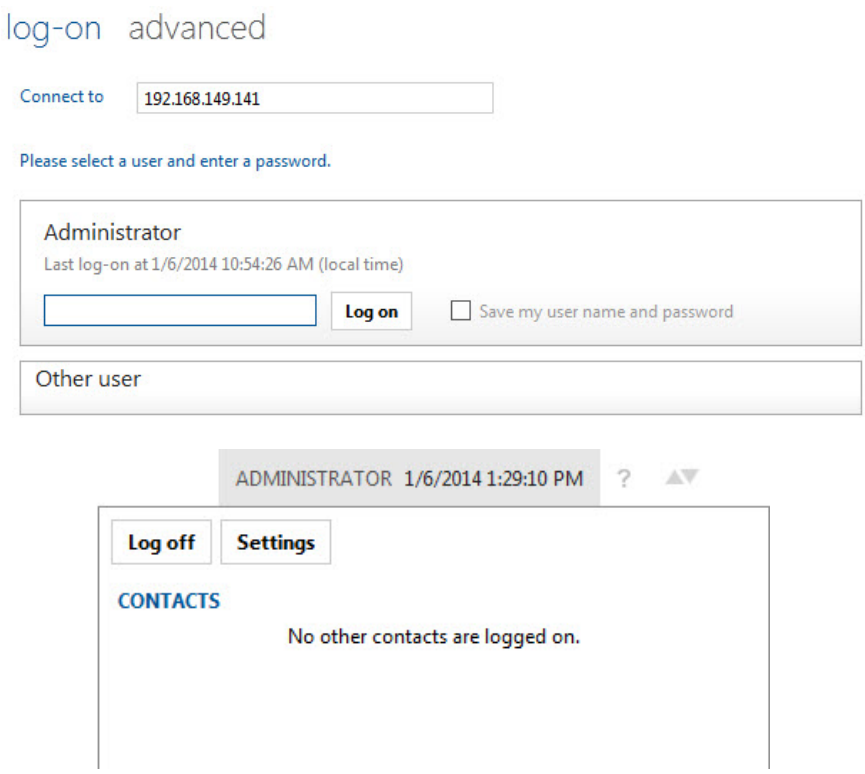


Figure 3–1. NetVue Logon

3. If necessary, enter a different NetVue agent IP address (in the cluster) in the **Connect To** box at the top of the logon screen.
4. Click one of the listed users, or select **Other user**.
5. For the initial log in, use the supplied login and password.
6. If desired, click **Save my User Name and Password** to save the logon information. The next time you start the NetVue client application, it logs on with the saved user name and password automatically.
7. Click **Log on**.

The NetVue client application connects to the specified NetVue Server, and the NetVue home page opens.

NetVue searches the client computer for cached settings for the logged–on user account. If none are found, NetVue loads the default user settings stored on the NetVue Server.

The NetVue client always attempts to login with the credentials of the local Windows user (or Domain account) first. If integrated into Windows Domain, or if the user/password of the local account matches the one configured in NetVue, then the application opens without showing the logon screen.

3.1.1.2 Override the Default Connection Type

The default connection type between the NetVue client application and the NetVue server is specified in a file kept on the local drive of the NetVue server:

C:\Skyline NetVue\Webpages\connectionsettings.txt

You can override the default connection type, if desired.

BEFORE you click **Log–on**, perform the following steps:

1. At the top of the **log–on** window, click **advanced**.

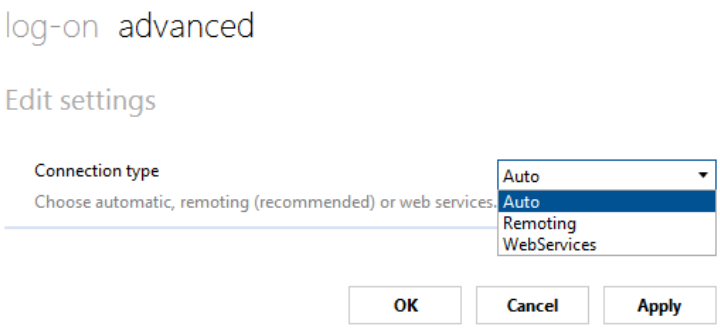


Figure 3–2. Select a Connection Type

2. Set the **Connection type** to either **Remoting** (TCP:8004) or **WebServices** (TCP:9004).
3. If necessary, change the related settings (*Destination port*, *Polling interval*, etc.).

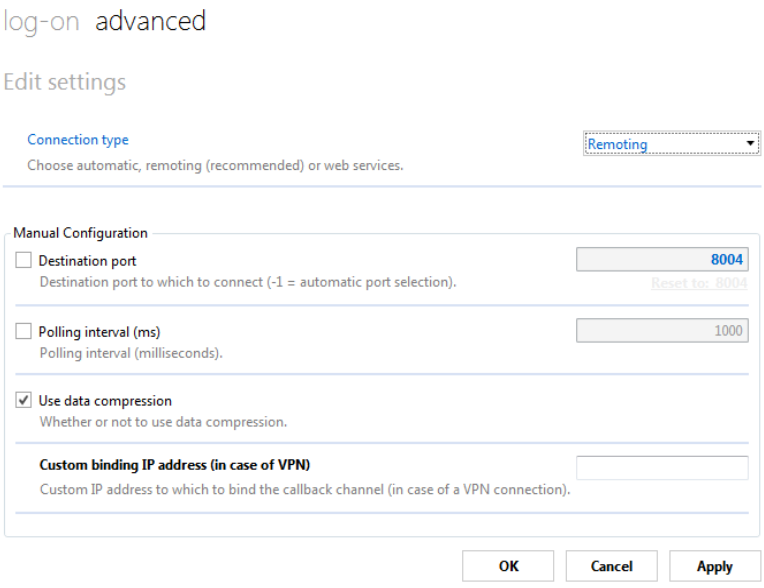


Figure 3–3. Edit Settings

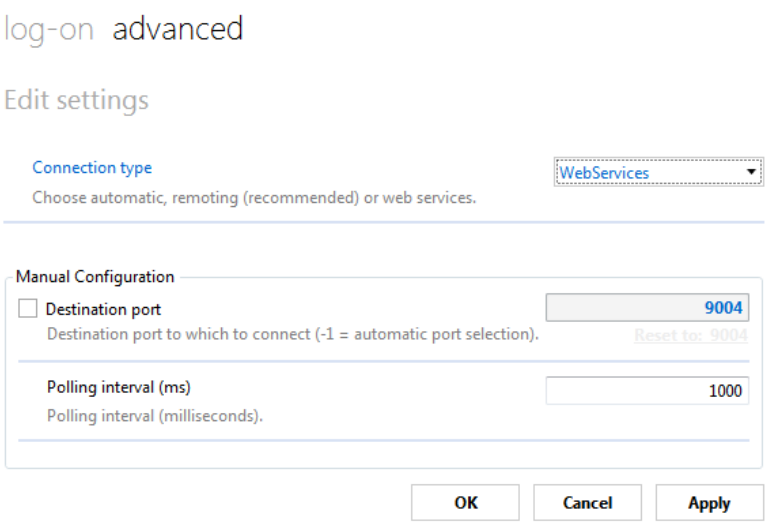


Figure 3–4. Log–on Advanced Window

4. Click **OK**.

3.1.1.3 Log off from NetVue Cube

- In the header bar, click the name of the logged–on user.
- At the top of the Contacts window, click **Log off**.

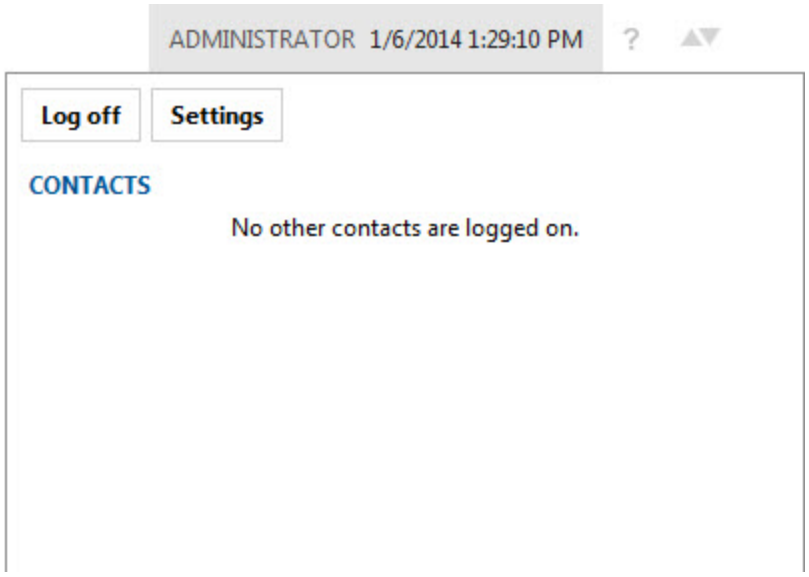


Figure 3–5. Cube Log Off

3.1.2 Navigate the NetVue Cube User Interface

The NetVue Cube user interface has these sections:

- Header bar
- Navigation pane
- Card pane
- Alarm console

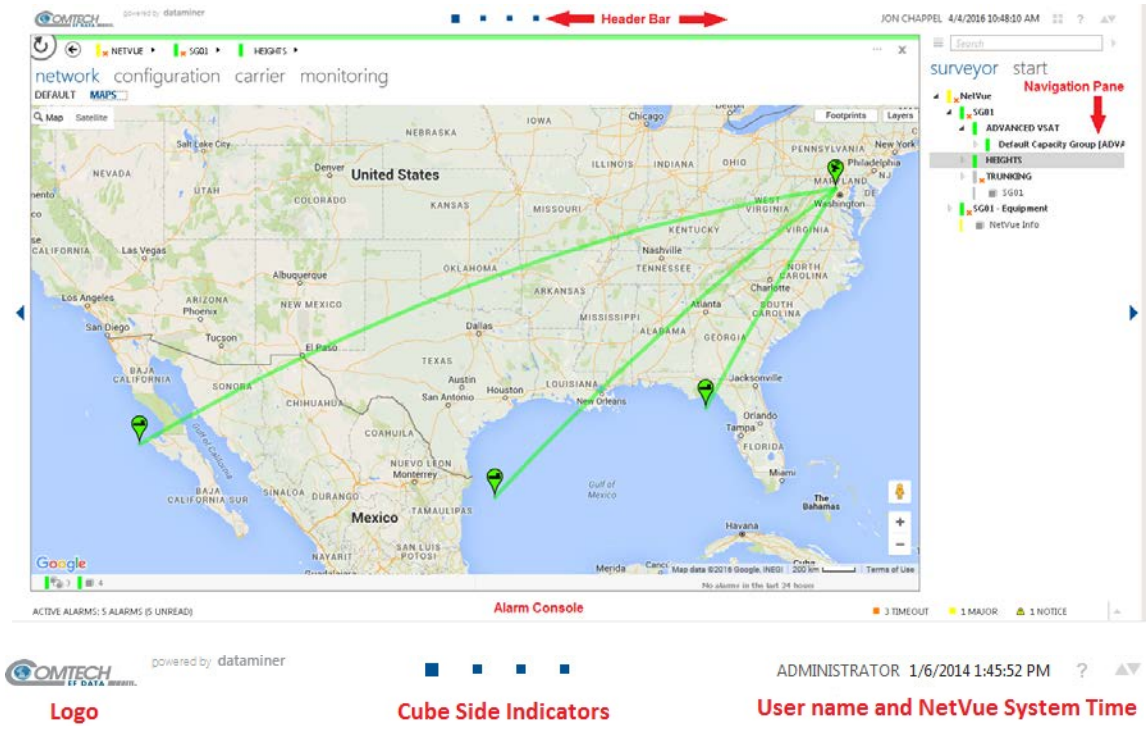


Figure 3–6. Cube Navigation

3.2 Get Started with the NetVue Cube Interface

3.2.1 NetVue Cube Header Bar

Figure 3–7. Cube Header Bar

The header bar of the NetVue Cube has these items:

Cube Side Indicators

Four blue squares, each represents one of the four Cube sides. A large square marks the Cube side that is displayed currently. Click a square to switch to a particular Cube side.

Figure 3–8. Cube Side Indicators

User Name and Time

This is the name of the logged–on user, followed by the NetVue System time. The NetVue System time is synchronized among all NetVue Servers in the cluster.

Figure 3–9. User Name/Time

1. Click to open the **Contacts** window, which allows you to exchange chat messages with other users of your NetVue System.
2. Click and select **Log off** to end your current NetVue Cube session.
3. Click and select **Settings** to open the **Settings** app.
4. Click and select **My account** to open your user card.

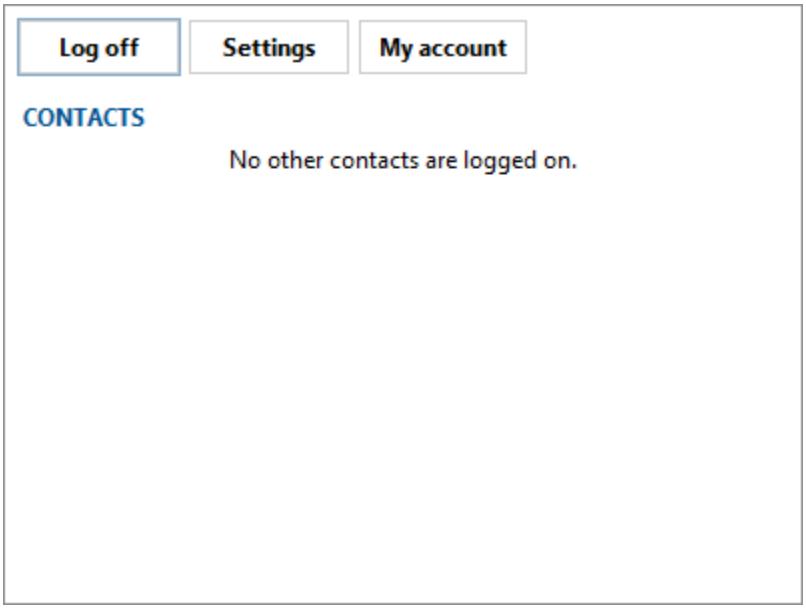


Figure 3–10. User Options

Card Layout Icon

Use this icon to change the layout of the cards in the Cube.

Figure 3–11. Card Layout Icon

Question Mark

Use this icon to get access to the online help and the *About* box.

Figure 3–12. Question Mark

NetVue Help/About Screen

1. Click and select **Help** to view the NetVue online help.
2. Click and select **About** to view the About box. This box has several tabs, and three buttons:
   - The **general** tab shows the upgrade version of your NetVue Server.
   - The **assemblies** tab shows the assemblies used by your NetVue Server.
   - The **connection** tab shows information about the connection of client to server.
   - The **versions** tab shows the server and client version, as well as the version of the various NetVue files and the NetVue Server upgrade history.
   - The **license** tab shows license information and activated license counter information.
   - The buttons at the bottom of the box allow you to export, email or copy the information for troubleshooting purposes.

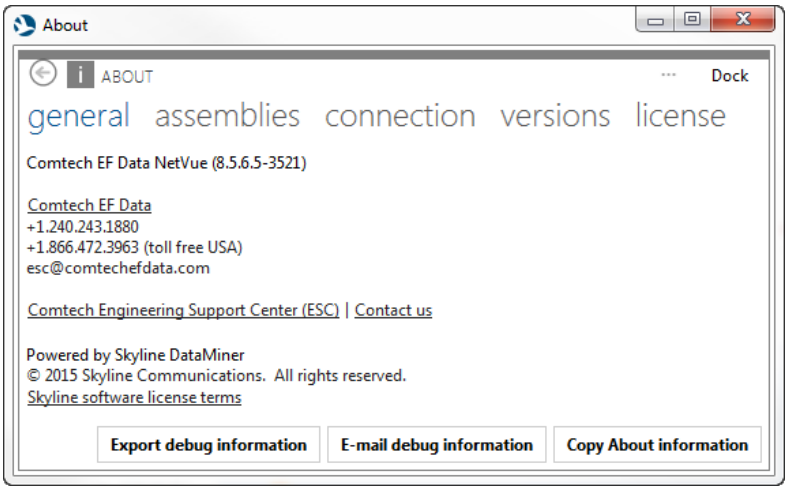


Figure 3–13. Help / About Screen

Client Communication Indicator

This icon shows the communication streams between the NetVue Server and the NetVue Cube application.

Figure 3–14. Communication Indicator

The up arrow on the left is blue when messages are sent from the client application to the NetVue Server.

The down arrow on the right is blue when messages are sent from the NetVue Server to the client application.

Click the icon to see all connected NetVue Servers, grouped per cluster, along with their status.

In that list, the right–click menu allows you to start, restart, stop, shut down, reboot or upgrade a NetVue Server. You can get access to the **NetVue redundancy** window, as well. The **System Center** and **Agents** buttons give quick access to the system configuration.

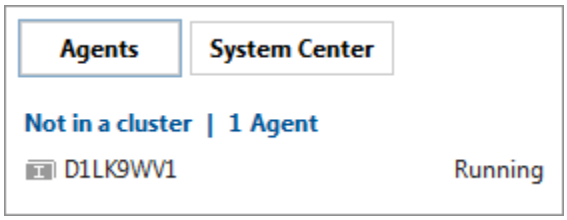


Figure 3–15. Agents Information

3.2.2 NetVue Cube Navigation Pane

Use the navigation pane to open views, services and elements using the **Surveyor** or the **Recent** list. Use it to open NetVue add–on modules and manage NetVue Cube Workspaces as well.

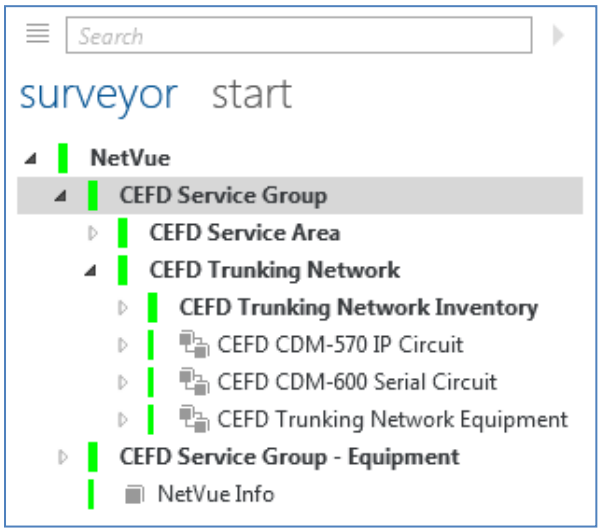


Figure 3–16. Navigation Pane

3.2.2.1 Location of the Navigation Pane: Left or Right

By default, the navigation pane is on the right–hand side of the screen.

- To move it to the left–hand side of the screen, click anywhere inside the pane and press **Ctrl+Alt+Shift+LeftArrow**.
- To move it to the right–hand side of the screen, click anywhere inside the pane and press **Ctrl+Alt+Shift+RightArrow**.

You can specify the default location of the navigation pane in **Settings > User > Surveyor Docking Position**.

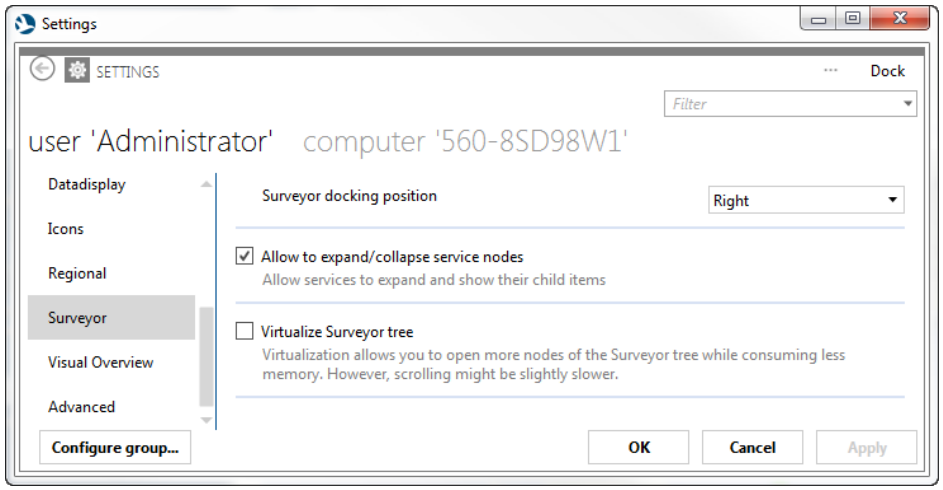


Figure 3–17. Surveyor Position

3.2.2.2 Surveyor

The Surveyor tab contains a hierarchical overview of your NetVue system: all views, elements, services, etc. It includes alarm bubble–up, state indication and more.

When you click an item in the tree, it opens in a card:

- If you click the item with the left mouse button, the new card replaces a card that is open already.
- If you click the item with the middle mouse button, a new card opens next to any cards that are open already.

3.2.2.3 Icons

The icons that precede an item name in the tree show what kind of item it is and its state and alarm conditions. Each type of item has a different icon:

Table 3–1. Icons

Icon	Description
	Element
	Protocol
	Redundancy Group
	Script
	Service
	Service Template
	SLA
	Template Group
None	View

Icons are preceded by a colored bar that shows the item's alarm state. In addition to the default colors showing the alarm severity, the colors listed in Table 3–2 are possible.

Table 3–2. Additional Alarm States

Color	Description
Gray	There is no alarm monitoring for this item.
Purple	The item is masked.
Orange	The item is in a timeout state.

The color showing is that of an item's most severe parameter alarm in effect currently.

There can be additional symbols on an icon to indicate a particular state:

Table 3–3. Additional Symbols

Symbol	Description
	Black square located in the corner of an icon to indicate that the item is stopped.
	"Pause" symbol located in the corner of an icon to indicate that the item is paused.
	Orange x indicates that an element in a view or service is in a timeout state.

3.2.2.4 Surveyor Right–Click Menu

In the Surveyor right–click menu, the options listed in Table 3–4 are available, depending on what type of item is right–clicked.

Table 3–4. Right–click Menu

Menu Option	Right–Click Item	Description
Expand all in alarm	View only	Expands all subviews with an active alarm
Collapse level	View only	Collapses the level of the right–clicked view
Open	Any	Opens the item in a card
Open in new card	Any	Opens the item in a new card
Open in new undocked card	Any	Opens the item in a new, undocked card
Status	Element only	Opens a shortcut that allows you to change the element state
Mask	Element only	Masks the element
Unmask	Element only	Unmasks the element
Multiple Set	Element only	Opens the *Multiple set* dialog box
View	Element, Service	Opens a shortcut menu that allows quick access to the protocol, alarm template or trend template of the element or service
Edit	Element, Service	Opens a card where you can change the settings of the element or service
Remove from parent	Any except view	Moves the item from the parent view to the root view
Delete	Any except root view	Removes the item
Duplicate	Element, Service	Duplicates the item
Rename	Element, Service, View	Allows the user to rename the item
New	Any	Opens a submenu where you can select to create a new element, service, service template or SLA. If you right–clicked a view, you can also select to create a new view.
Actions	Element, Service, View	Opens a shortcut menu with options to configure personal alerts, start Correlation analyzers, and other options depending on the right–clicked item
Properties	Element, Service, View	Opens the item's *Properties* window
Drag and drop editing	Any	Enables drag–n–drop view editing mode

3.2.2.5 Recent

1. Click **Start > Recent** to go to the list of recently viewed items.
2. Click an item in the list to open it in a card.

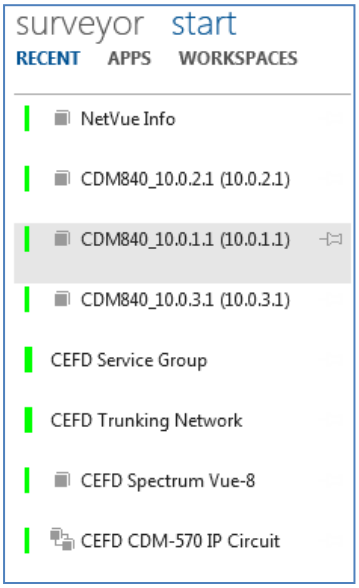


Figure 3–18. Recent List

If you hold the mouse cursor over an item, a small pin appears to the right of the item.

To fix the item to the list, click the pin. If you fix the item to the list, the item moves to a separate section at the top of the list. It stays there until you unpin it.

To unpin the item, click the pin again. The item moves back to its original position in the list.

3.2.2.6 Apps

Click **Start > Apps** to go to the list of installed, add–on modules known as *apps*.

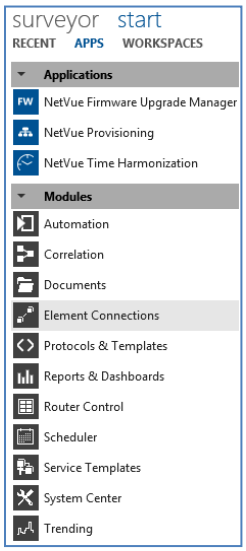


Figure 3–19. Apps

Open any app in the list by clicking it.

3.2.2.7 Workspaces

Click **Start > Workspaces** to go to the list of available Workspaces.

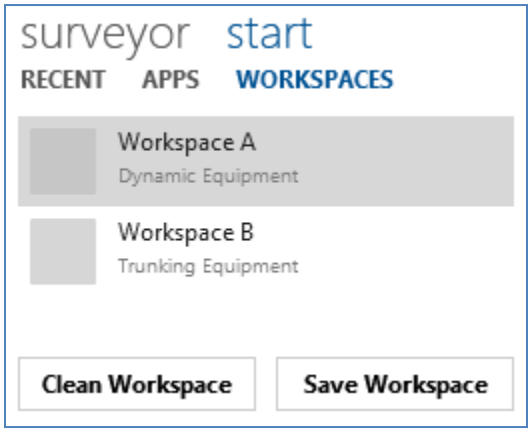


Figure 3–20. Workspaces

3.2.3 NetVue Cube Card Pane

When you click an item in the Surveyor, or when you right–click an alarm in the Alarm Console and select **Open Alarm Card**, the details of that item or that alarm are shown in a special window called a *card*.

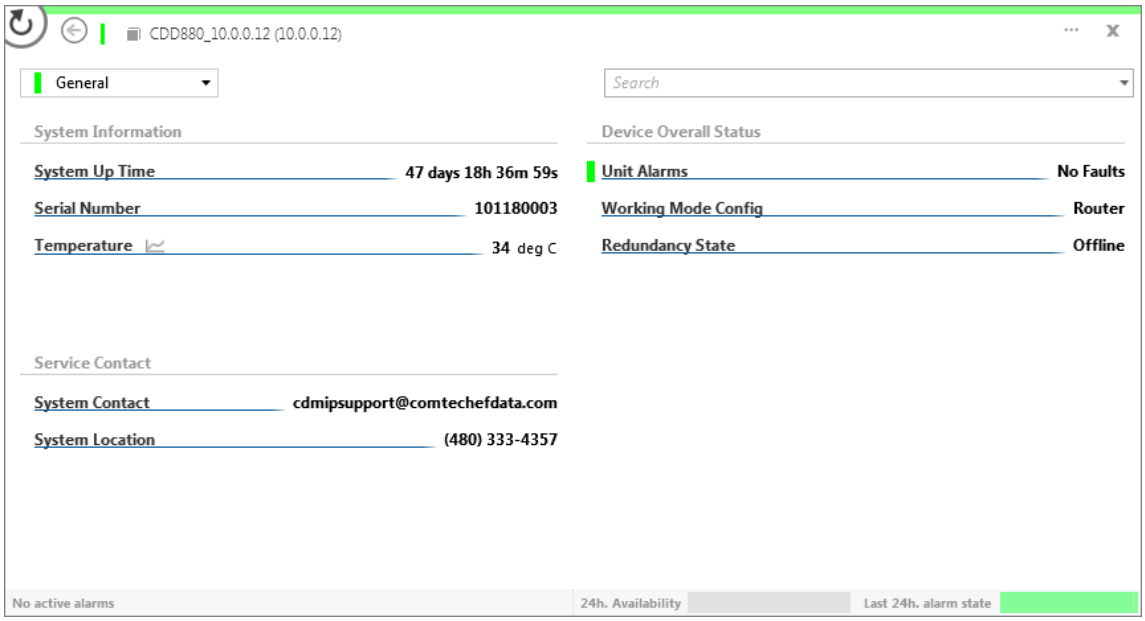


Figure 3–21. Card Pane Example

3.2.3.1 Card Types

There are several, different types of cards:

- Element cards
- Service cards
- View cards
- Alarm cards
- User cards
- Spectrum analyzer cards
- And more...

3.2.3.2 Card Sides

Each card has a front and a back. Both the front and back of the card can have several pages.

If a card opens on a particular page, and you open another card; then the second card opens automatically on the page most similar to the page opened on the first card.

The front of the card shows a visual overview. This is a Microsoft Visio drawing depicting a graphical view of the selected item.

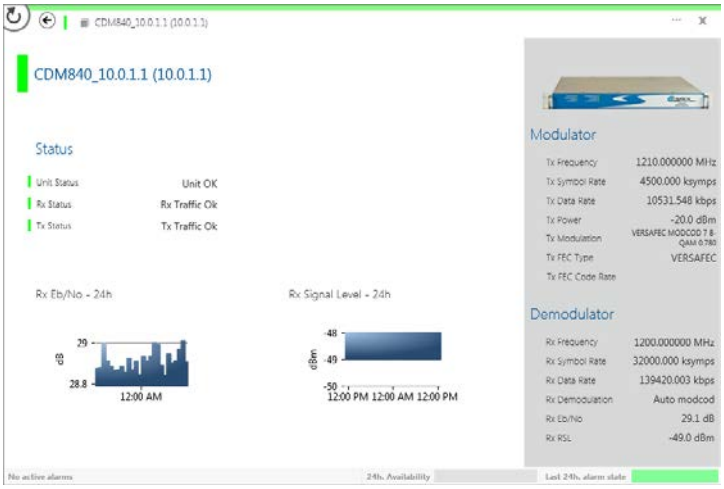


Figure 3–22. Front Side of Card

The back of the card shows all data associated with the selected item.

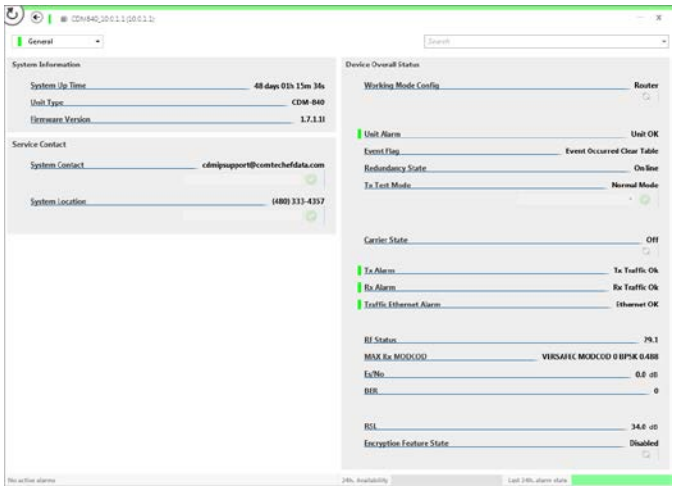


Figure 3–23. Back Side of Card

3.2.3.3 Work with Cards

3.2.3.3.1 Open Cards

By default, if you left–click cards, each new card replaces the previously opened card. You can then navigate among the cards with the **Back** and **Forward** commands.

However, you can also open items in a new card next to any cards that are already open. To do this:

- Click an item with the middle mouse button in the Surveyor or on a view card.
- Hold **Ctrl** when you click an item in the Surveyor.
- Select **Open in new card** in the item's right–click menu.

There is a limit to the number of cards, docked or undocked, that can be open on each side of the cube. By default, this number is 16, but you can change it in the user settings.

If you try to open more cards, a message tells you that the maximum number has been reached, and you must first close a card to continue.

3.2.3.3.2 Change the Card Layout

There are several ways to get access to the card layout options:

- Right–click the card header bar and select **Card Layout**.
- Click the … button in the top right corner and select **Card Layout**.
- Click the card layout icon to the right of the user name and NetVue time in the Cube header bar, and select the card layout you want.
- To change the card layout on the fly, drag the edge of the card to adjust its size.

Table 3–5 lists the available layout options.

Table 3–5. Card Layouts

Layout	Description
Proportional	The sizes of the displayed cards are adapted so that they all have the same size.
Master left	One large card on the left is the master. All other open cards show to its right, in proportion.
Master right	One large card on the right is the master. All other open cards show to its left, in proportion.
Master top	One large card at the top is the master. All other open cards show below it, in proportion.
Master bottom	One large card at the bottom is the master. All other open cards show above it, in proportion.
Tab layout	The different open cards show in a row of tabs at the top of the screen. Click a tab to switch to that card.
Reset card layout	Resets any card layout changes that were made manually. The cards return to the size set by the selected card layout.

3.2.3.3.3 Drag Cards

You can drag a card to its destination by left–clicking and dragging the colored header bar.

You can drag a card if:

- More than one card is open, to make the cards switch places. This can be useful in a Master/Detail card layout, to change which card is the master.
- A maximized card is open above other cards, to drag the maximized card aside and see what is behind it.
- You want to undock a card by dragging it out of the workspace.

3.2.3.3.4 Undock Cards

There are several ways to undock cards:

- Drag an open card out of the workspace.
- Hold **Shift** when you click an item in the Surveyor.
- Select **Open in new undocked card** in an item's right–click menu.

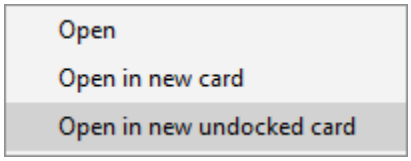


Figure 3–24. Undock Card

By default, the undocked window opens in the middle of your screen, unless you undocked the card by dragging it.

If you open a different card from inside an undocked card, it replaces the undocked card in the same window.

3.2.3.4 Header Bar Buttons

At the top of each card, there are several buttons:

Table 3–6. Header Bar Buttons

Button	Description
	*Go to front/Go to back* button in the top left corner, use it to flip a card. To flip all open cards, shift–click the button.
	*Back* button to the right of the flip card button, use this button to go back to a previous card, if possible.
	Options button in the top right corner of a card, gives access to a shortcut menu that has several commands.
	*Maximize/Restore* button, use it to maximize the card in the workspace, or restore it to its previous state.
	*Close* button, use it to close the card. Shift–click the *Close* button to close all open cards.

3.2.3.5 Header Bar Shortcut Menu

If you right–click in the colored bar at the top of the card, or click the button in the top right corner, an Options menu opens.

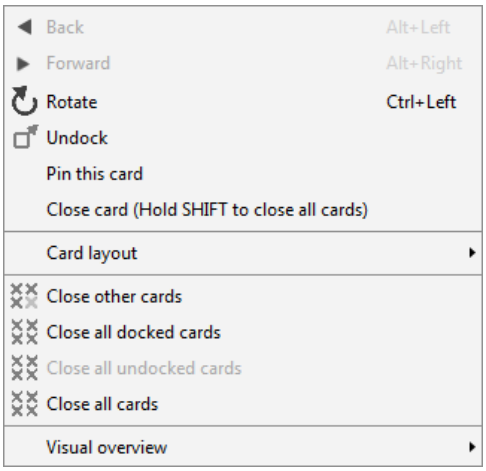


Figure 3–25. Options Menu

- **Back:** Goes to the previous open card.
- **Forward*:*** Goes to the next open card.
- **Rotate*:*** Flips the card from the visual overview side to the data side, or vice–versa.
- **Undock*:*** Opens the card in a separate, undocked window; at the bottom of the window is an Alarm Console filtered to apply to that card only.
- **Pin this card*:*** Select this option to keep the card opened in the same position when other cards are opened. To unpin the card, click this option again.
- **Close card*:*** Closes the applicable card.
- **Card layout*:*** Offers several choices for the layout of the cards in your workspace.
- **Close other cards*:*** Closes all cards, except the one you have clicked.
- **Close all docked cards*:*** Closes all cards that opened in the main Cube window, but not in a separate window.
- **Close all undocked cards*:*** Closes all cards that opened in a separate window.
- **Close all cards*:*** Closes all cards.

3.3 NetVue Cube Alarm Console

Chapter 9. ALARMS

The Alarm Console is the section of the NetVue Cube user interface that allows you to see and manipulate active alarms, historical alarms and information events.

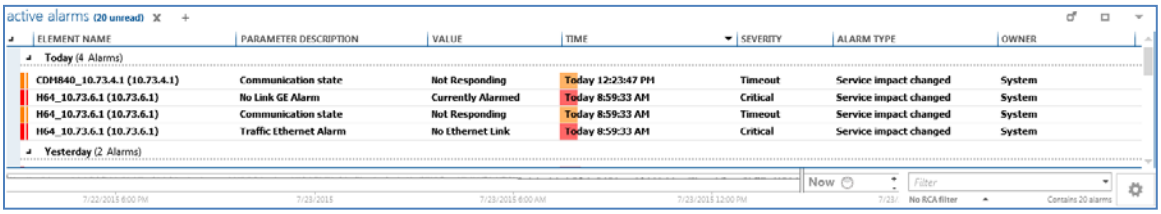


Figure 3–26. Alarm Console

For more information on how to use the Alarm Console, see **Chapter 9. ALARMS**.

3.4 Search in NetVue Cube

If you want to search for an item throughout your NetVue System, enter a word, or at least three characters, in the search box at the top of the Navigation pane.

With every character you type, search results show in the Navigation pane. The results are grouped by item type (elements, services, views, protocols, parameters, etc).

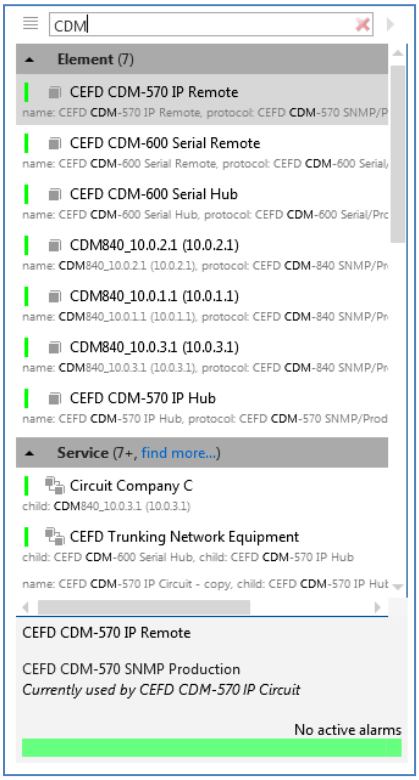


Figure 3–27. Search

Browse through the results by scrolling, or by using the **Up** and **Down** keys. When you select an item in the list, basic information about the item shows at the bottom of the Navigation pane.

1. Select an item and press **Enter**, or click an item to open it in a card.
2. Click an item with the middle mouse button to open the item in a new card, next to any existing cards.
3. To clear the search box and erase the list of search results, click the red X on the right.

3.4.1 What to Enter in Search Box

To search for an **element**, enter any part of these items:

- An element name
- A protocol name
- A protocol version
- An alarm template name
- A trend template name
- An element description
- An alarm severity (e.g., critical, etc.)
- An element property shown in Surveyor

To search for a **service**, enter any part of these items:

- A service name
- A service description
- A name of a child element or child service
- An alarm severity (e.g., critical, etc.)
- A service property shown in Surveyor

To search for a **redundancy group**, enter any part of these items:

- A redundancy group name
- A redundancy group description

To search for an **element parameter**, enter any part of these items:

- A display name
- An element name
- A protocol name
- A protocol version
- A row display key (for columns, only if one of other criteria matches a column parameter)

To search for a **user**, enter any part of these items:

- A logon name
- A full name

To search for a **user group**, enter any part of this item:

- A group name

To search for a **view**, enter any part of these items:

- A view name
- A view property displayed in Surveyor

To search for a **protocol**, enter any part of these items:

- A protocol name
- A protocol version

To search for a **document**, enter any part of these items:

- A document title
- A document description
- A file name

3.4.2 Special Search Options

To search for items that do not match a specific search term, put an exclamation mark in front of the search term. This is known as a negative search.

- Example: !redundancy

To search for an exact phrase of several words, surround the phrase by double quotes.

- Example: “CEFD CDM–570L”

In the search box, special search options show in meaningful colors:

- Negative search terms are **red**
- Special search keywords are **blue**
- Strings surrounded by quotes are **gray**

Table 3–7 lists special keywords you can use with a search term, separated from the term with a space.

Table 3–7. Special Search Options

Enter	Results
trend	elements that have been assigned trend templates as well as trended parameters
trending	
trended	
monitored	only elements and parameters that are being monitored
alarm	
inalarm	only elements and parameters of which the state is not equal to “normal” or “undefined”
online	only users who are currently logged in
element	only elements
elements	
view	only views
views	
service	only services
services	
servicetemplate	only service templates, listed in the search results under “Services”
servicetemplates	
parameter	only parameters
parameters	
redundancy	only redundancy groups

Enter	Results
user	only users
users	
usergroup	only user groups
usergroups	
protocol	only protocols
protocols	
document	only documents
documents	
critical	only elements, services and parameters with the specified alarm severity
major	
minor	
warning	
timeout	
normal	
masked	

3.4.3 Search with Wildcard Characters

You can use these wildcard characters:

- * which represents 0 or more characters
- ? which represents one character

Examples:

*Washington**

- Matches …
  - Washington–HPA–1
  - Washington–HPA–2
- Does not match …
  - NewYork–HPA–1
  - DC–Washington–HPA

Washington–HPA–?

- Matches …
  - Washington–HPA–1
- Does not match …
  - Washington–HPA–22

**–HPA–?*

- Matches …
  - Washington–HPA–1
  - NewYork–HPA–1

3.5 Use Quick Filters in NetVue Cube

You will often find filter boxes in the NetVue Cube that you can use to filter the displayed data. Filter boxes can be at the top of a card, above a table or in the Alarm Console.

Figure 3–28. Quick Filter

Some tips on the use of quick filters:

- The filter box is a combo box. You can type in it, or click the down arrow on the right side of the box to choose from a list of suggestions. Depending on where you are using the filter box, you might have to type a few characters before suggestions show.
  A filter box keeps a history of past searches. These show underneath the suggestions. By default, the history keeps 10 items maximum. You can change this number in the user settings.
- To filter more effectively, you can use wildcards in filters.
- To create a negative filter, use an exclamation mark. Example: !warning.
- To use comparisons in the filter, use the greater than or smaller than symbols. Example: “Service Impact”>1
- To search for an exact combination of characters, enclose them in double quotation marks.
- To search in a specific column when using a table filter, enter the name of the column followed by a colon, and then the value you wish to search for (column:value).
- To search for a value followed by a colon, enclose the search term in double quotation marks.
- To deactivate the filter, click the red X in the filter box.

3.6 Work with NetVue Cube Workspaces

Click **Start > Workspaces** to go to the list of available **Workspaces** (see Figure 3–20).

A Workspace is a saved Cube screen layout. If you use the same set of cards often, try saving the set in a Workspace. Any time you open the Workspace, those same cards open immediately in the layout you saved.

The saved layout can include apps, such as a dashboard, and undocked alarm tabs, but not the position of the entire alarm console. If a page was selected on the data display side of cards, this is saved in the Workspace also.

You can do these tasks in the **Workspaces** tab of the navigation pane:

- To open a Workspace, click a Workspace in the list.
- To open a Workspace in a new, undocked window, right–click a Workspace in the list and select **Open Workspace in undocked window.**
- To delete a saved Workspace, right–click the Workspace in the list and select **Delete Workspace.**
- To rename a Workspace, right–click the Workspace in the list and select **Rename Workspace.**
- To change the description of a Workspace, right–click the Workspace in the list and select **Edit description.**

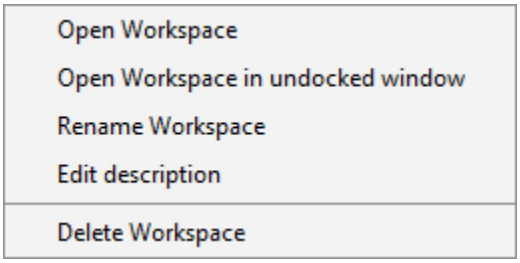


Figure 3–29. Workspace Right–Click Options

- To close all open cards, at the bottom of the list, click **Clean Workspace.**
- To create a workspace containing all open cards:
    1. At the bottom of the list, click **Save Workspace**.
    2. In the **Name** field, enter the name of the Workspace.
    3. If the workspace is to be used for items that do not always have the same ID, but do always have the same name, select **Select the name of the open cards**.

Figure 3–30. Clean/Save Workspace

3.7 NetVue Cube User Settings

You can change many settings in NetVue to your preferences. Do this in the **Settings** window.

There are two ways to get access to the user settings in the NetVue Cube:

1. Click **Start > Apps > Settings**.

Figure 3–31. User Settings (Apps)

2. Click the current user in the top–right corner of the screen, and click **Settings**.

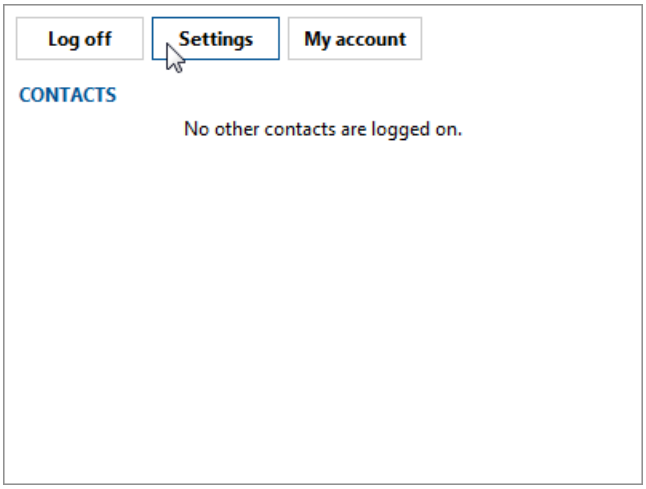


Figure 3–32. User Settings (top–right)

The window has two tabs. The tab with the user settings opens by default. It consists of 11 pages that you can navigate with the table of contents on the left.

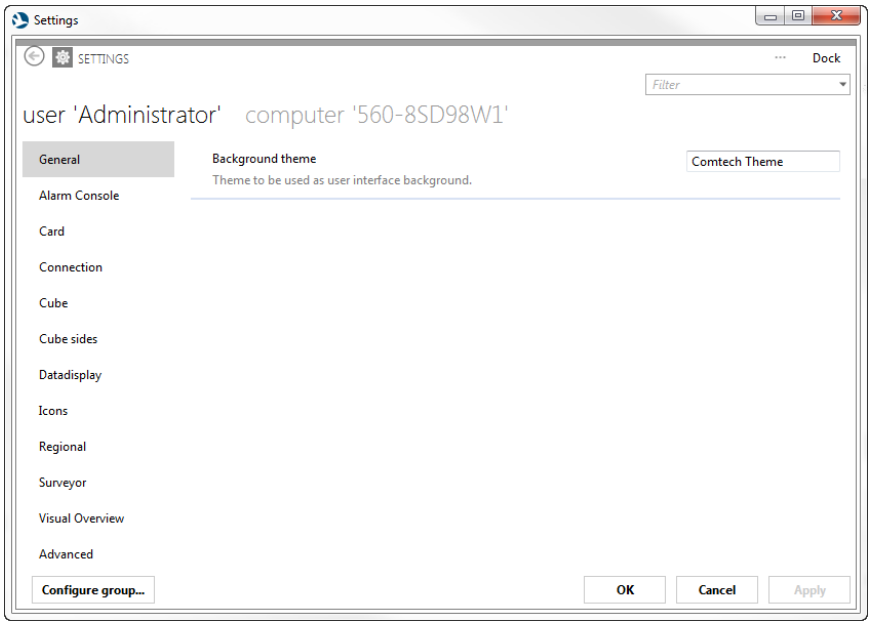


Figure 3–33. User Settings Page

3.7.1 General Settings

In the **General** page, you can set the background theme for the NetVue Cube; for example, Comtech theme.

3.7.2 Alarm Console Settings

In the **Alarm Console** page, several settings are possible:

- **Display Alarm Console group statistics:** When this setting is selected, and the grouping feature is enabled in the Alarm Console, group statistics will be shown next to each group title.
- **Display horizontal scrollbar in the alarm list:** Select this setting to show a horizontal scrollbar in the Alarm Console. This can be useful when many columns have been added in the list in the Alarm Console.
- **Alarm Console time format:** Select **Time/Yesterday** to use the numeric date format only for dates earlier than yesterday, or select **Full date** to always show the complete date in numeric format.
- **Time before alarm banner hides:** Select this setting to set a delay of 30 seconds before the alarm banner hides. To set a different delay, select the setting and enter a different number of seconds in the box on the right.
- **Enable alarm storm prevention:** Select this setting; in the boxes on the right, configure the number of alarms to start and stop the alarm storm.
- **Filter the alarms before they enter Cube:** Select this setting and then select one of the existing alarm filters in the drop–down list to use it as a sever–side alarm filter. When you do so, the **Active alarms** tab of the Alarm Console will list alarms that only match this filter.
- **Configure Alarm Console:** With this setting, you can configure the tabs in the Alarm Console for the different sides of the Cube.

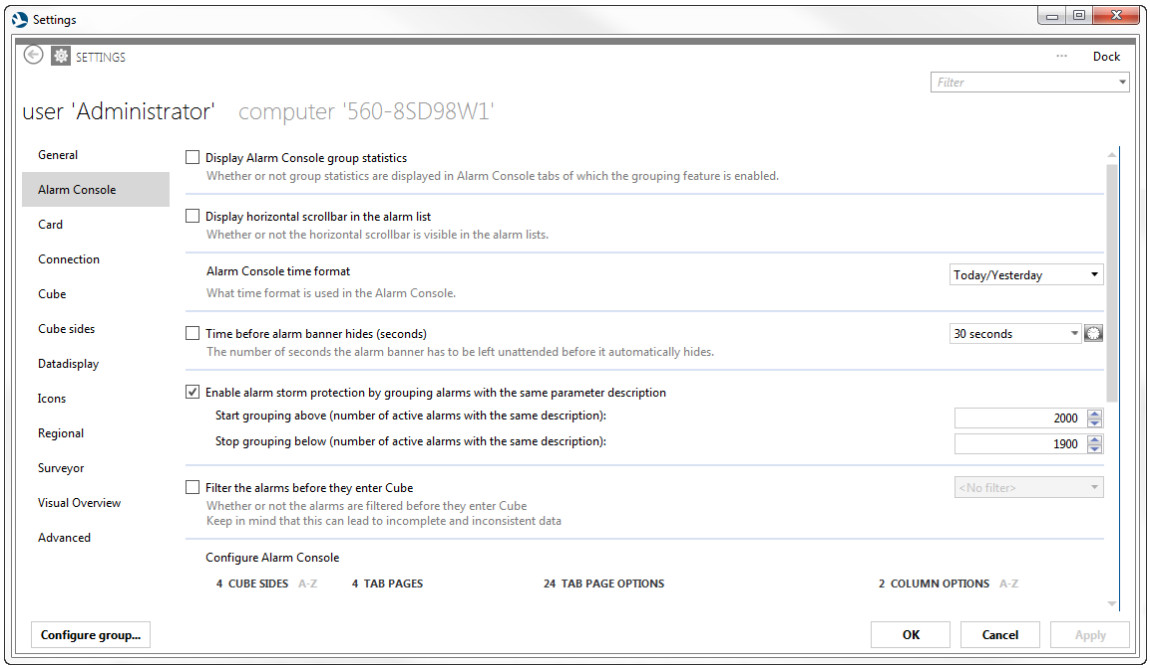


Figure 3–34. Alarm Console Settings

3.7.3 Card Settings

In the **Card** page, several settings are possible:

- **Open Element Cards undocked*:*** Select this setting to open element cards in a new, undocked window. The setting is applicable to parameter cards as well.
- **Default View/Element/Service/Card side*:*** With these settings, you can choose which side of view, element and service cards show when you open them. By default, this is the visual overview side. It is also possible to show the side that was last visible when the card was closed, or to show the visual overview side only if a Visio file has been assigned.

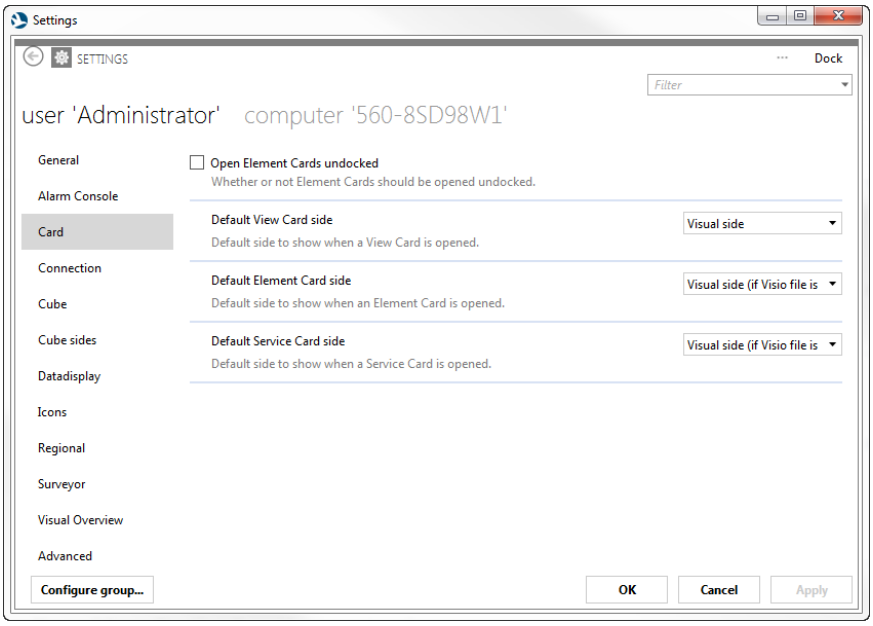


Figure 3–35. Card Settings

3.7.4 Connection Settings

In the **Connection** page, two settings are possible:

- **Time before automatic disconnect (minutes)*:*** Select this setting to enable automatic disconnection when the NetVue Cube is left unattended for some time, and fill in the number of minutes after which you want automatic disconnection to occur.
- **Automatic reconnect after connection loss*:*** Select this setting to ensure that the NetVue Cube will automatically reconnect after a connection has been lost.

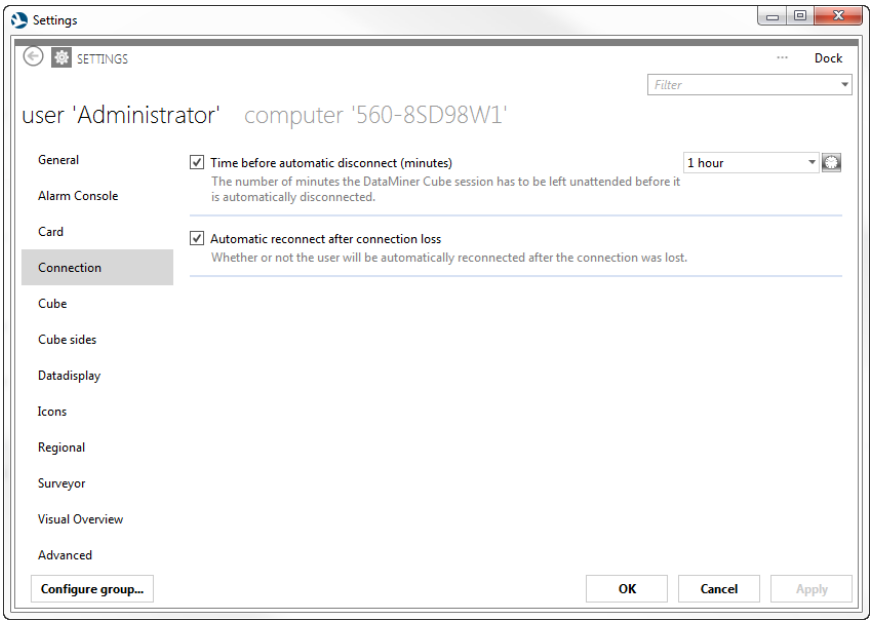


Figure 3–36. Connection Settings

3.7.5 Cube Settings

In the **Cube** page, two settings are possible:

- **Never ask for confirmation after setting parameter value:** When you select this setting, no confirmation boxes show when a parameter value is set.
- **Do not show compatibility warnings for Visio drawings:** When you select this setting, no compatibility warnings occur when you open a Visio file; for example, when you open a VDX file in a recent version of MS Visio.

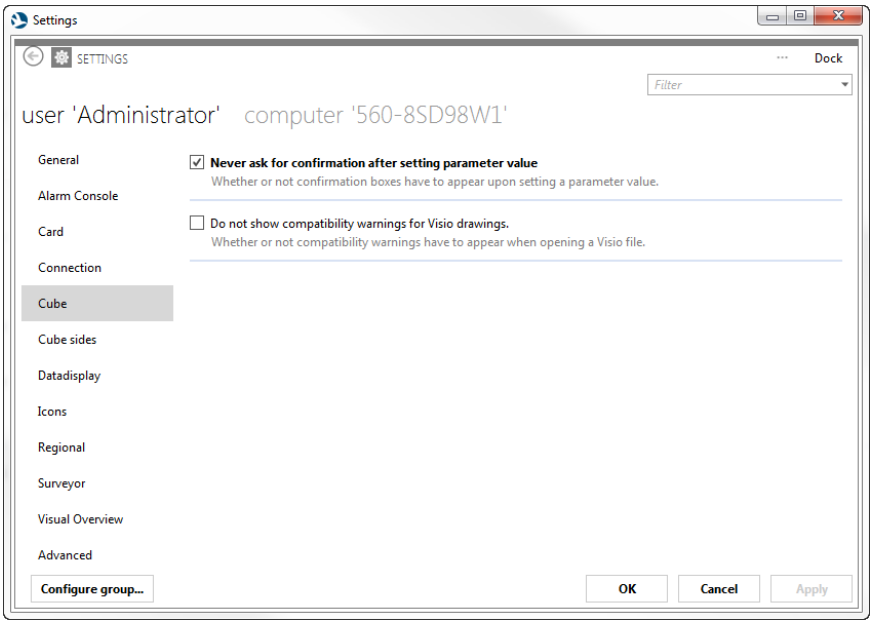


Figure 3–37. Cube Settings

3.7.6 Cube Sides Settings

In the **Cube sides** page, you can change the settings for each side of the Cube:

- **Default Workspace*:*** The workspace that loads when the NetVue Cube is started.
- **Background theme*:*** The background theme for the separate sides of the Cube.
- **# Cards*:*** The maximum number of cards that can be opened on a side of the Cube.

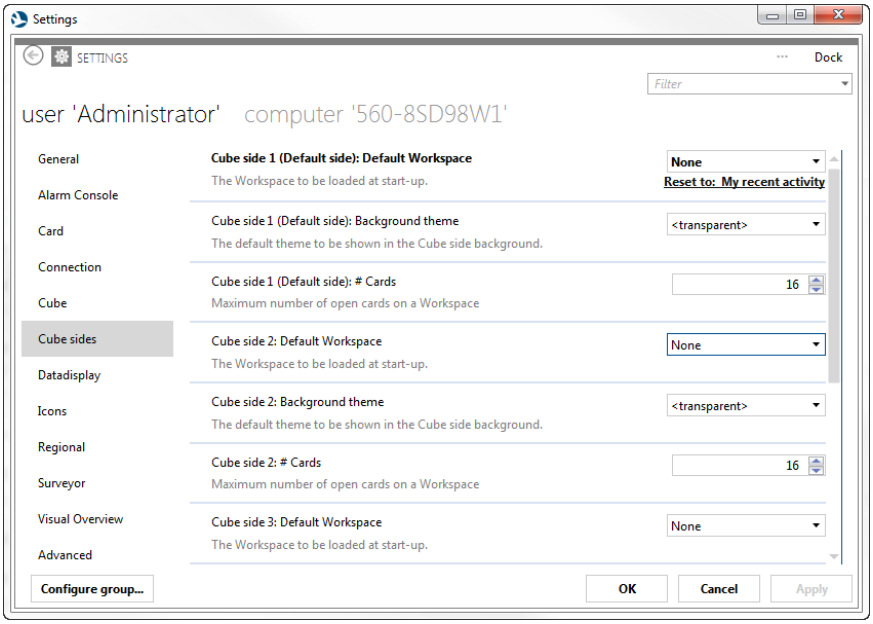


Figure 3–38. Cube Side Settings

3.7.7 DataDisplay Settings

In the **Datadisplay** page, several settings are possible, some of which are only applicable for Lite mode.

- **Page Selection Mode*:*** To change the way you can navigate to different pages on a card, choose between **Combobox** and **Treeview** in the drop–down list.
- **Parameter Display Mode*:*** With this option, you can choose whether to see parameter controls in **Normal** mode or **Lite** mode. When you select Lite mode, parameters show in a more compact way. Several options to customize the way parameters are shown are also available for Lite mode.
- **Analog Display Mode*:*** Only available in Normal mode. This setting allows you to choose whether analog parameters show with an LED bar or an oscilloscope.
- **Parameter Title Font*:*** Only available in Lite mode. With this setting, you can change the title font for parameters.
- **Parameter Value Font*:*** Only available in Lite mode. With this setting, you can change the font for parameter values.
- **Parameter Value Alignment*:*** Only available in Lite mode. With this setting, you can set whether the parameter values are aligned on the left or on the right.
- **Always show editor controls*:*** Only available in Lite mode. Select this setting to show the write controls for parameters.
- **Outer margin*:*** Only available in Lite mode. Enter 1, 2 or 4 values, separated by commas, to set the outer margin between parameters.
- **Inner margin*:*** Only available in Lite mode. Enter 1, 2 or 4 values, separated by commas, to set the inner margin between parameters.
- **Show General Parameters debug page*:*** Select this setting, along with the computer setting **Debug settings visible**, to show an additional DataDisplay page called **General parameters DEBUG**. This page contains all the general parameters that are not visible typically.
- **Trend Y axis mode*:*** Select **Auto** to optimize the vertical range of a trend graph automatically during pan and zoom operations. Select **Range** to fix the vertical range to the minimum and maximum defined in the protocol.
- **Trend Y axis includes exceptions*:*** Only applicable when the trend Y–axis mode has been set to **Range**. Select this setting to allow the vertical range of the Y–axis to extend with exception values.
- **Show alarm template colors on vertical axis*:*** Enable this setting to show the alarm colors next to the vertical axis of trend graphs. The setting **Display the alarm template in the trend graph** allows you to specify how the alarm colors are displayed.
- **Display the alarm template in the trend graph*:*** In the drop–down list next to this setting, choose **Line** to show alarm template colors as a small line next to the Y axis, or **Band** to show them as semi–transparent horizontal bands across the trend graph.
- **Show most detailed data:** If you select this option, the most detailed data available is shown, instead of average data. To ensure optimal performance in case a large amount of trend data must be displayed, this option is by default not selected.
- **Enable heat map on table parameters:** Enable this setting to give table cells with numeric parameters a background color intensity that matches their value.
- **Enable histogram link on table column parameters:** Enable this setting to show a link in the column headers of table parameters, which shows a histogram with the spread of the column values.

- **Enable Header Sum on table column parameters:** Enable this setting to show an extra label in the column header of table parameters, which indicates the sum of the column values.
- **Maximum number of items kept in the table parameter filter history:** To set the number of items kept in the filter history of filter boxes for table parameters, enter a value in the box for this setting.

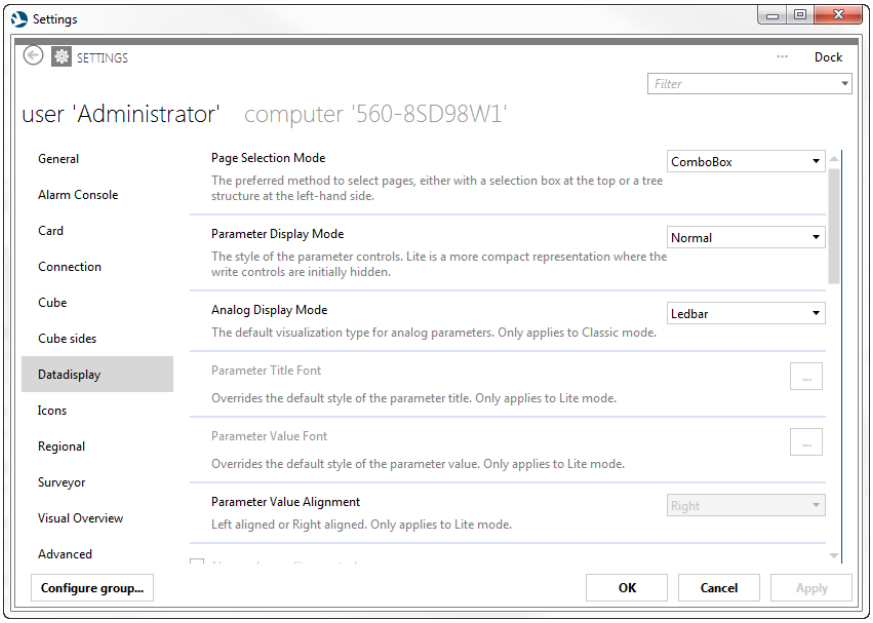


Figure 3–39. Data Display Settings

3.7.8 Icon Settings

Use these settings to specify which alarm levels and icons show next to the icons of views, services and elements in the NetVue Cube user interface.

- **View alarm level*:*** In the drop–down list next to this setting, choose either **Consolidated** to show the alarm level of all child items, or **Split** to show the alarm level of the first–level child items on the left and the alarm level of the child items on the deeper levels on the right.
- **View latch level*:*** In the drop–down list next to this setting, choose either **Show** to show the latch level for views, or **Hide** to hide it.
- **View aggregation level:** With this option, aggregated alarms on views show with a triangle next to the colored bar to indicate the view alarm level. In the drop–down list next to this setting, choose either **Show** to show this triangle, or **Hide** to hide it.
- **Element alarm level:** In the drop–down list next to this setting, choose either **Separate from timeout** to show a timeout icon and the last–known alarm level, or **Timeout overrules** to show a timeout icon and the timeout color.
- **Element latch level:** In the drop–down list next to this setting, choose either **Show** to show the latch level for elements, or **Hide** to hide it.
- **Service latch level:** In the drop–down list next to this setting, choose either **Show** to show the latch level for services, or **Hide** to hide it.

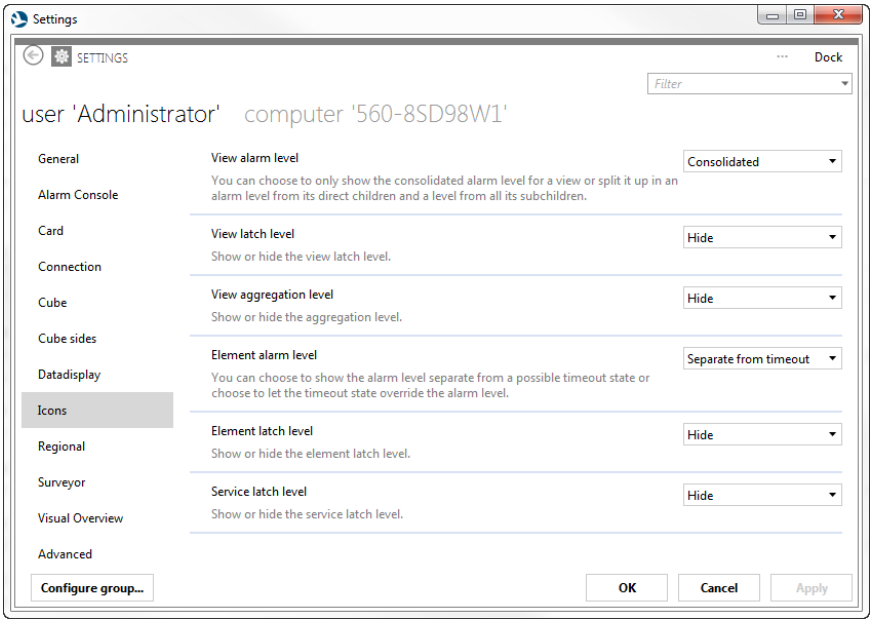


Figure 3–40. Icon Settings

3.7.9 Regional Settings

In the **Regional** page, two settings are possible:

- **Language of the user interface:** Choose the language for the user interface. You must restart the NetVue Cube for this setting to take effect.
- **Regional date and time format:** Select a culture in the drop–down list to customize the format of dates and times in the NetVue Cube to that culture.

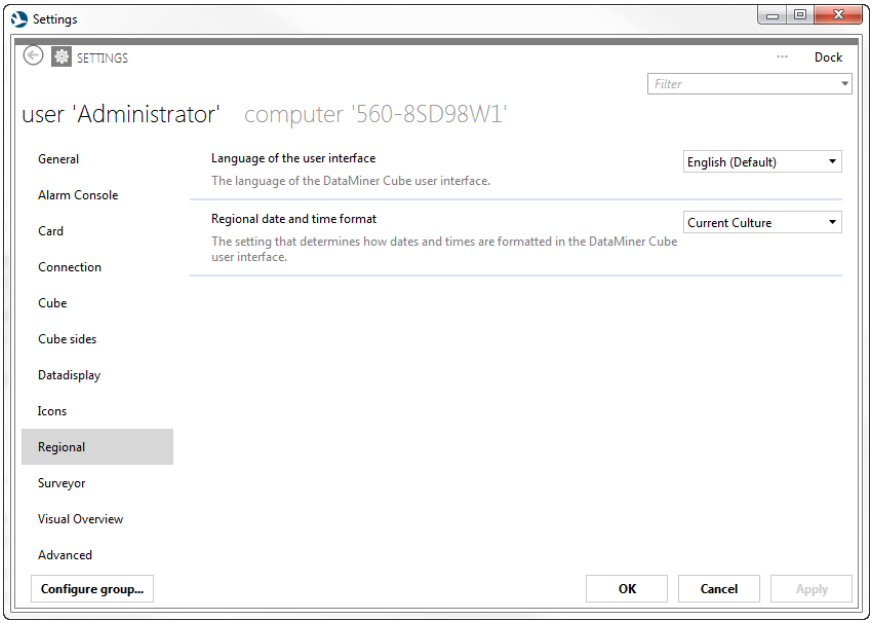


Figure 3–41. Regional Settings

3.7.10 Surveyor Settings

In the **Surveyor** page, several settings are possible:

- **Surveyor docking position:** Select **Right** or **Left** to determine at which side of the screen the Surveyor shows.
- **Allow to expand/collapse service nodes:** Select this setting to enable users to expand services in the Surveyor to see the child items of the services.
- **Virtualize Surveyor tree:** Select this setting to virtualize the Surveyor tree. This means that less memory will be required to expand items in the tree, though scrolling may go more slowly.

Virtualization of the Surveyor tree is advisable in case of large view structures, to avoid load delay. However, by default, this setting is not activated.

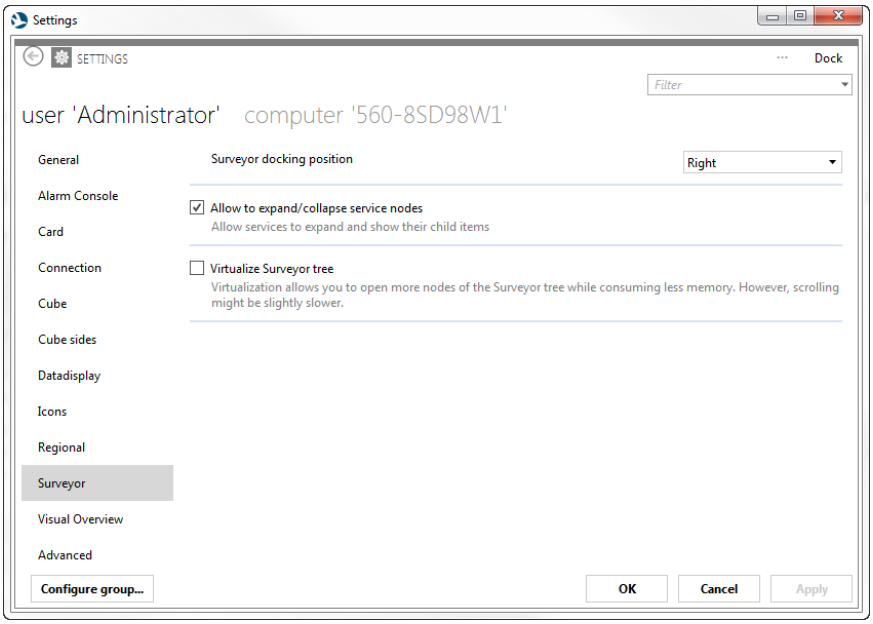


Figure 3–42. Surveyor Settings

3.7.11 Visual Overview Settings

In the **Visual Overview** page, two settings are possible:

- **Enable coloring when severity is normal or undefined:** Select this option to make sure that elements, services and views show colors if their alarm severity level is normal or undefined.
- **Maximum number of child shapes in a 'Children' container shape:** Enter a value in the box to set the maximum number of dynamically generated Visio shapes in a 'Children' container shape.

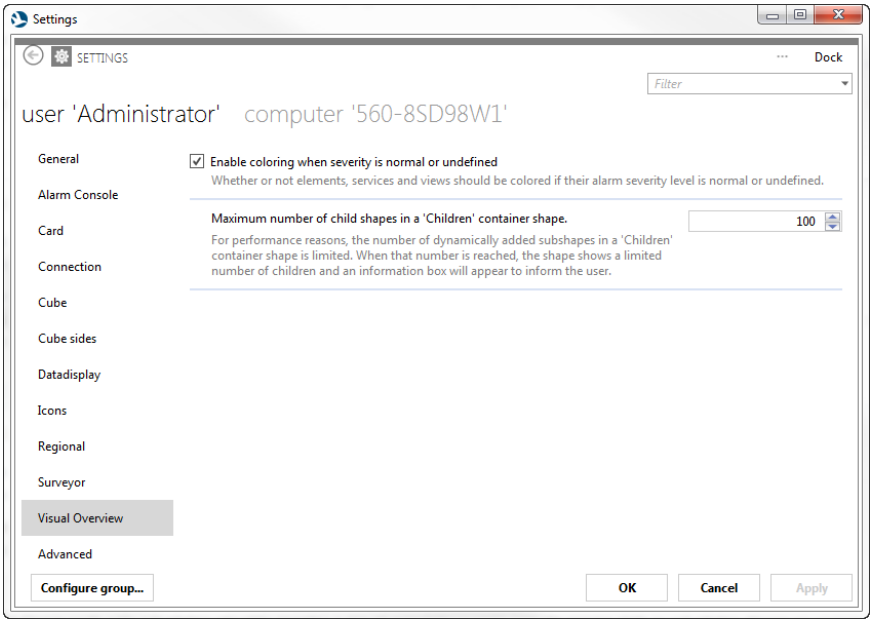


Figure 3–43. Visual Overview Settings

3.7.12 Advanced Settings

In the **Advanced** page, two settings are possible:

- **Group profile:** Select a group in the drop–down list to override all user settings with the settings of this group.
- **DataMiner Cube User [username] reset:** Click the button **Factory defaults** to reset all settings back to default values.

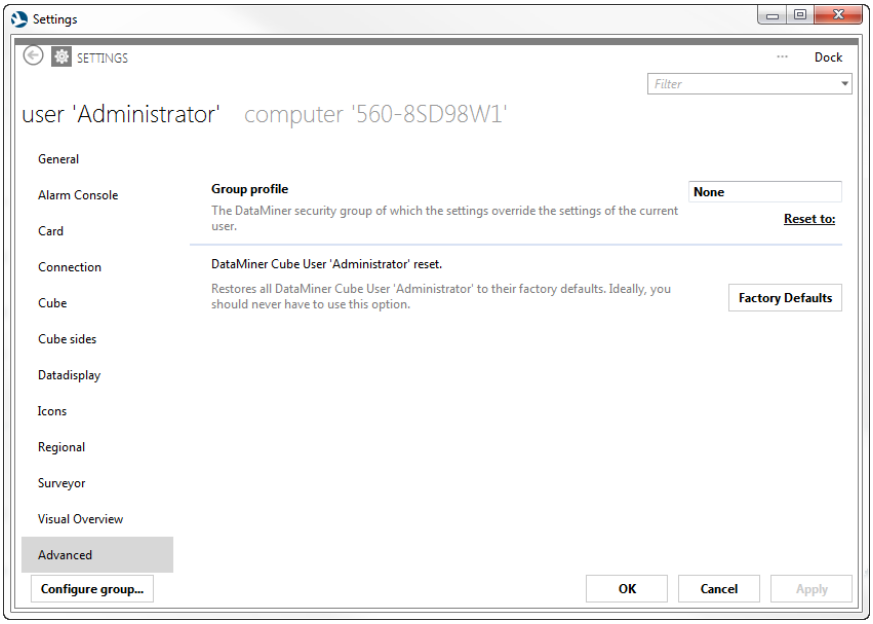


Figure 3–44. Advanced Settings

3.8 NetVue Cube Computer Settings

Any user preferences in the NetVue Cube related to the user's computer are grouped in the tab **computer** in the **Settings** window.

To access the computer settings in the NetVue Cube:

1. Go to the settings window:
   - Click **Start > Apps > Settings** (see Figure 3–31), or
   - Click the user in the top–right corner of the screen, and click **Settings** (see Figure 3–32).
2. Click the **computer** tab.

The tab consists of five pages, through which you can navigate using the table of contents on the left.

3.8.1 Connection Settings

On this page, you can select settings related to the connection of your computer to the NetVue Cube. These settings are available in the Cube logon window also.

- **Automatic log–on with saved user name and password:** Select this setting to have the NetVue Cube remember your user name and password, so that you do not have to enter these except after an explicit logout.
- **Connection type:** Select a connection type in the drop–down list. By default, this is set to **Auto**. When you select other connection types, **Remoting** or **WebServices**, more settings show that must be specified (destination port, polling interval, etc.).

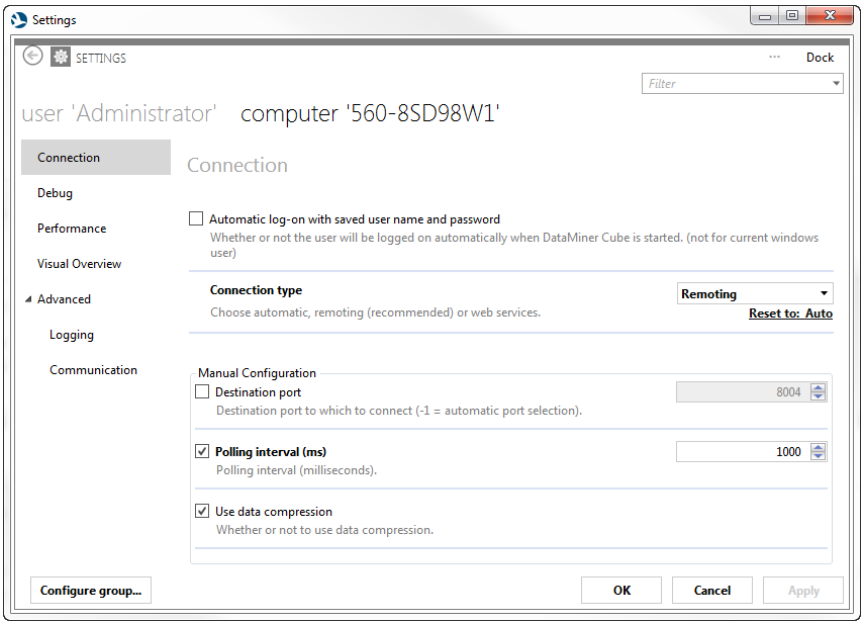


Figure 3–45. Connection Settings

3.8.2 Debug Settings

There are two debug settings:

- **Debug settings visible:** Select this setting, along with the user setting **Show General Parameters debug page**, to show an additional **Data Display** page named **General parameters DEBUG**. This page contains all the general parameters that are not visible usually.
- **Trace mode:** When you enable this setting, Cube debug logging is saved in a file in this folder: **C:\ProgramData\Skyline\DataMiner\DataMinerCube\Traces**. This mode helps to solve problems, and is unnecessary during normal operations.

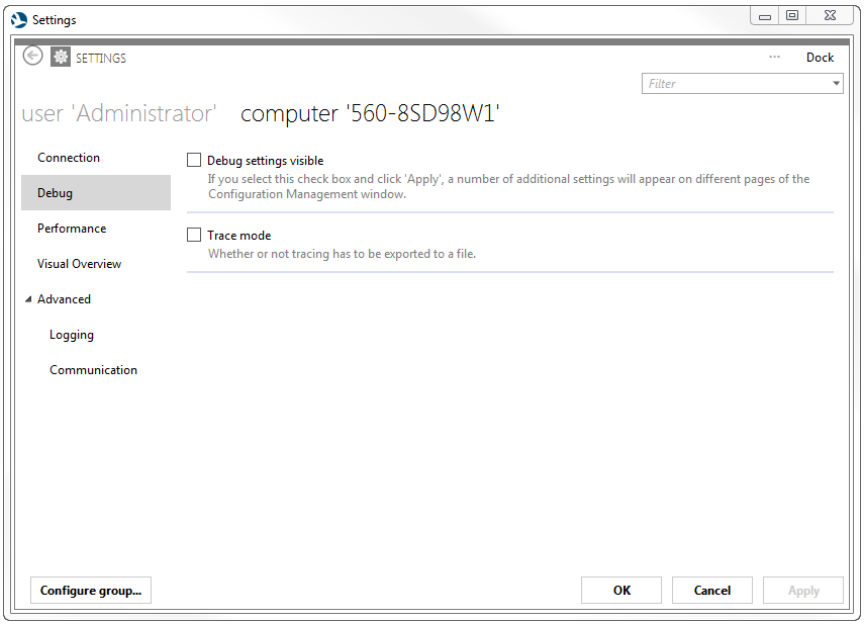


Figure 3–46. Debug Settings

3.8.3 Performance Settings

Performance settings are applicable to your computer's performance:

- **3D effects:** Select this setting to enable 3D effects, such as the animation that shows when a card is flipped to the other side.
- **Use hardware rendering:** Select this setting to set the graphics rendering mode to hardware rendering.

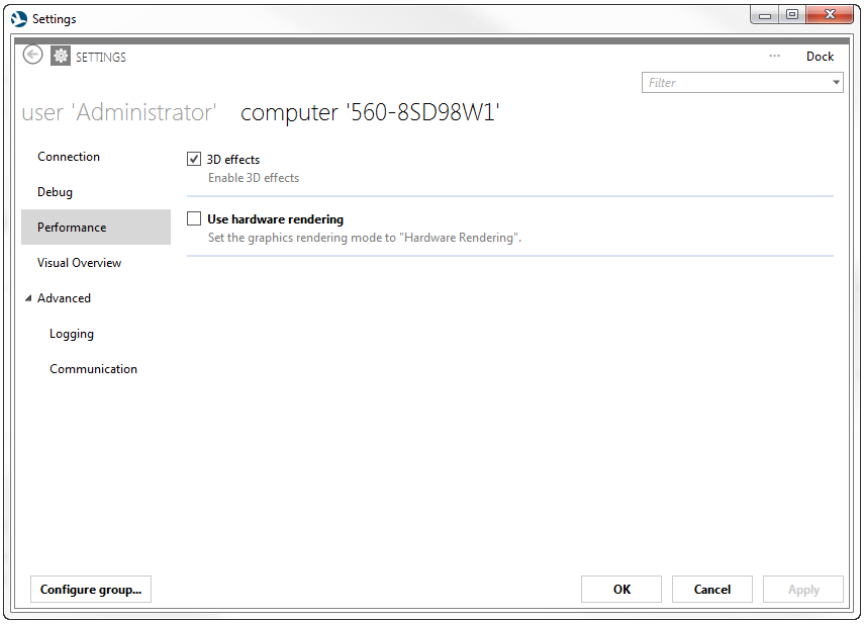


Figure 3–47. Performance Settings

3.8.4 Visual Overview Settings

There is only one setting on this page:

- **Working folder:** Select this setting and specify the folder where you want to keep all Visio files that have been edited on your computer. In this folder, the Visio files can be edited offline, so that they can be synchronized later.

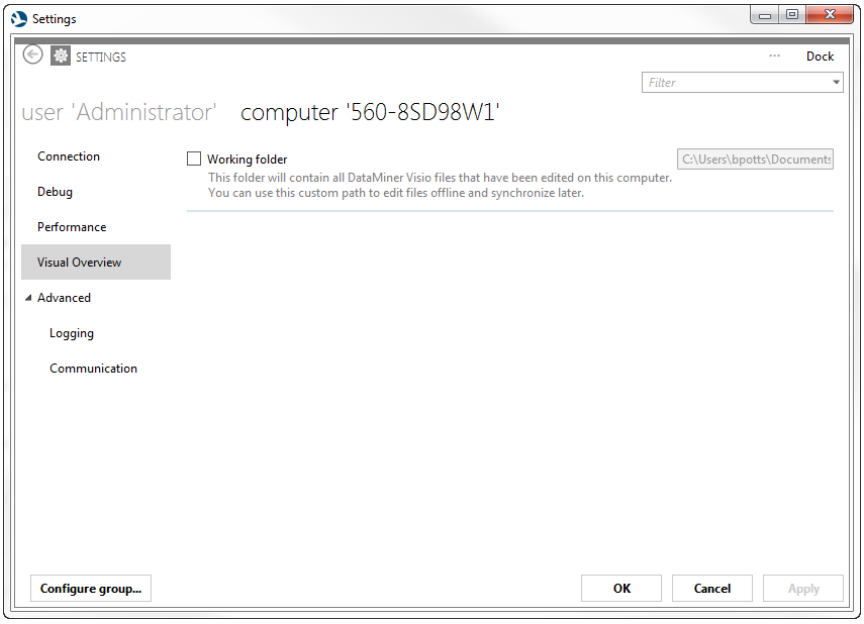


Figure 3–48. Visual Overview Settings

3.8.5 Advanced Settings

In the main **Advanced** page, two settings are possible:

- **Connection timeout(ms):** In the box next to this setting, you can specify the number of milliseconds for the connection timeout.
- **DataMiner Cube computer [computername] reset:** Click the button next to this setting to reset all computer settings back to default. In normal circumstances, this option is unnecessary.

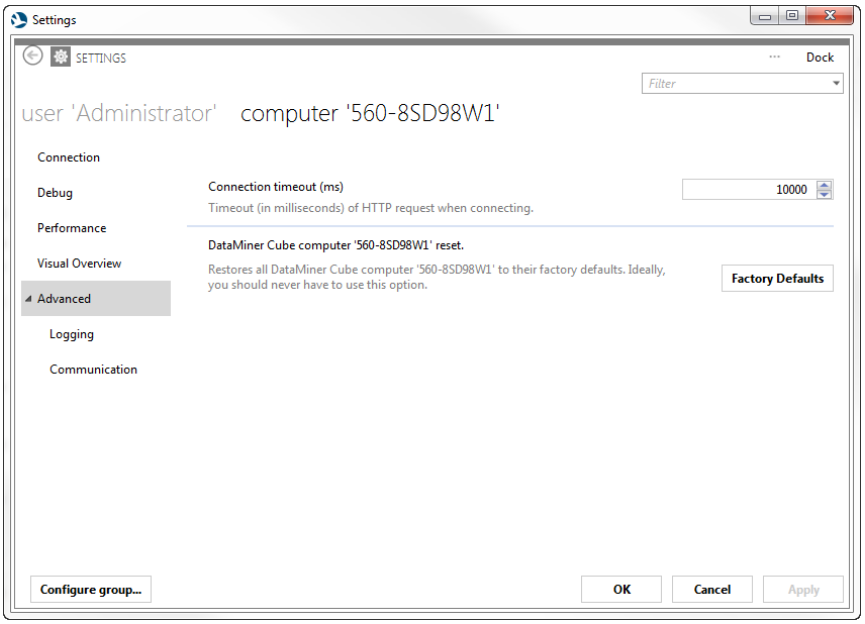


Figure 3–49. Advanced Settings

There are also two subpages: **Logging** and **Communication**.

3.8.5.1 Logging Page

This page allows you to set the number of log entries kept in the NetVue logging, as well as the general log level.

- **Minimum number of log entries:** The minimum number of log entries that are kept when older entries are deleted.
- **Maximum number of log entries:** The maximum number of log entries that are stored in memory. If this number is exceeded, the oldest entries are deleted.
- **Level of logging:** The level of detail recorded in the log entries. The higher the value, the more detailed the logging.

The higher levels of logging, *Log_Everything* or *Development_Logging*, require a large amount of computer resources.

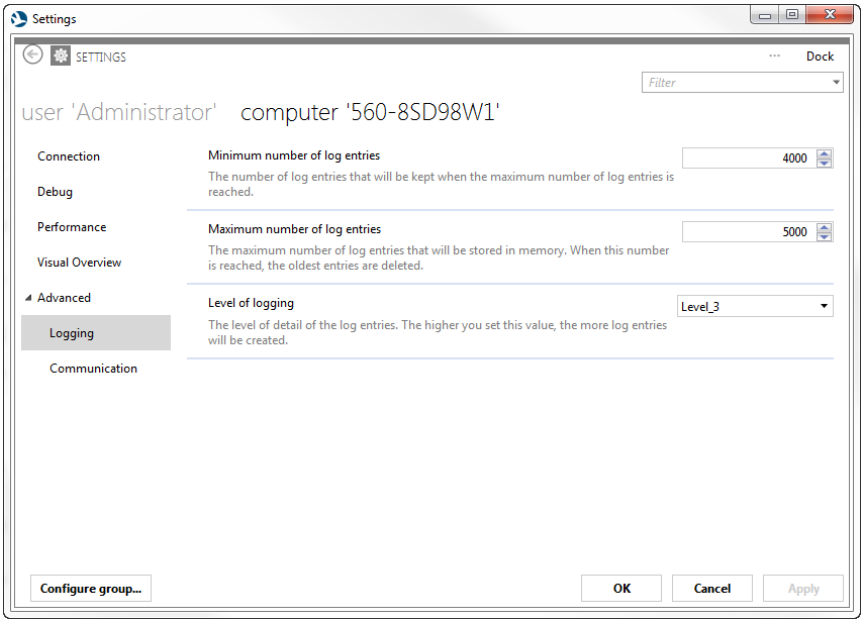


Figure 3–50. Logging Settings

3.8.6 Communication Settings

This page contains settings that affect communication between the computer and the NetVue System.

- **Maximum number of sent messages:** In the box to the right of this setting, enter the maximum number of sent messages that can be stored.
- **Maximum number of received messages:** In the box to the right of this setting, enter the maximum number of received message that can be stored.
- **Fallback sent messages:** In the box to the right of this setting, enter the minimum number of sent messages to keep when older messages are deleted.
- **Fallback received messages:** In the box to the right of this setting, enter the minimum number of received messages to keep when older messages are deleted.
- **Store full messages:** As soon as you select this setting, details are stored for each message. These can be seen in a separate **Details** pane when you click the message in the communication logging.

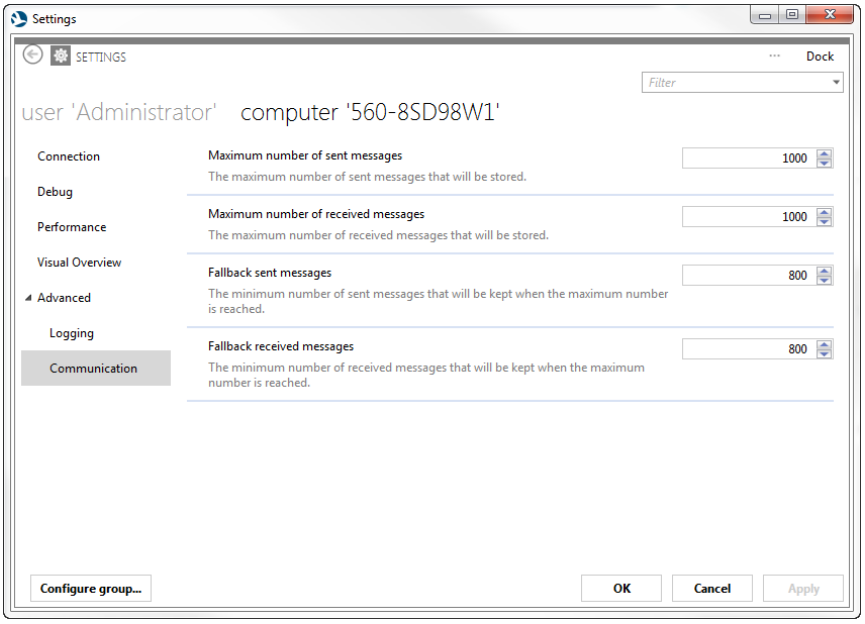


Figure 3–51. Communications Settings

3.8.6.1 Network

Use the Network Tab to see a map view of the deployed network(s). Each level shows the child objects contained below that level.

For example, at the Service Group level, all Service Areas are shown. The Service level shows all remotes contained within each Capacity Group and QoS Group.

There are two sub tabs within the Network Tab.

- If the NetVue Server is connected to the public internet and can communicate with the Google Maps Server, the *Maps* sub tab allows you to integrate Google Maps into a NetVue Monitoring System.
- Use the *default* tab to map the network topology within a closed network, using a static map.

Both tabs show real time alarms. When using Google Maps, additional features can be shown that may not be available in the static view. Clicking on a site will display some basic information about the site, and for remote sites, there is a link to each circuit that the site belongs to.

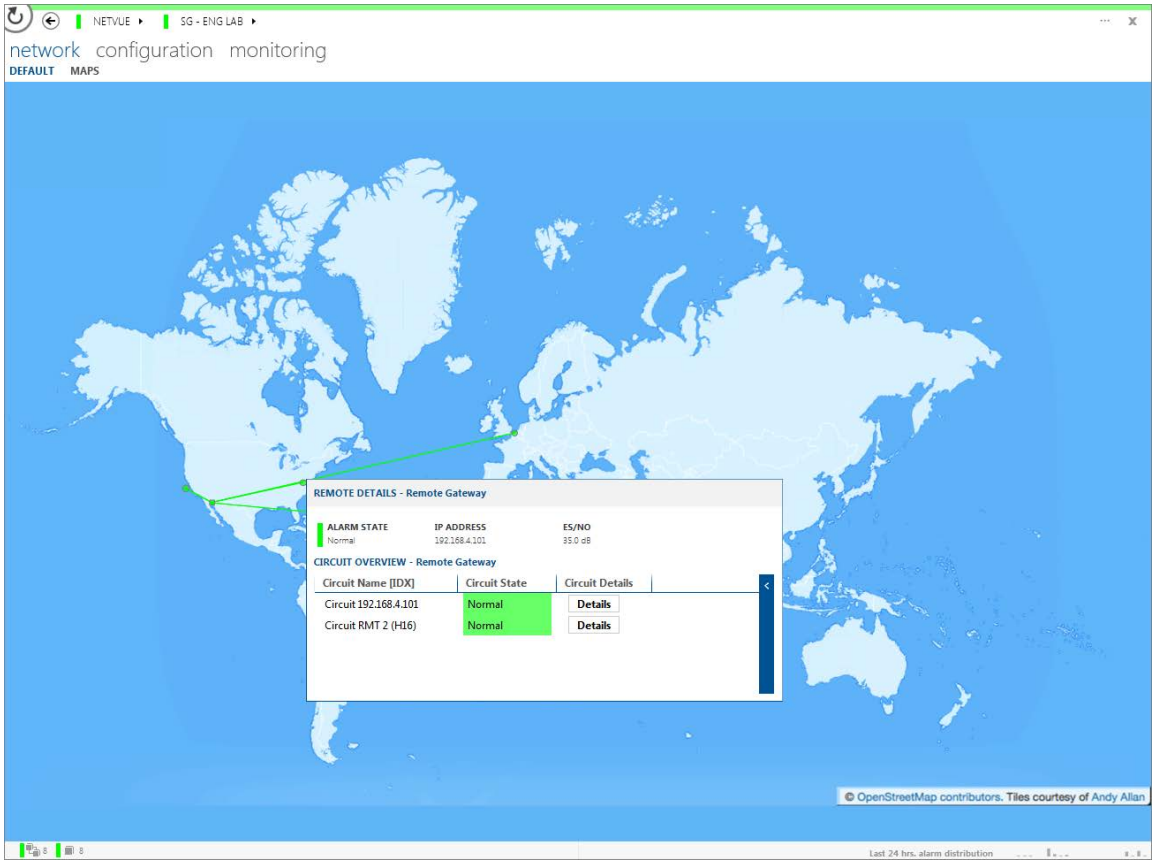


Figure 3–52. Network Static Maps

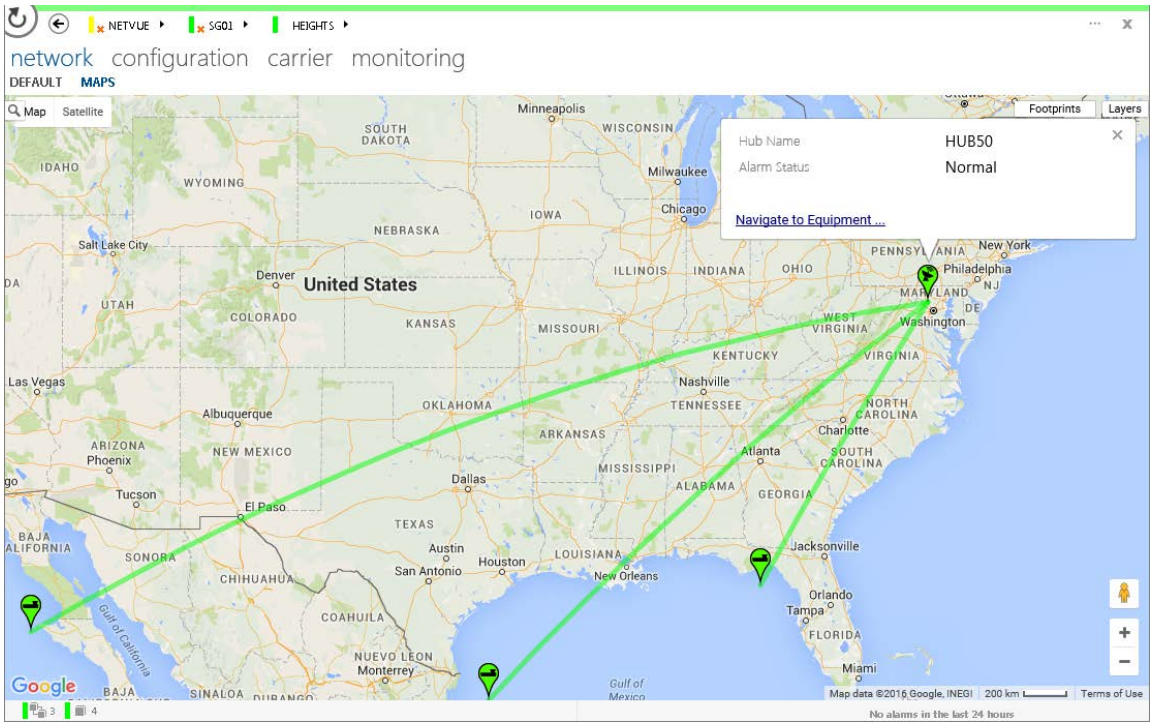


Figure 3–53. Network Google Maps

NetVue needs access to the public internet to communicate with the Google Maps Servers.

3.8.6.2 Configuration

The configuration section lets the operator configure the NetVue system.

At the root level, the operator can configure the Service Group. A Service Group consists of any number or type of Service Areas. It is used to associate several types of services. A Service Area is a single, shared outbound carrier, including all of the Comtech EF Data Hub and Remote equipment required to provide the service.

At the Service Area level, the configuration section allows the creation, modification and deletion of a capacity group. The capacity group is the highest level of QoS that allows the outbound carrier to be subdivided and reserved by the HNO for use by a VNO or a Customer OpCo. A QoS Capacity Group can be sub–divided into multiple QoS Groups (2nd Level of Outbound QoS). Each QoS Group represents a reservation of bandwidth within each QoS Capacity Group. Use this allocation for a single remote or for multiple remotes, depending on how you want to allocate the bandwidth.

3.8.6.2.1 Configuration – Service Group

The Configuration Page at the Service Group level lets you create Service Areas. Use it to add the VMS Element, as well as create and define the Satellite properties.

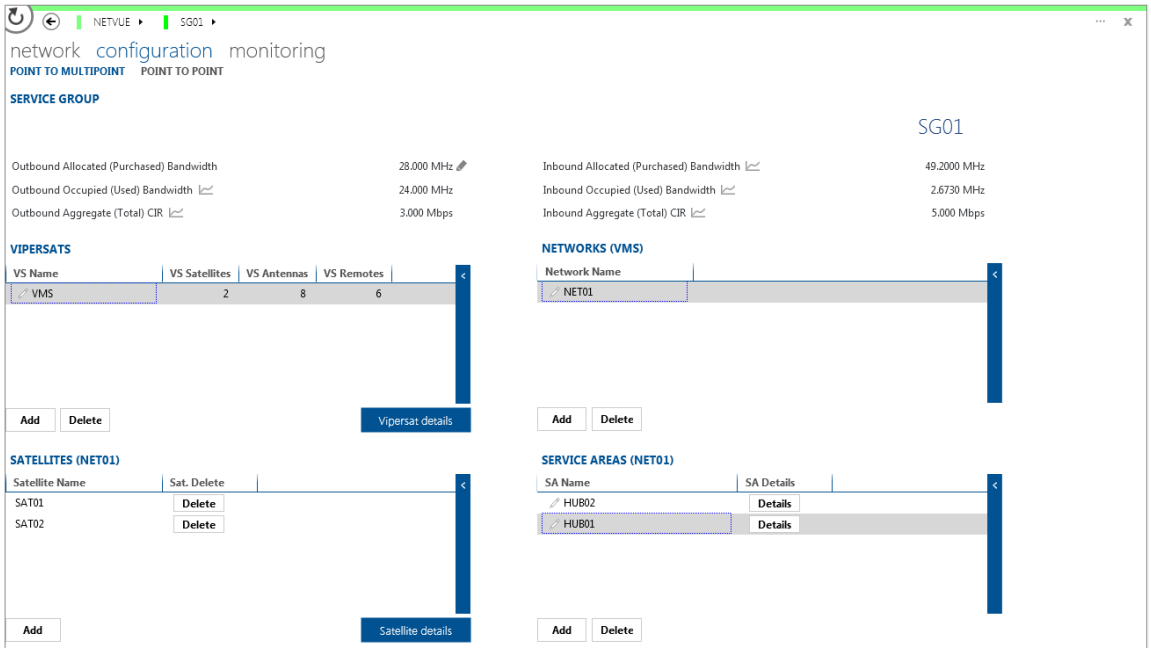


Figure 3–54. Configuration Page – Service Group

The Configuration Page shows an overview or quick snapshot of the accumulated statistics for all the Service Groups in a Service Area. Figure 3–55 lists examples of these statistics.

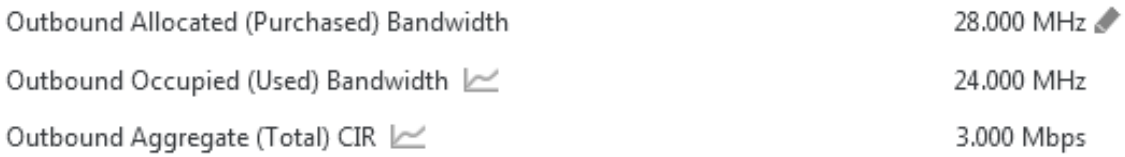


Figure 3–55. Service Group Outbound Statistics Example

- **SG – Outbound Allocated Bandwidth*:*** A static, user–defined value, that represents the total allocated bandwidth in Mbps allocated for the Service Areas Outbound(s) in this specific Service Group. This field is solely for reference purposes only to compare the occupied bandwidth with the total allocated bandwidth.
- **Outbound Aggregated CIR*:*** The aggregated Committed Information Rate(s) in Mbps for all the Service Areas Outbound(s) Capacity and QoS Groups in the specific Service Group

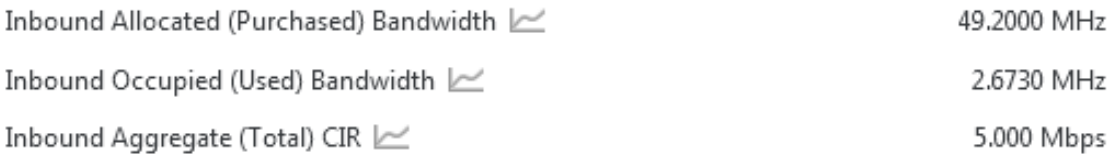


Figure 3–56. Service Group Inbound Statistics Example

- **SG – Inbound Allocated Bandwidth*:*** The aggregated bandwidth in Mbps for the Inbounds for all the Service Areas in the specific Service Group
- **Inbound Aggregate CIR*:*** The aggregated Committed Information Rate in Mbps for all the inbounds in the specific Service Group
- **Outbound Aggregate BW*:*** The Aggregated bandwidth in MHz for all of the outbound in the specific Service Group

The Vipersat section lets you link NetVue with Vipersat Management System. The table lists all Vipersat(s) allocated for this specific Service Group. It gives a quick overview of how many satellites, antennas and remotes exist in this Service group.

Once ViperSat Management System has been linked with NetVue, *DO NOT* make any changes through Vipersat. Doing so can cause serious problems for both platforms.

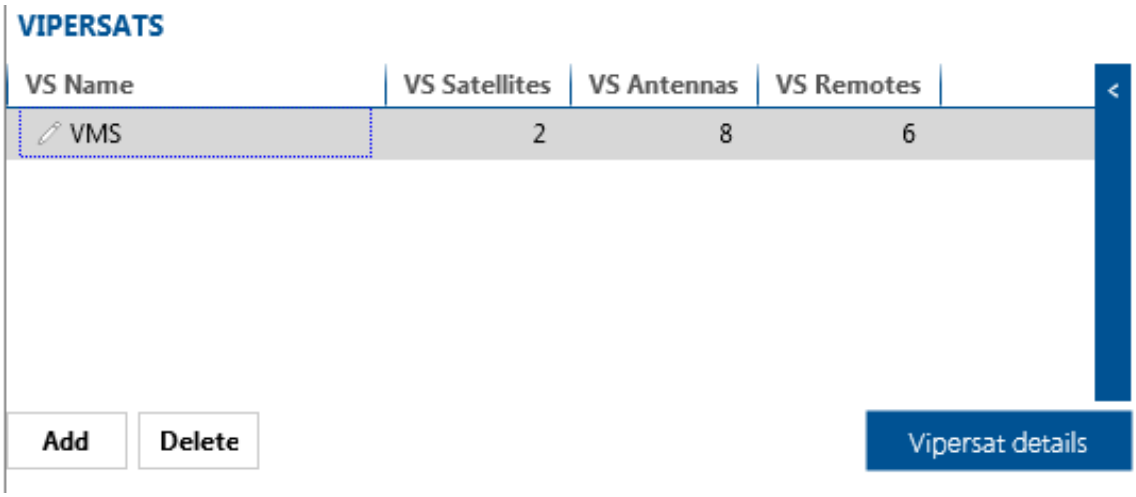


Figure 3–57. Vipersat Section

Once a VMS has been linked, a user can create/display/modify any network associated with the Bandwidth Manager.

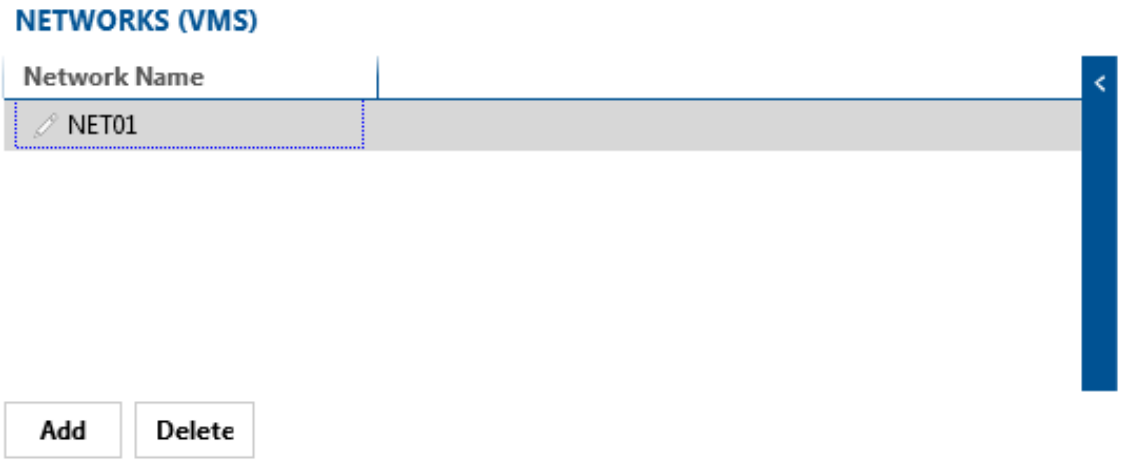


Figure 3–58. Networks Section

Satellite(s) are linked to a Network in the Satellite Section and can be created by clicking on the add button and displayed/modified by clicking the Satellite row and clicking Satellite Details.

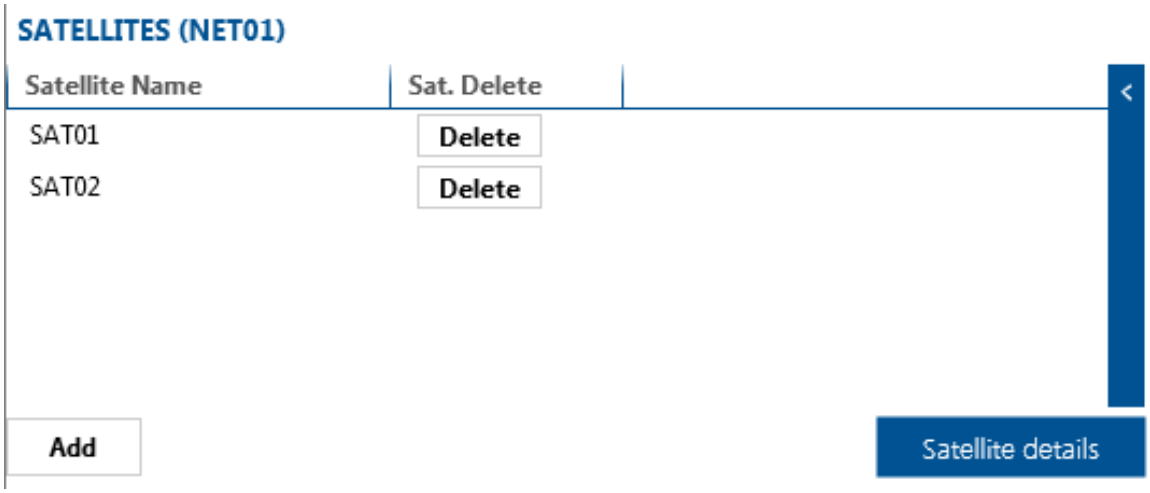


Figure 3–59. Satellites Section

After Vipersat is linked and a Network and Satellite are created, a Service Area can then be created. A Service Area is a single, shared outbound carrier including all of the CEFD Hub and Remote equipment required to provide the service.

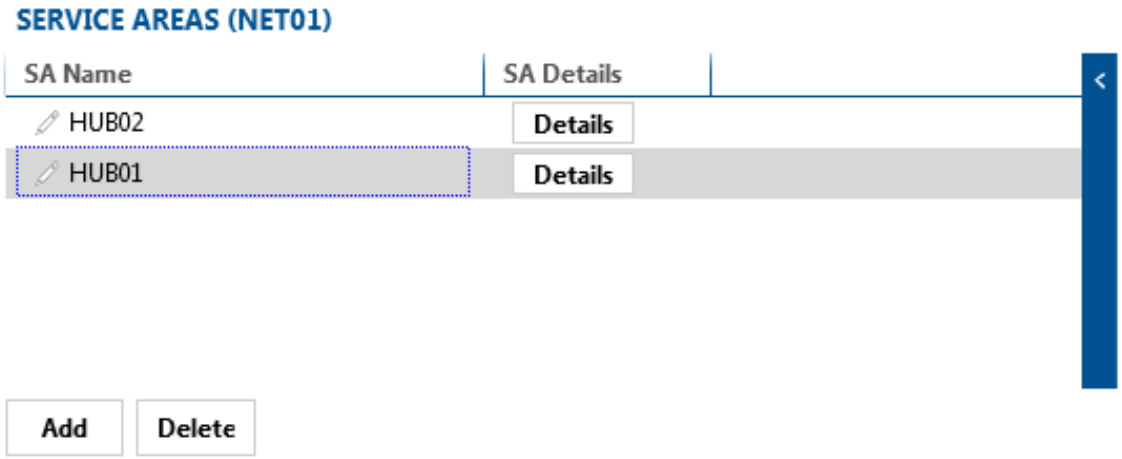


Figure 3–60. Service Area Section

3.8.6.2.2 Configuration – Point–to–Multipoint Service Area

Do not create Capacity or QoS Groups in the CTOG HTTP Interface, because there is dynamic linking in NetVue for Monitoring and Statistic gathering purposes.

The configuration section at the Service Area level lets you create, modify and delete a Capacity group. A Capacity group is the highest level of QoS that allows the outbound carrier to be subdivided and reserved by the HNO for use by a VNO or a Customer OpCo.

3.8.6.2.2.1 General Page

The General Page at the Service Area level gives a high level overview of the Service Area.

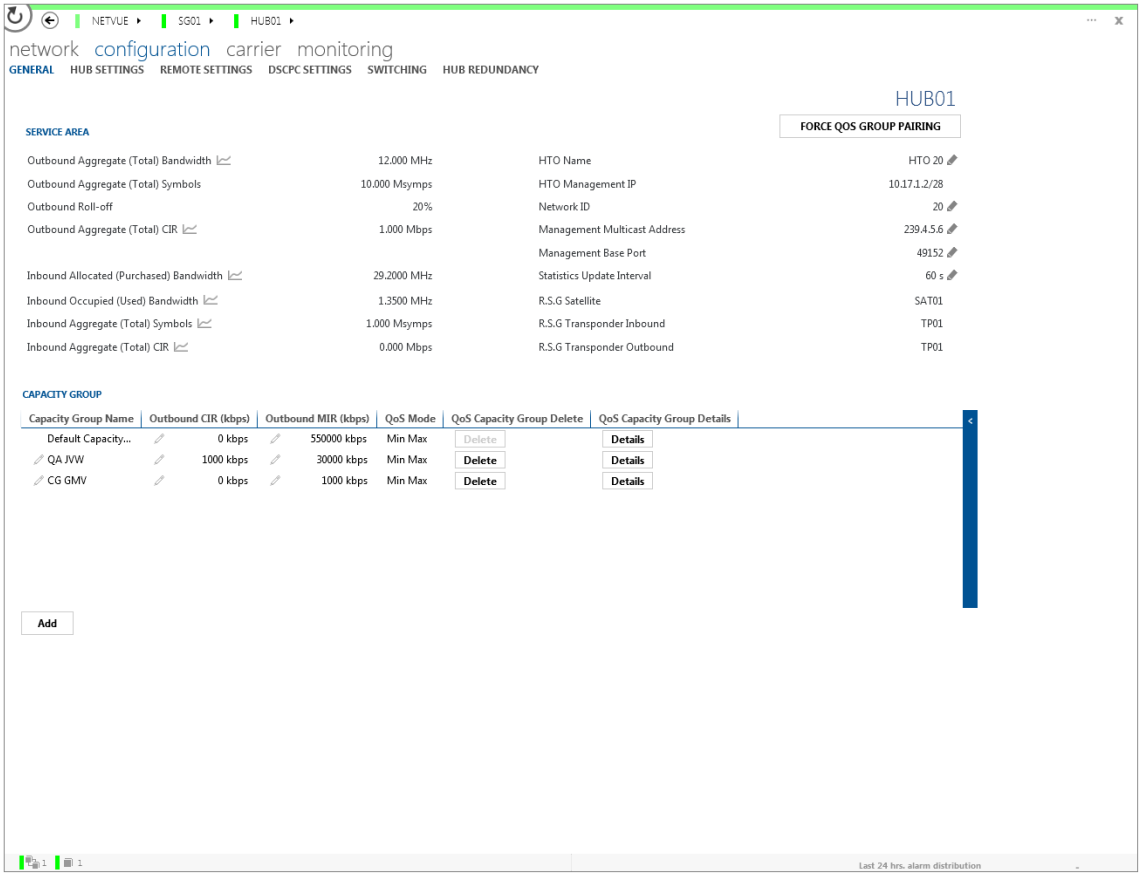


Figure 3–61. Configuration – Service Area – General Page

- **Force QoS Group Pairing:** Triggers NetVue to scan the Service Areas for new devices/circuits.
- **Outbound Aggregate (Total) Bandwidth*:*** The total bandwidth for the Outbound in MHz.
- **Outbound Aggregate (Total) Symbols*:*** The total symbols for the Outbound in ksmps.
- **Outbound Roll–Off*:*** The configured Roll Off for the Outbound.
- **Outbound Aggregate (Total) CIR*:*** The total aggregated CIR for all the capacity groups in the Outbound in kbps.
- **Inbound Allocated (Purchased) Bandwidth*:*** The total available inbound bandwidth in ksmps.
- **Inbound Occupied (Used) Bandwidth*:*** The total bandwidth in use in ksmps.
- **Inbound Aggregate (Total) Symbols*:*** The total aggregated symbols for the inbound.
- **Inbound Aggregate (Total) CIR*:*** The total aggregated CIR for the inbound in kbps.
- **CTOG/HTO Name*:*** The associated name for the Outbound.
- **CTOG/HTO Management IP*:*** The Management IP address and Subnet for the Outbound.
- **Network ID*:*** The unique Network ID assigned to the Outbound.
- **Management Multicast Address*:*** The Multicast Address assigned to the Service Area.
- **Management Baseport*:*** The Management Baseport assigned to the Service Area (Default is 49152).
- **Statistical Update Interval*:*** The interval in seconds in which the statistics are updated.
- **Satellite*:*** The Satellite assigned to the Outbound.
- **Transponder Outbound*:*** The Transponder in which the Outbound is located.
- **Transponder Inbound*:*** The Transponder in which the Inbound is located.

Any parameter with this icon:  ***means that this value is being trended.***

Any parameter with this icon:  ***means that this value can be modified.***

3.8.6.2.2.2 Hub Settings

Use the Hub Setting pages to create a hub. There are two pages.

- **The General Page:** Shows the site location and the RF attributes associated to the HUB site.
- **The Equipment Page:** Shows the assigned an available modulator and demodulator. It also is used to set the ECM Controller and the allocatable demodulators.

For more information on ECM and Device Allocation, see the VMS User Guide.

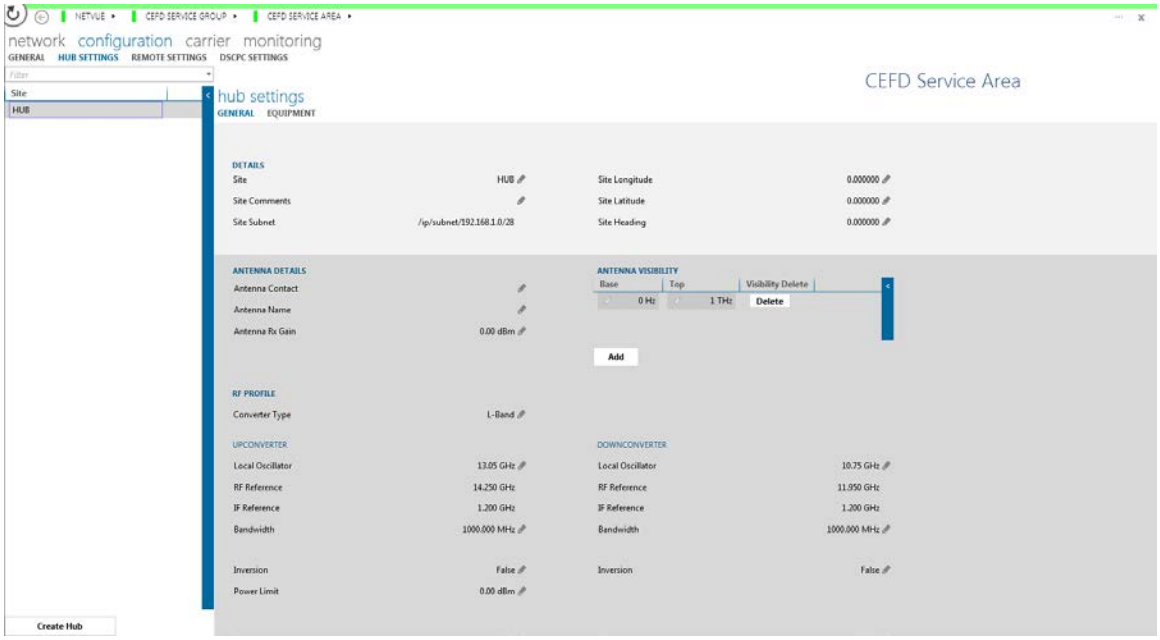


Figure 3–62. Hub Settings General Page

3.8.6.2.2.3 Remote Settings

Use the Remote Settings pages to create remotes. There are seven pages:

- **General Page:** Shows the site location and RF configuration.
- **Equipment Page:** Shows the assigned an available modulator and demodulator. It also is used to set the allocatable demodulators for Mesh networks.
- **Inband Page:** Shows the return path switching configuration.
- **Reservations:** Shows the device reservations.
- **Policies:** Shows the application policies.
- **Distributions:** Shows the distribution lists and remote destinations.
- **MODCOD:** Shows the default MODCOD and MODCOD thresholds.
- **dSCPC:** Show the selected remote's dSCPC configuration.

For more information on inbanding see the VMS User Guide.

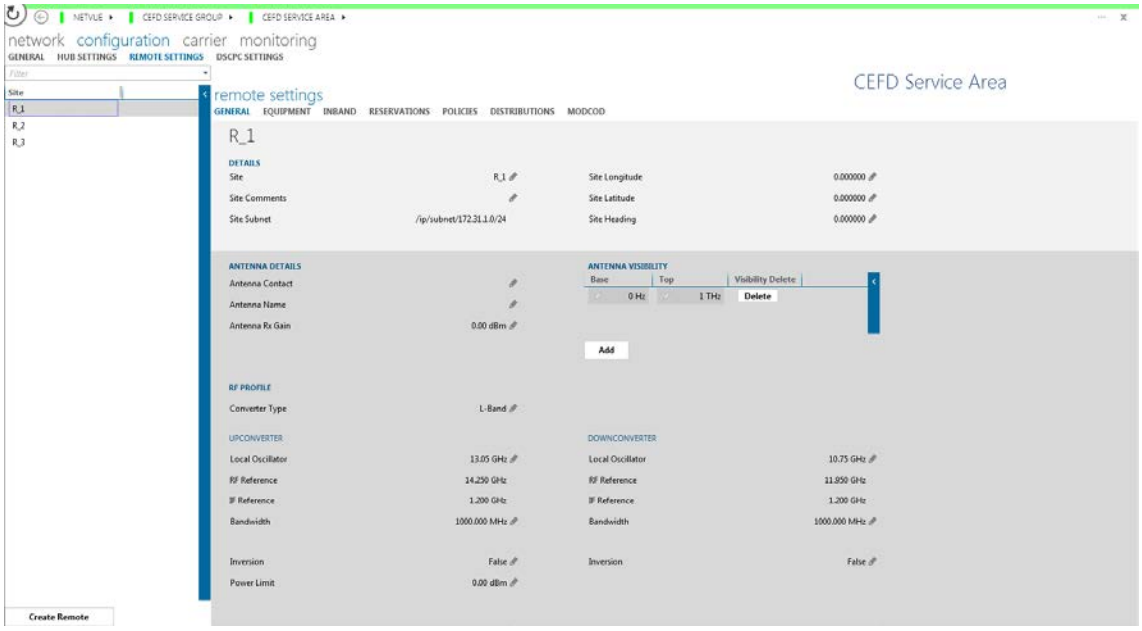


Figure 3–63. Remote Settings General Page

3.8.6.2.2.4 dSCPC

Use the dSCPC page to configure the global policies for dynamic SCPC. All configurations made at this level are inherited by the child objects, unless modified specifically for each site.

For more information on dSCPC, see the VMS User Guide.

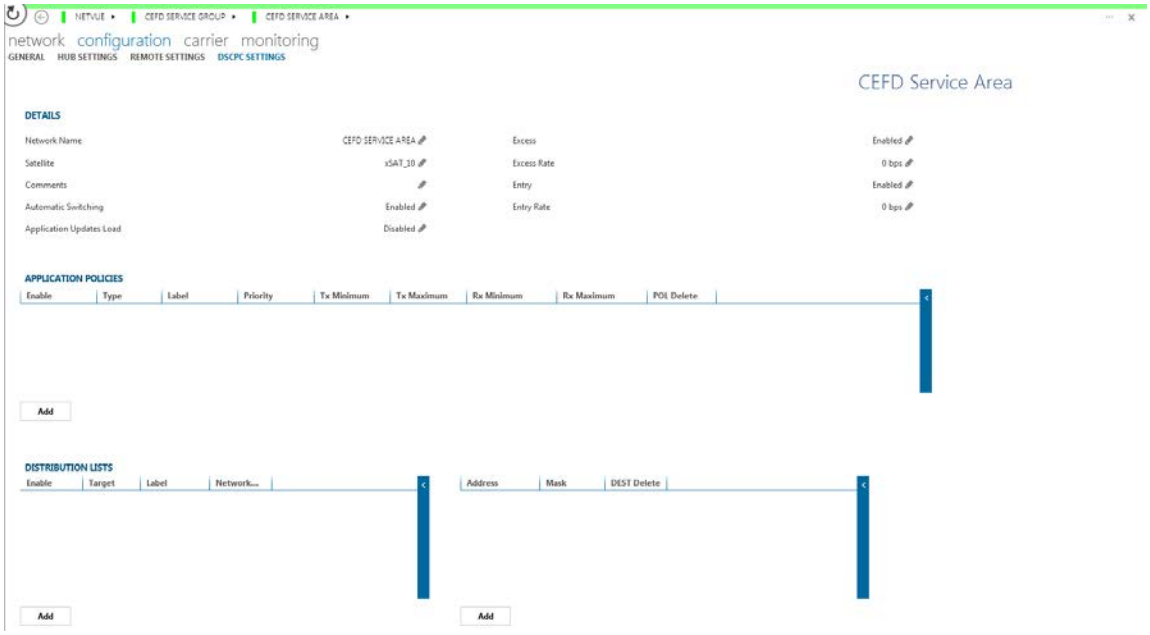


Figure 3–64. dSCPC Settings

3.8.6.2.2.5 Switching

The **Service Area–>Configuration–>Switching View** provides the user a single view to control and monitor the switching state of the remote sites. In this view, the user can configure:

- Diagnostics (Revert, Setup, Reset)
- Application Sessions

The diagnostic revert, setup, and reset are tools to help the user commission a site, perform testing, and help recover a site and/or bandwidth when there is a configuration/communication issue. A diagnostic setup configures a remote site to a user specified data rate and MODCOD. When a remote site is configured to a diagnostic setup, it ignores any dynamic switching and carrier recovery requests from the bandwidth manager so it is not recommended to use this feature in a live network. To return a site back to normal operation, a diagnostic revert needs to be performed. The diagnostic revert and reset commands are recovery mechanisms take the remote site out of the dynamic pool and return it to the ECM channel. The key difference between a revert and a reset is that a revert retains its bandwidth slot and doesn't allow that slot to be used by other remotes where as a reset returns the bandwidth back to the pool. An important note is that a since a reset returns the bandwidth, it is important that the remote's carrier is off in case the reset fails and another remote tries to use the same bandwidth causing interference.

An application session setup provides the means for the user to manually set and execute a new application switch. The user created session requires that there first be a defined application policy either at the network level or at the site level. The benefit of using an application session over a diagnostic setup is that an application session is used along with dynamic switching and will not interfere with the bandwidth manager and therefore can be safely used in a live network.

The Switching View provides the following monitoring status:

- Tx Status
- Switch Type
- Switch Status
- Tx Bit Rate
- Associated Hub and Remote Mesh Demodulators
- Application Session Status (Current Sessions, Tx Maximum, Tx Minimum)

The Switch Status and Tx Bit Rate are trended values that can be used in analyzing the remote site's demand, uptime, and switching frequency.

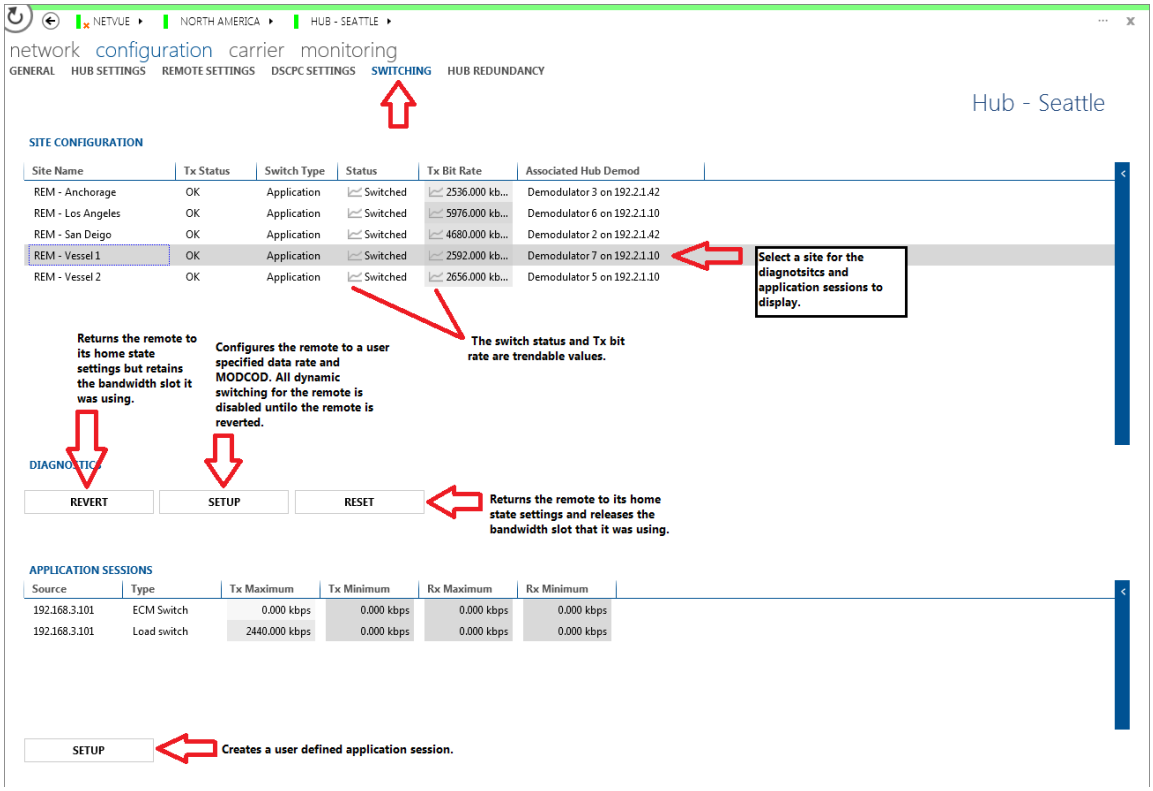


Figure 3–65. Switching Page

3.8.6.2.2.6 Hub Redundancy

Hub redundancy is described in Appendix B.

3.8.6.2.3 Configuration – Capacity Group

The configuration section at the Capacity Group level is the highest level of QoS that allows the outbound carrier to be subdivided and reserved by the HNO for use by a VNO or a Customer OpCo. A QoS Capacity Group can be sub–divided into multiple QoS Groups (2nd Level of Outbound QoS). The configuration page gives an overview of the specific Capacity Group, allows modifications to the capacity group, and the creation of QoS Groups.

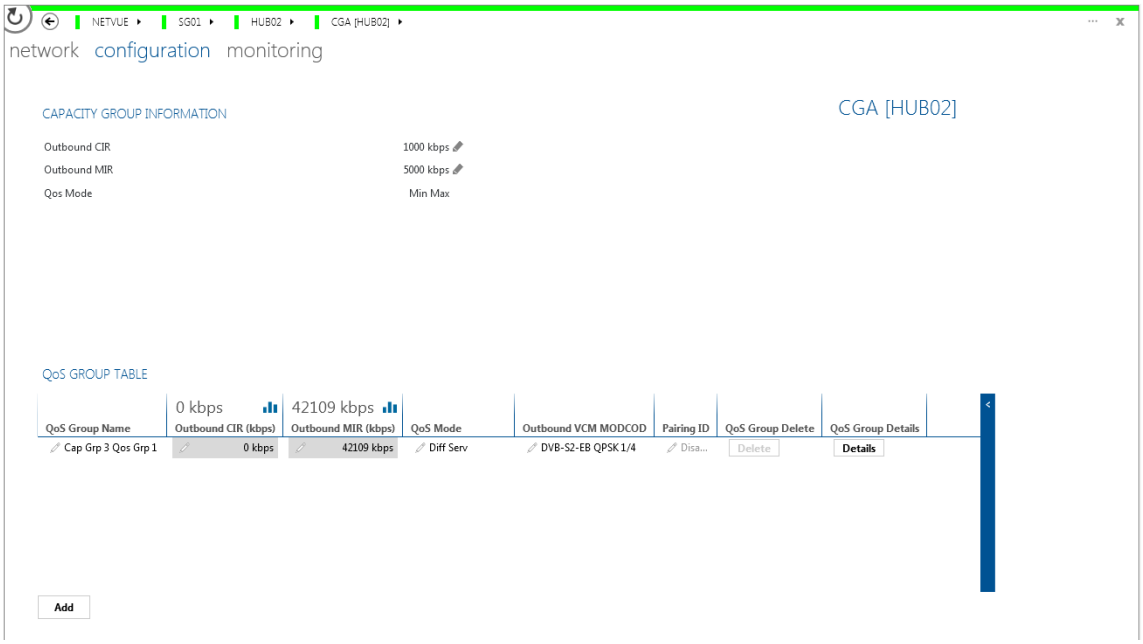


Figure 3–66. Configuration – Capacity Group Level

Capacity Group Information:

- **Outbound Committed Information Rate (CIR)*:*** The guaranteed data rate of the outbound assigned to this specific Capacity Group.
- **Outbound Maximum Information Rate (MIR):** The maximum data rate that this specific Capacity Group is allowed to use of the total outbound.
- **QoS Mode:** The QoS mode configured for this Capacity Group.

QoS Group Table:

- **QoS Group Name*:*** Unique label to identify the QoS Group.
- **Outbound CIR (kbps):** The guaranteed data rate in kbps of the Capacity Group's CIR assigned to a specific QoS Group.
- **Outbound MIR (kbps):** The maximum data rate in kbps of the Capacity Group's MIR assigned to a specific QoS Group.
- **QoS Group Mode*:*** The operating mode assigned to this specific QoS Group. The modes of operation are Diffserv, Max–Priority, Weighted–Priority, Min/Max, Max–Priority.
- **Outbound VCM MODCOD:** The assigned default MODCOD for non–ACM and multicast traffic.
- **Pairing ID:** An ID used to match outbound and inbound QoS Groups to create circuits.
- **QoS Group Delete*:*** Deletes the QoS Group.
- **QoS Group Details*:*** Navigates to the QoS Group page.

For more information on the specific modes of QoS, see the user manual for each supported product.

3.8.6.2.4 Configuration – QoS Group

The configuration section of the QoS Group represents a reservation of bandwidth in each QoS Capacity Group. This allocation can be used for a single remote or for multiple remotes, depending on how you want to allocate the bandwidth.

3.8.6.2.4.1 Outbound

The outbound subpage lets you make changes to an individual QoS group for the Outbound. On this page, you can set:

- **Outbound Committed Information Rate (CIR):** The committed information rate for the QoS group. It can be set greater than the CIR of the capacity group to support oversubscription.
- **Outbound Maximum Information Rate (MIR):** The maximum information rate for the QoS group.
- **Pairing ID:** An ID used by NetVue to pair remote QoS groups with the hub QoS goups.
- **QoS Mode:** DiffServ, Min/Max, Max/Priority, Priority/Weighted.
- **Outbound VCM MODCOD:** The static MODCOD that is used for multicast traffic and QoS groups with no matching remote site.
- **Remote(s):** Dynamically and user created table of remote sites listed by management IP addresses.
- **Subnet(s):** User created table of traffic destination subnets used to match traffic to a QoS group.
- **VLAN(s):** User created table of destination VLANs used to match traffic to a QoS group.
- **Outbound QoS Rule(s):** User created table of rules used to shape traffic.

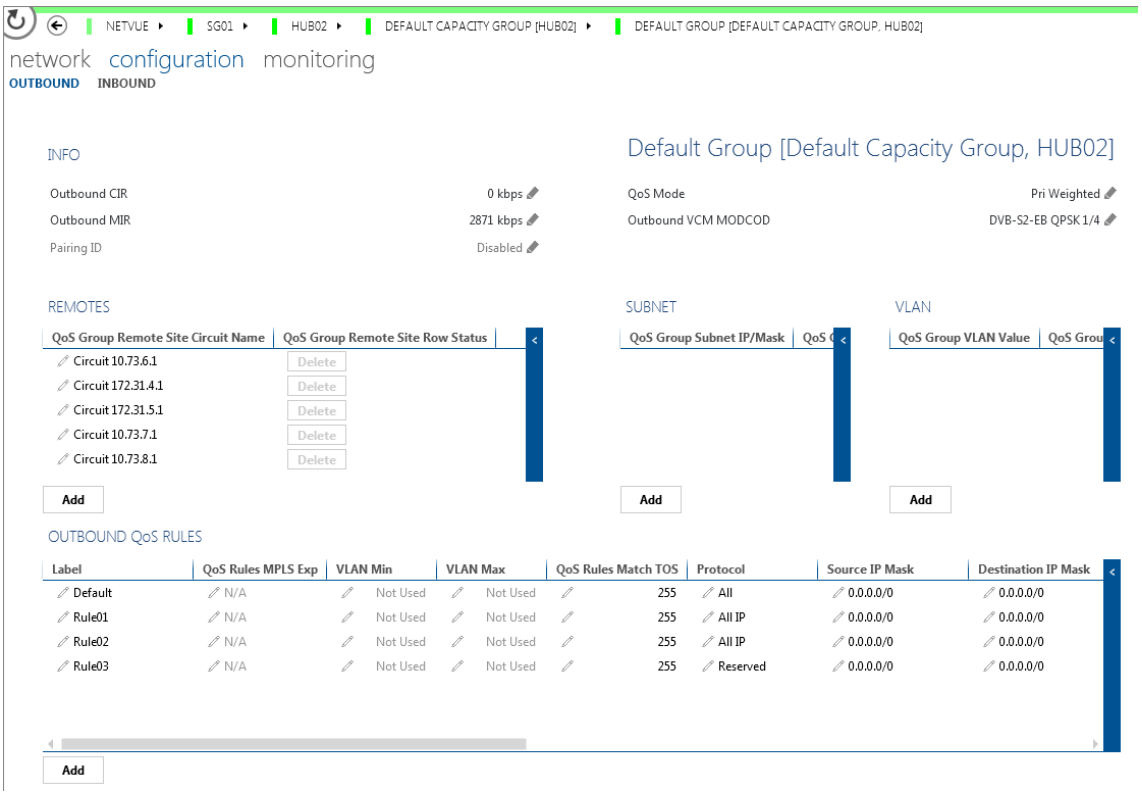


Figure 3–67. QoS Group Configuration Outbound

3.8.6.2.4.2 RF Equipment in Circuit View

The RF equipment that is used along with the modems can be added to the circuit to become integrated into the M&C of the circuit. RF devices are manually added to the Network container as elements and then are provisioned into the circuit by the user. To add an RF device to a circuit, take follow steps:

1. Add the RF device to the appropriate Network container. The Network container needs to be the same as the modem that it will be connected to.
2. Select the circuit in the Surveyor and then select the Circuit View.
3. Click on the '+' sign in the triangle symbol for the appropriate up/down converter that is being added.
4. Select the RF device from the drop–down list. If no device is listed, it is either added to another modem or it is not in the same Network container.
5. Click the "Add" button and the RF device will now be shown in the circuit view along with its status.

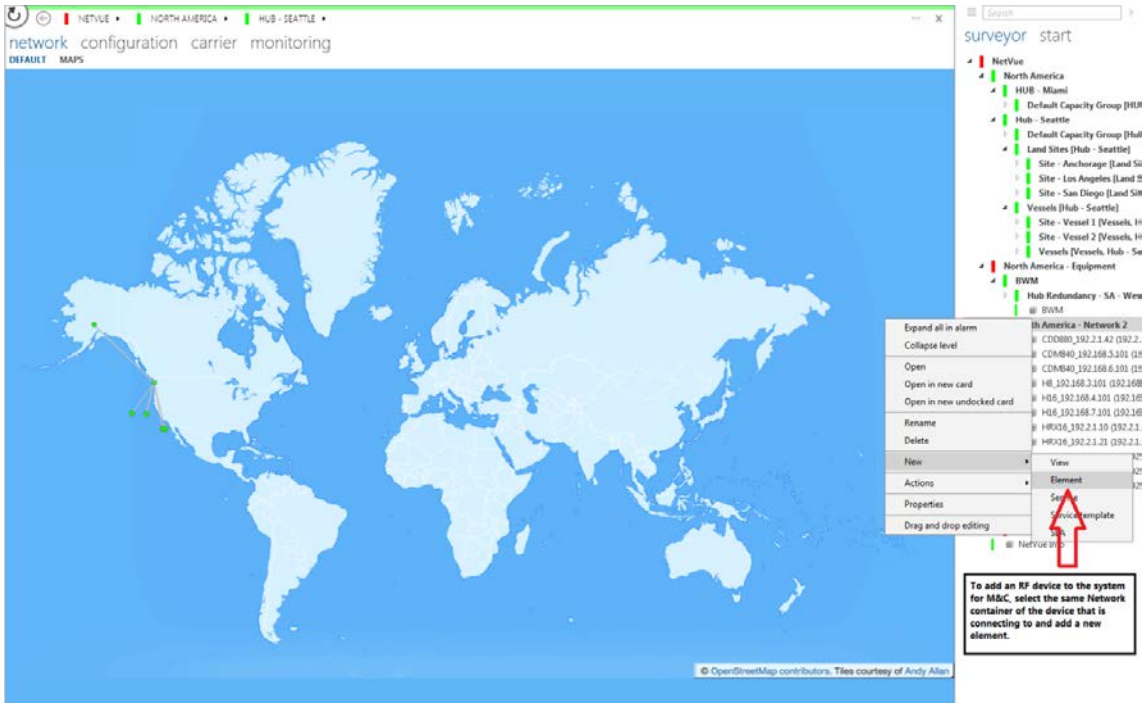


Figure 3–68. Create an RF Device Element

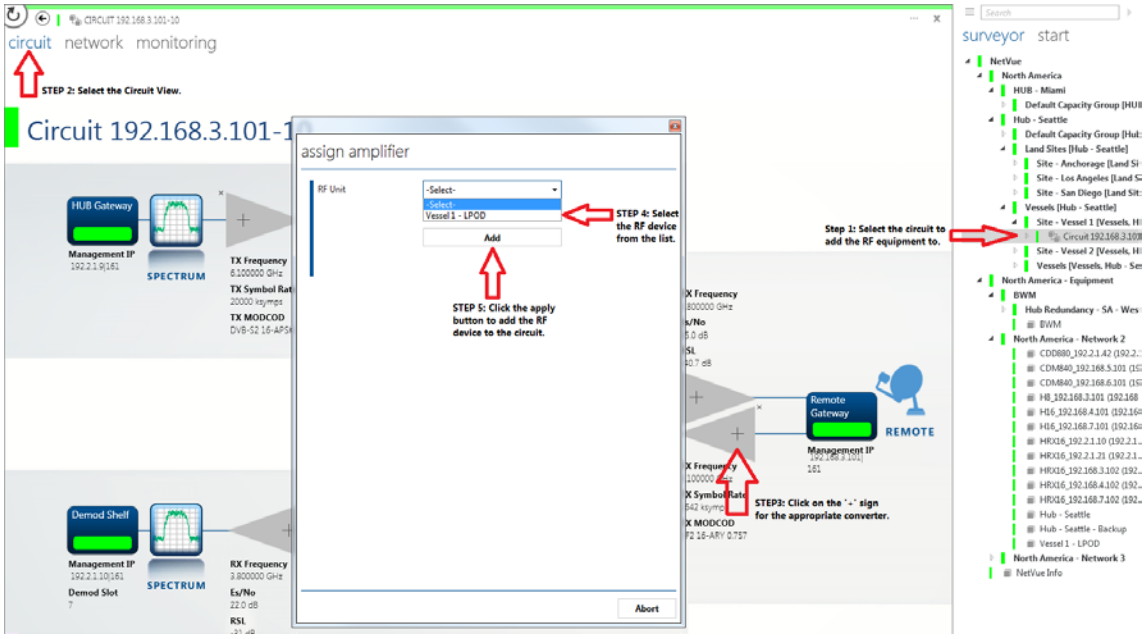


Figure 3–69. Add the RF Device to the Circuit View

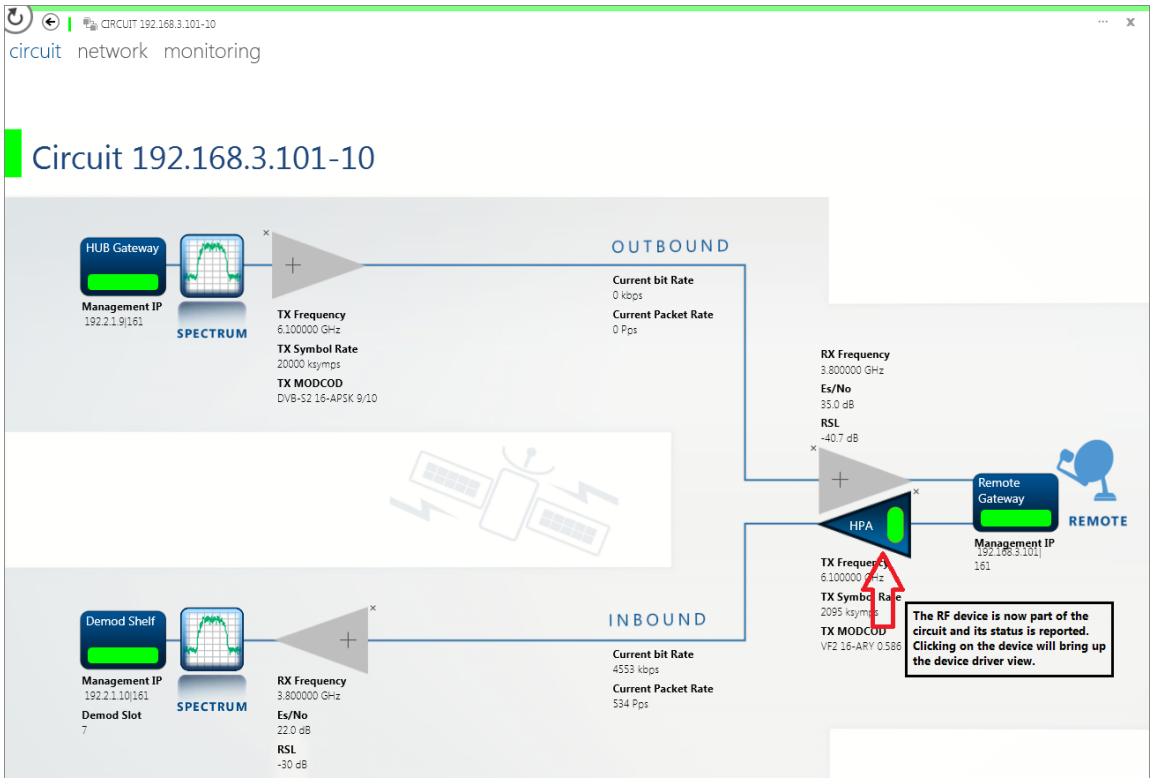


Figure 3–70. Circuit View with RF Device

3.8.6.2.4.3 Auto–learn QoS Configuration

Auto–learning the QoS Configuration is a feature supported in Heights firmware 2.4.x and newer. This feature provides functionality that helps keep NetVue and the outbound/inbound QoS configuration in–sync as the network is built and/or re–built.

To use this feature, each hub and remote QoS Group (with the exception of the default QoS group) must have their pairing ID set such that the remotes that are listed in the hub QoS group attribute list have their QoS group pairing ID set the same pairing ID as the hub QoS group. If these IDs do not match, then there is a chance that in the event the network is re–built, NetVue won't know how to link the remote to the proper hub QoS group and a circuit will not be made.

There are three ways to configure the remote QoS group pairing ID:

- Adding the remote to the hub QoS group.
- Manually configuring the pairing ID of the remote (inbound) QoS group.
- Pre–configuring a remote before commissioning it into the network.

3.8.6.2.4.3.1 Add a Remote to the Hub QoS Group

When a remote is added to a hub QoS Group, the pairing ID value of the hub QoS Group will be assigned to the remote QoS Group. Make sure that the pairing ID of the hub QoS group is set before adding the remote, or the remote's QoS Group pairing ID will be set to 0.

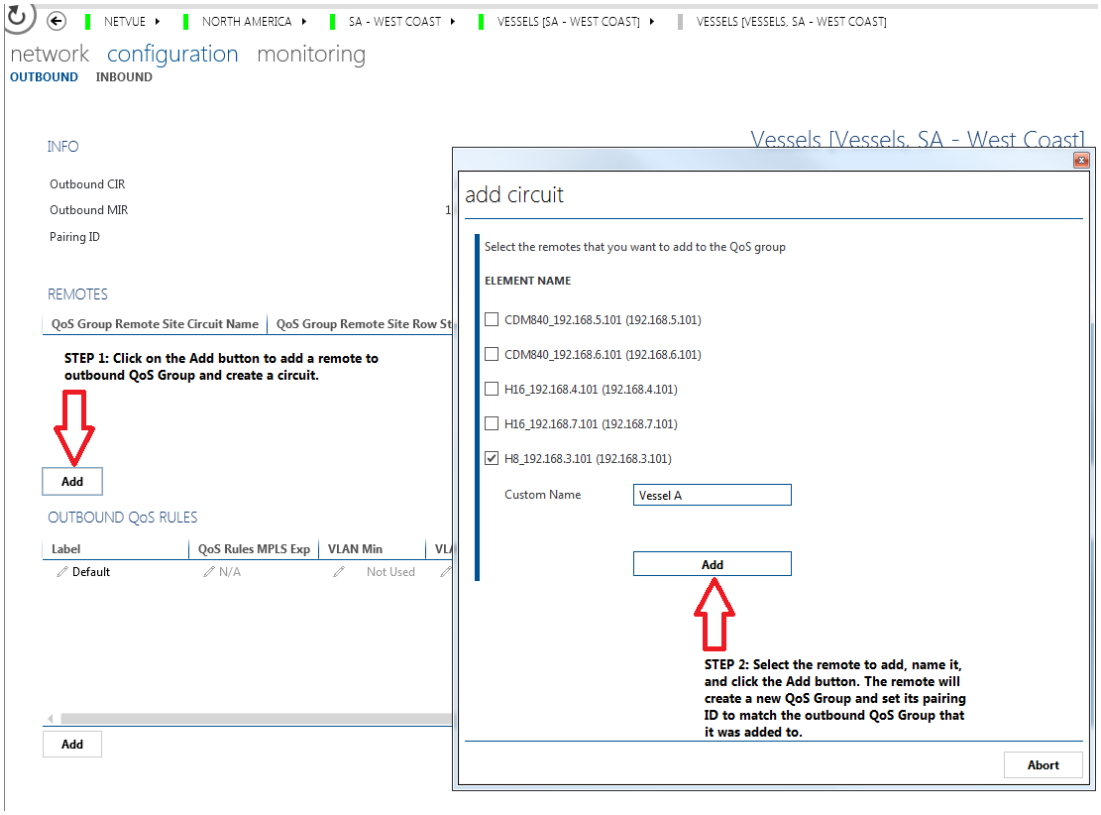


Figure 3–71. Add a Remote to a QoS Group with Pairing ID

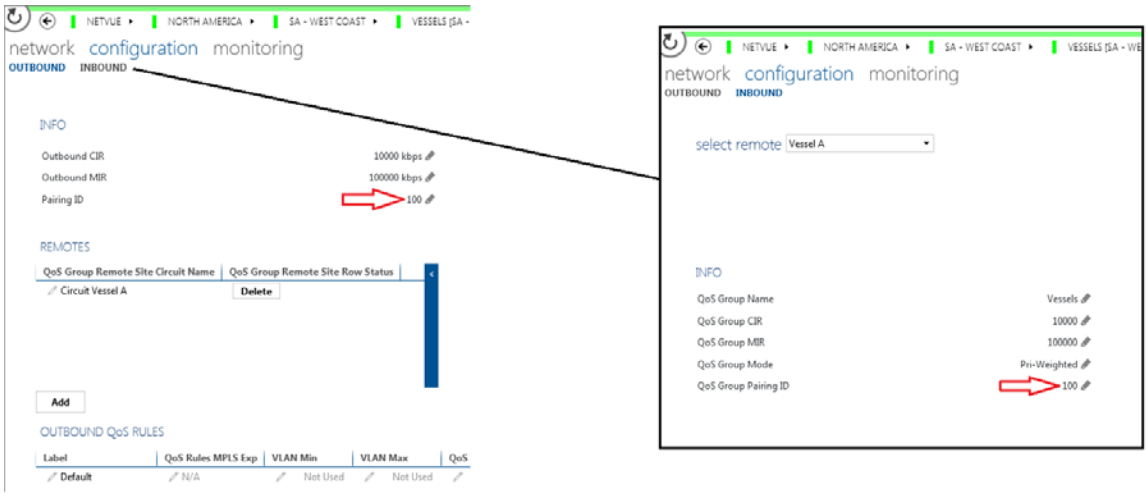


Figure 3–72. Remote QoS Group Pairing ID Automatically Configured

3.8.6.2.4.3.2 Manually Configure Remote QoS Group Pairing ID

For existing networks where the outbound/inbound QoS groups were created outside of NetVue, the best way to introduce the QoS configuration to NetVue is to manually configure the outbound/inbound QoS Group pairing IDs and then have NetVue perform a linking update.

3.8.6.2.4.3.3 Pre–configure a Remote before Commissioning

Another approach that is used is to pre–configure a remote device before it is deployed and commissioned. When configuring the QoS groups, make sure to set the pairing IDs such that they are properly matched with the outbound QoS Groups that the remote is planned to be a part of. When the device is installed and commissioned, a simple click of the “Force QoS Group Pairing” button will add the remote to the outbound QoS Group and create the circuits.

For example, if there is a hub QoS Group with a pairing ID of 100 and a remote QoS Group that is to be linked to it, then the remote QoS Group pairing ID needs to be manually configured to a value of 100 and the “Force QoS Group Pairing” button needs to be pressed to trigger NetVue to scan for changes.

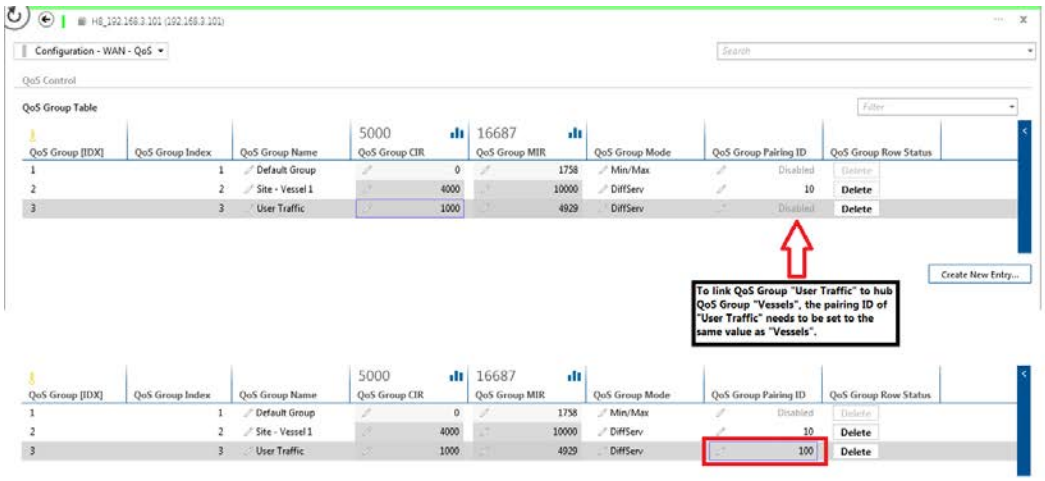


Figure 3–73. Configuring Remote QoS Group Pairing ID

This figure shows that the hub QoS Group pairing ID is set to 100 and that it doesn't know about the remote, the remote QoS Group, or the circuit.

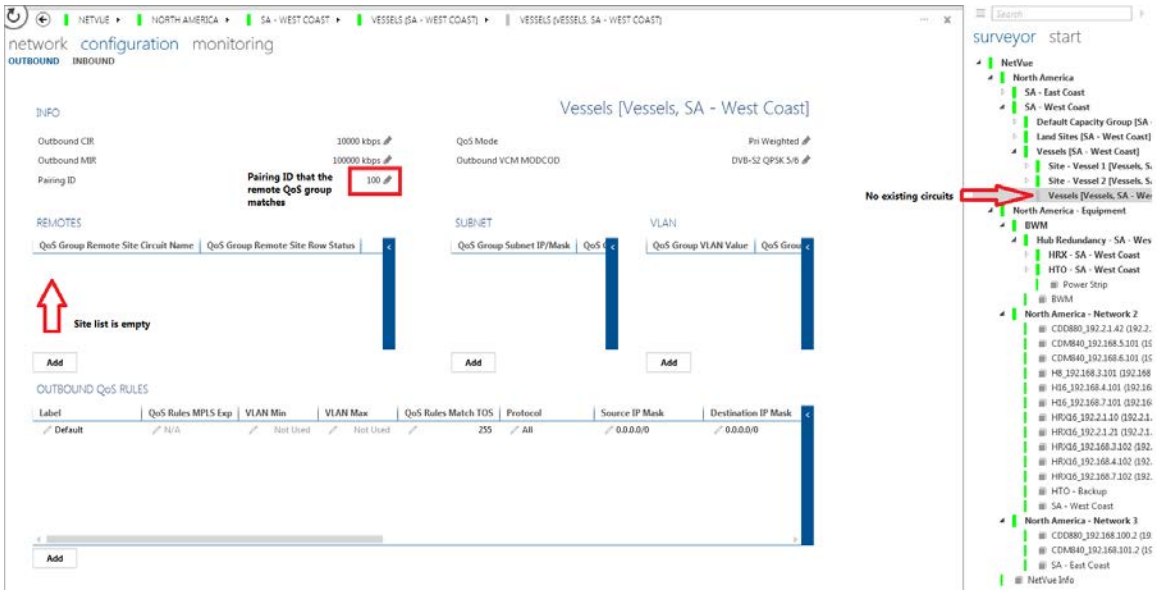


Figure 3–74. Outbound QoS Group before Pairing

Click on the "Force QoS Group Pairing" button in the Service Area–>Configuration–>General view to trigger NetVue to scan for new pairings.

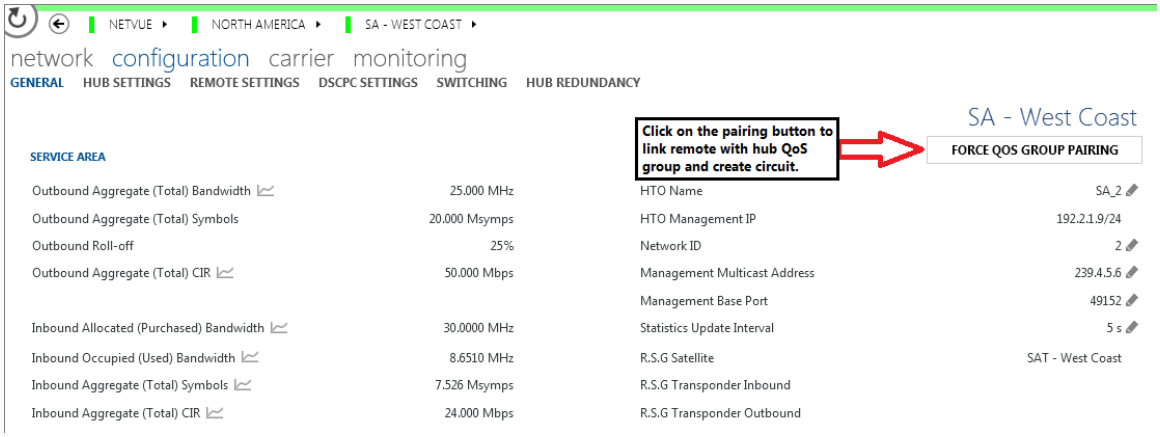


Figure 3–75. Force QoS Group Pairing

After NetVue has finished scanning the network for new pairings, it will automatically add remotes to the paired hub QoS Group(s) and create the circuit(s).

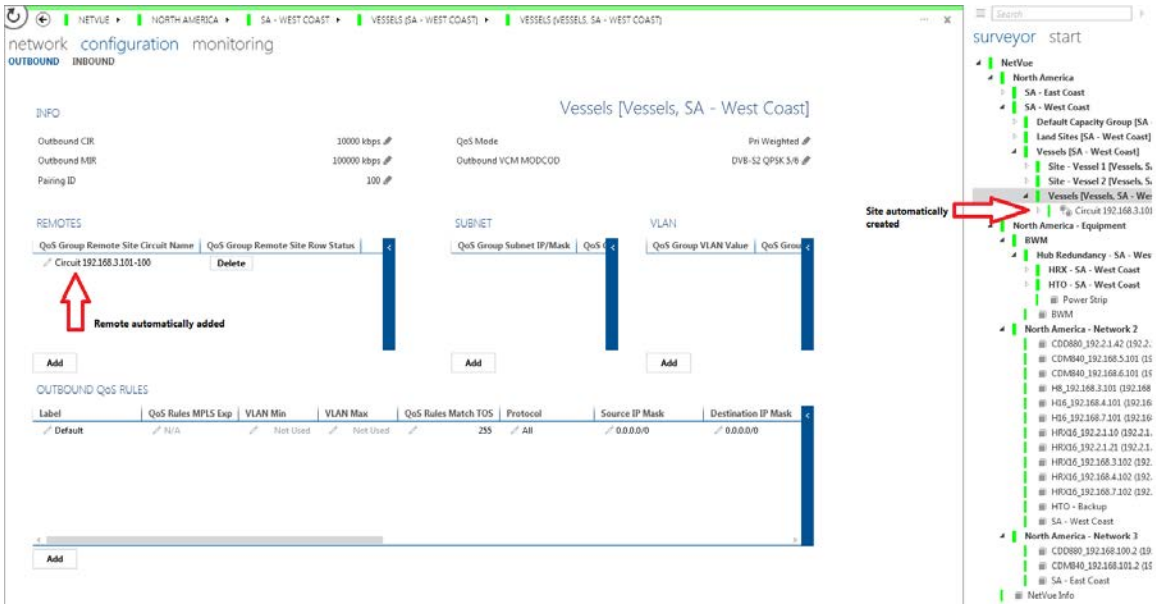


Figure 3–76. Automatically Created Pairing and Circuit

3.8.6.2.5 Configuration - Point–to–Point Service Area (Beta)

Automated Point–to–Point Service Area provisioning will be supported in a future release. It is currently supported via the NetVue manual provisioning application. For more information on automated provisioning, refer to Section 5.2.5.1 – Point–to–Point Networks.

3.8.6.3 Monitoring

The Monitoring page shows different statistics for each level viewed. Use it to see a snapshot of the bandwidth in use, and to drill down to see information specific to a level. NetVue Monitoring Views provide detailed information of the traffic performance and traffic shaping based on the Hub and the remote's QoS configuration. Starting at the QoS Group View, data is collected and is then aggregated up through the QoS hieracrchy to the highest level – The Service Area View. The trended data can be used for reporting bandwidth usage and CIR availability from a per site basis up to a per Service Area basis.

3.8.6.3.1 Service Group Monitoring

The Monitoring view at the Service Group level shows the aggregated traffic statistics for all managed devices under the Service Group. At the Service Group level, you can see the aggregated total Datarate (kbps), Symbols used (ksps) and total Satellite Spectrum under–managed for all of the devices in the NetVue management Service Group Monitoring Tab. There are three Service Group Monitoring pages (Reports, Trend Outbound, Trend Inbound).

3.8.6.3.1.1 Reporting

The Service Group Reporting page shows the aggregated statistics for all the Service Areas it contains. This includes cases where the Service Areas are AdvVSAT Service Areas or Heights Service Areas.

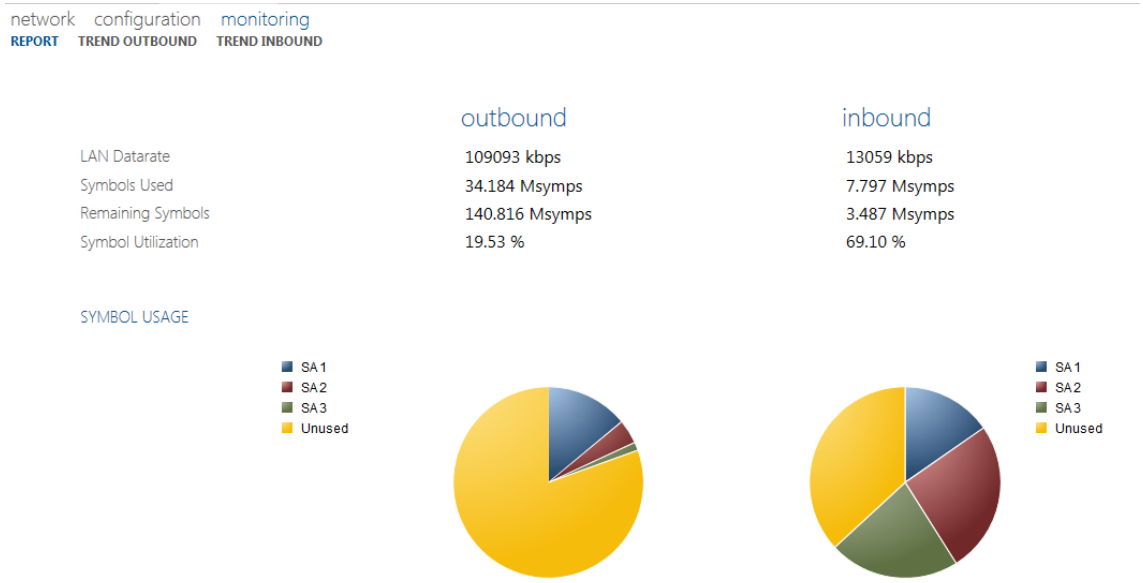


Figure 3–77. Service Group Report

The top half of the report page for the Service Group shows key statistics for both the Outbound and Inbound. The bottom half of the report page shows pie graphs of the symbol usage.

Table 3–8. Service Group Report Type and Description

Type	Description
LAN Data Rate	Total LAN Data throughput of all Service Areas.
Symbols Used	Total symbols used for all Service Areas to satisfy LAN data.
Remaining Symbols	Total unused symbols available from all Service Areas.
Symbol Utilization	The ratio of used symbols to total symbols presented as a percentage.

3.8.6.3.1.2 Trending

The Service Group Trending tab allows you to see the Symbol Utilization reported as symbols used and symbols unused per Service Area and for the Service Groups for both the Outbound and Inbound. The default view is the Last Day, with options to see the Last Hour, Last Week and Last Month. You can manipulate the Trend Graphs to see a specific area of interest.

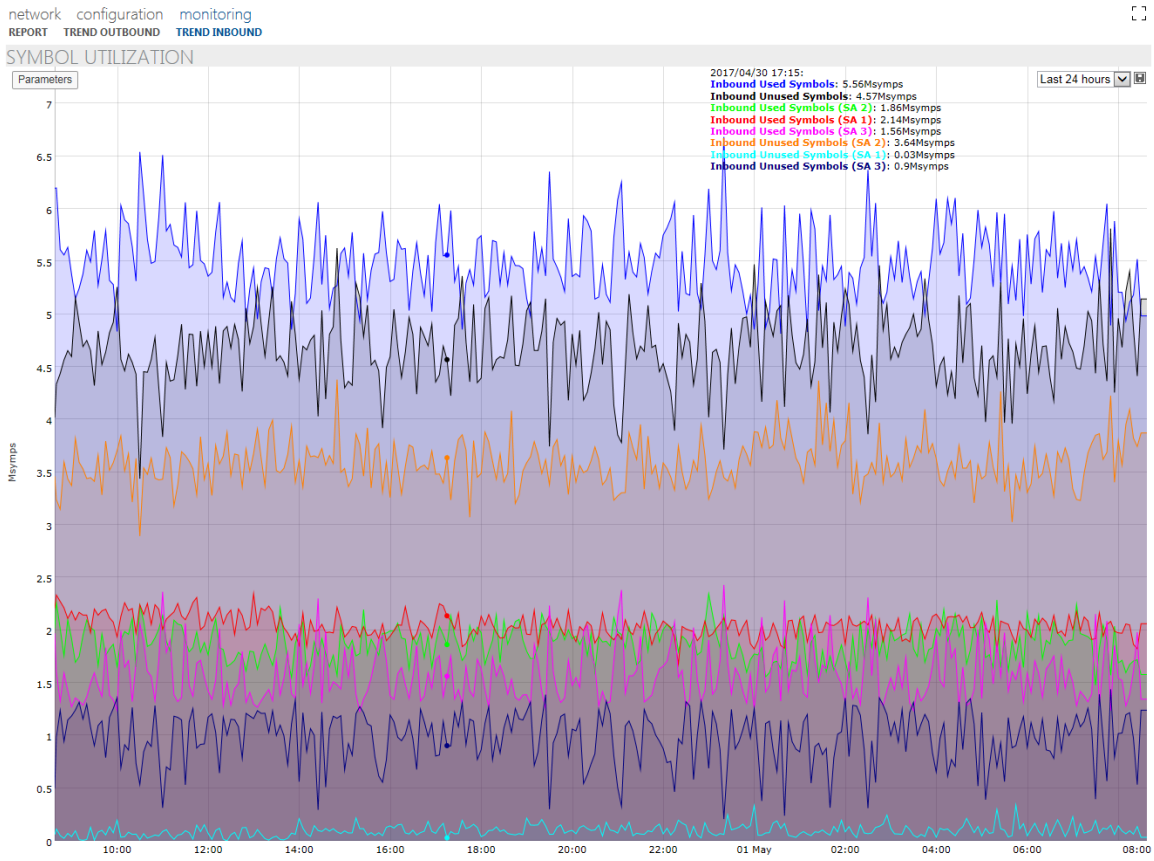


Figure 3–78. Trending Inbound

3.8.6.3.2 Service Area Monitoring

The Monitoring view at the Service Area level shows the aggregated traffic statistics for all managed devices in the Service Area. Each Service Area represents the aggregated statistics for all of the configured Capacity Groups.

There are five Service Area Monitoring pages: Capacity Groups, Bandwidth, MODCOD, Trend Outbound and Trend Inbound.

3.8.6.3.2.1 Capacity Group

The Service Area Capacity Group page is a display of the aggregated statistics for all the configured Capacity Groups in the Service Area.

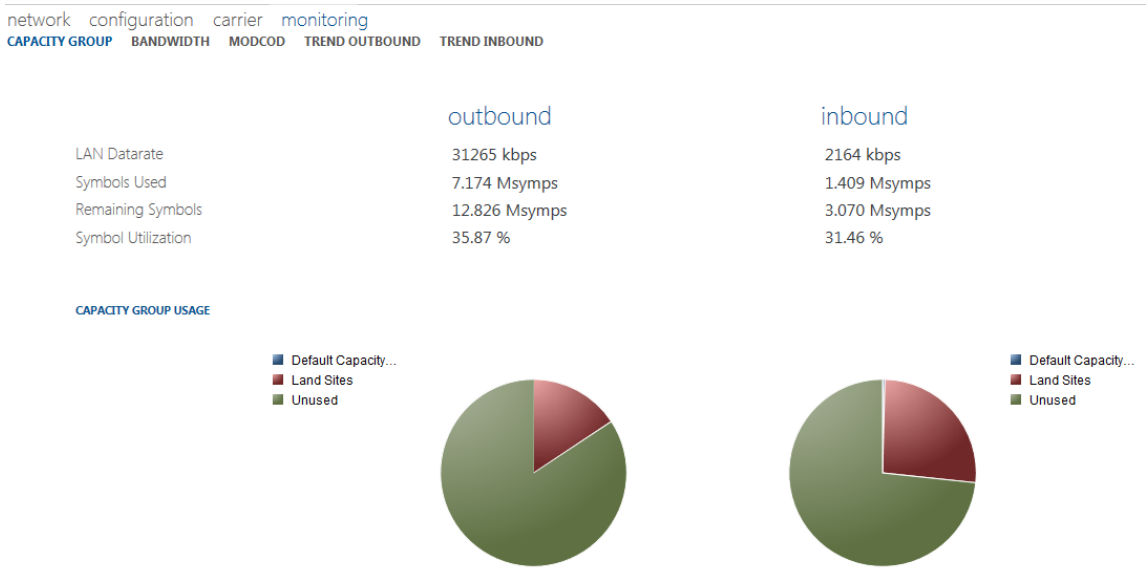


Figure 3–79 Service Area Capacity Group

The top half of the report page for the Service Group shows key statistics for both the Outbound and Inbound. The bottom half of the report page shows pie graphs of the symbol usage.

Table 3–9. Service Area Capacity Group Type and Description

Type	Description
LAN Data Rate	Total Occupied LAN Data Utilized sorted by Outbound and Inbound
Symbols Used	The amount of symbols being used by traffic
Remaining Symbols	The amount of symbols that are available for the outbound and inbound
Symbol Utilization	The usage of symbols

The Total Remaining Capacity (ksps) on the Inbound shows the current usage of the allocated Return Links.

When running in SCPC mode, this number is the sum of all statically–configured SCPC return links.

When the Return Links are managed by VMS, and are changing dynamically, the Total Remaining Capacity (ksps) shows the amount of available and unused Return Link capacity remaining in the configured Bandwidth Pools.

3.8.6.3.2.2 Bandwidth

The Bandwidth page shows the Capacity Group information, and gives more information on the bandwidth itself, including compression savings and Average LAN bits/Symbols per Second.

For information on the top portion of the statistics, see Capacity Group.

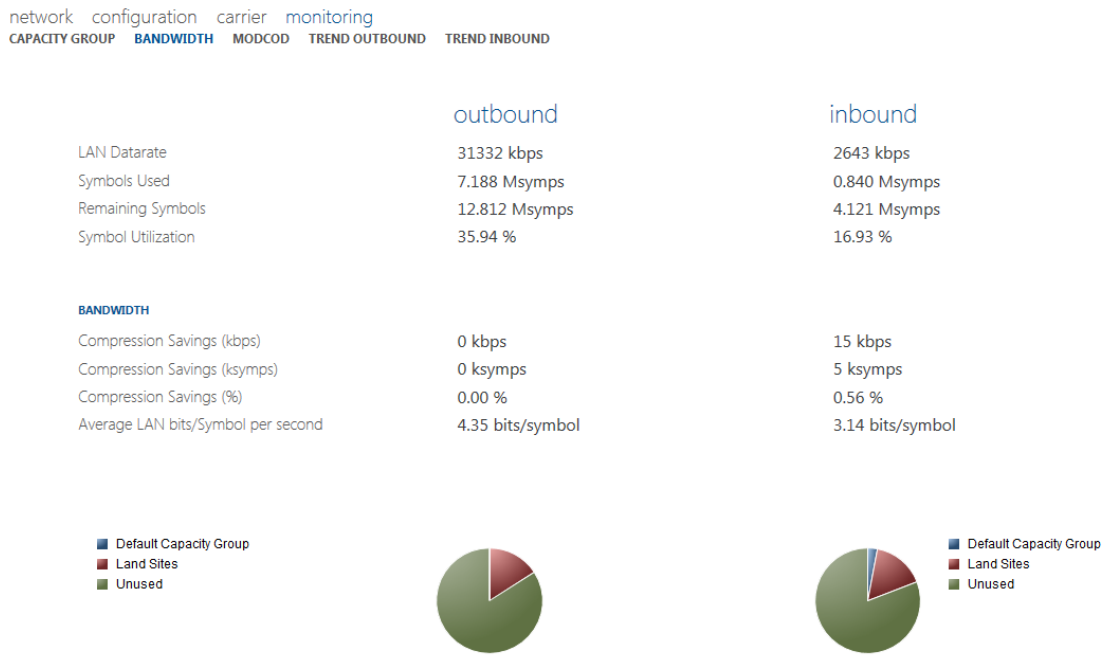


Figure 3–80. Service Area Bandwidth

Table 3–10. Service Area Bandwidth Type and Description

Type	Description
Compression Savings (kbps)	The amount of savings after Header and/or Payload compression is enabled in kbps
Compression Savings (ksmps)	The amount of savings after Header and/or Payload compression is enabled in ksmps
Compression Savings (%)	The amount of savings after Header and/or Payload compression is enabled in percentage
Average LAN bits/Symbol per second	Average Bits to Symbols per second
Total Symbols	Total Symbols in use

3.8.6.3.2.3 MODCOD

Use the Service Area Monitoring MODCOD to see the Outbound and Inbound utilization in the MODCOD. It shows the LAN Data Rate usage, similar to the Capacity Group.

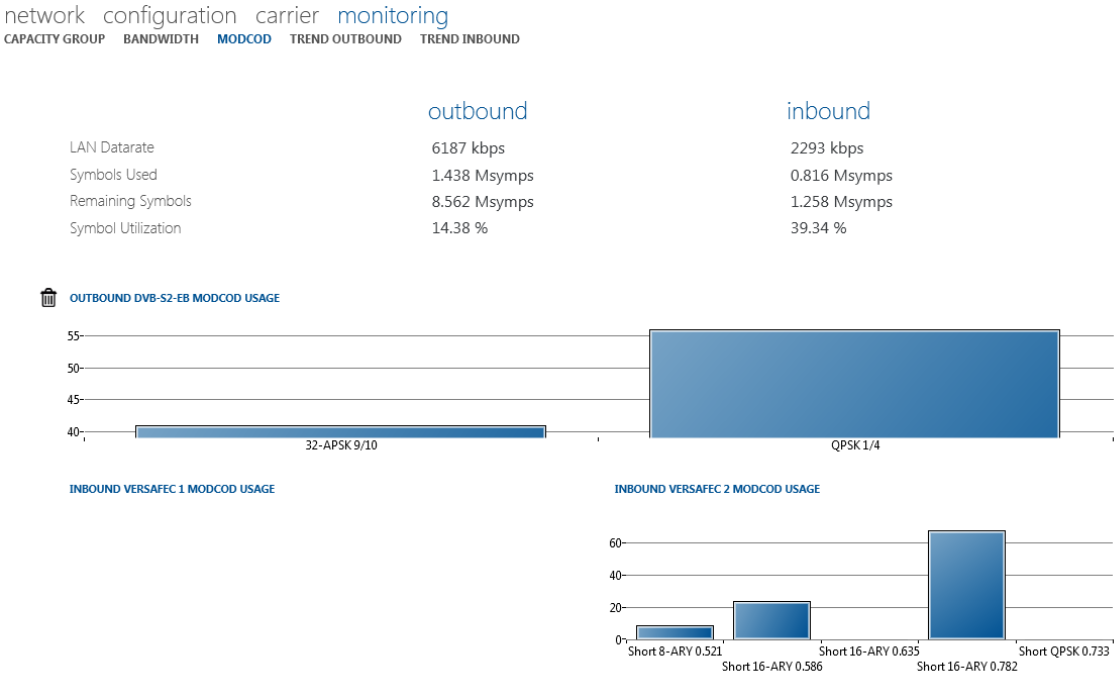


Figure 3–81. Service Area MODCOD Usage

3.8.6.3.2.4 Trending

The Service Area Trending tab lets you see the Symbol Utilization, CIR Availability and CIR Deficit for both the Outbound and Inbound. The default view is the Last Day, with options to see the Last Hour, Last Week or Last Month. Manipulate the Trend Graphs to see a specific area of interest.

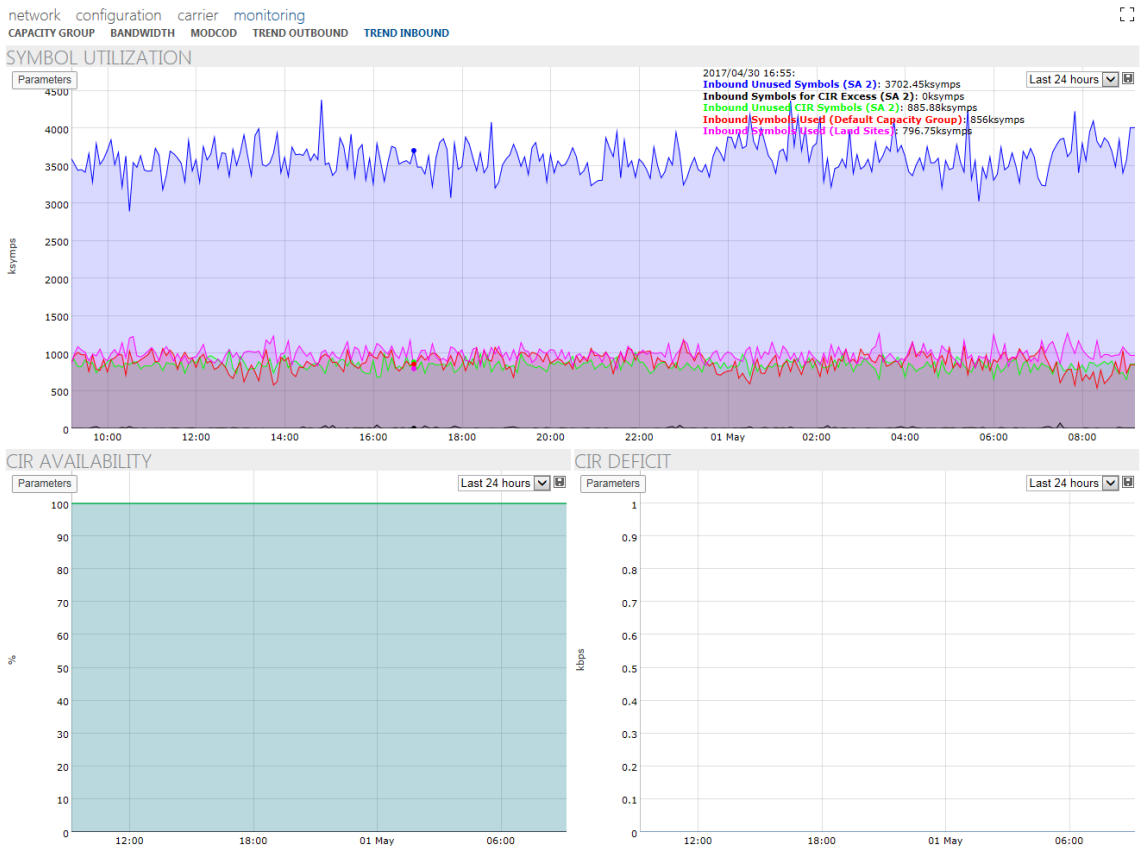


Figure 3–82. Trending Inbound

3.8.6.3.3 Capacity Group Monitoring

The Monitoring view at the Capacity Group level shows the aggregated traffic statistics for all configured QoS Groups in the Capacity Group.

3.8.6.3.3.1 Reporting

The Capacity Group Reporting page shows the aggregated statistics for all of the configured QoS Groups in the Capacity Group.

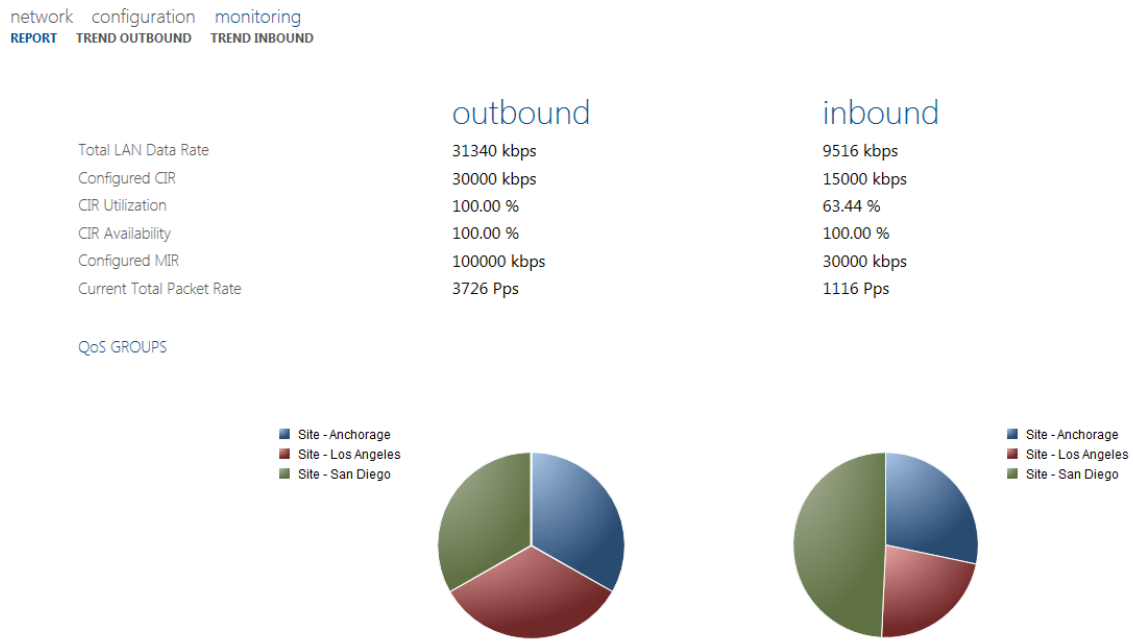


Figure 3–83. Capacity Group Report

The top half of the report page for the Capacity Group shows key statistics for both the Outbound and Inbound. The bottom half of the report page shows pie graphs of the symbol usage.

Table 3–11. Capacity Group Report Type and Description

Type	Description
Total LAN Data Rate	Total Occupied LAN Data Utilized sorted by Outbound and Inbound for the individual Capacity Group
Configured CIR	The aggregated Configured Committed Information Rate for all QoS Groups
CIR Utilization	The aggregated Committed Information Rate (CIR) for all QoS Groups
CIR Availability	The aggregated available Committed Information Rate (CIR) for all QoS Groups
Configured MIR	The configured Maximum Information Rate (MIR) accumulated for all QoS Group
Current Total Packet Rate	The current Packet Rate accumulated for all Service Areas

3.8.6.3.3.2 Trending

Use the Capacity Group Trending tab to see the Traffic Utilization and CIR Availability for both the Outbound and Inbound. The default view is the Last Day, with options to see the Last Hour, Last Week or Last Month. Manipulate the Trend Graphs to see a specific area of interest.

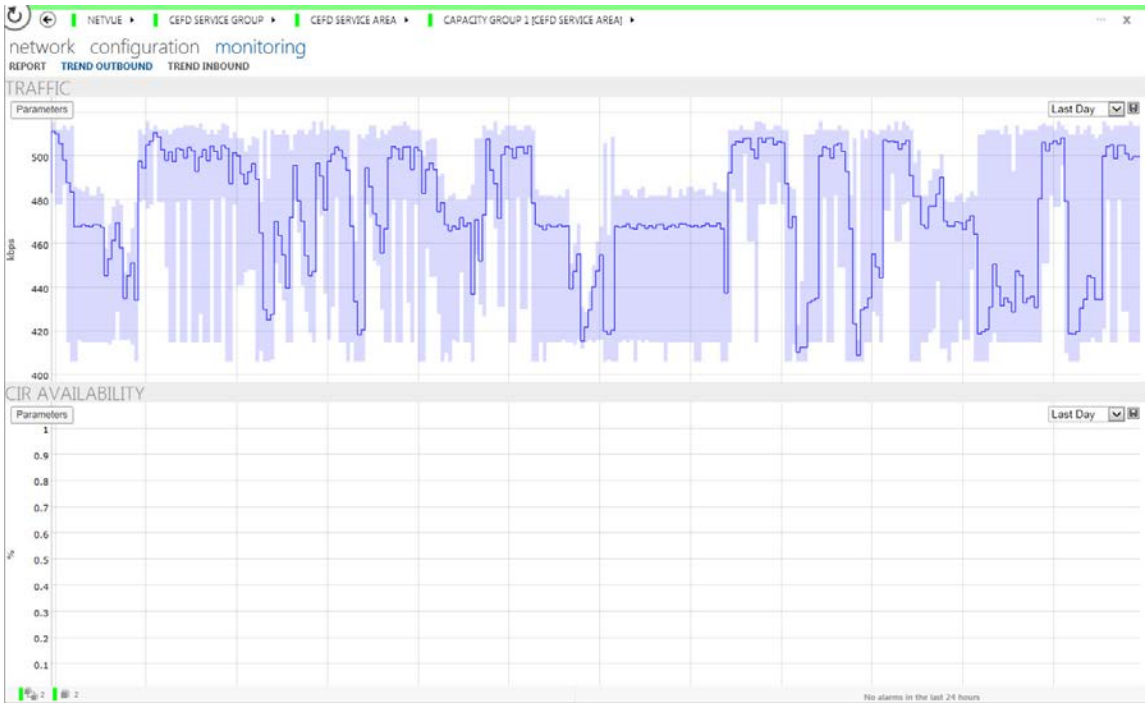


Figure 3–84. Trending Capacity Group

3.8.6.3.4 QoS Group Monitoring

The Monitoring view at the QoS Group level shows the aggregated traffic statistics for all managed devices in that QoS Group. There are six QoS Group Monitoring pages: Outbound, Inbound, Protocol, Trend Outbound, Trend Inbound and Trend Protocol.

3.8.6.3.4.1 Outbound

The QoS Group Outbound page is a display of the statistics for the configured QoS Group and the Rule Utilization.

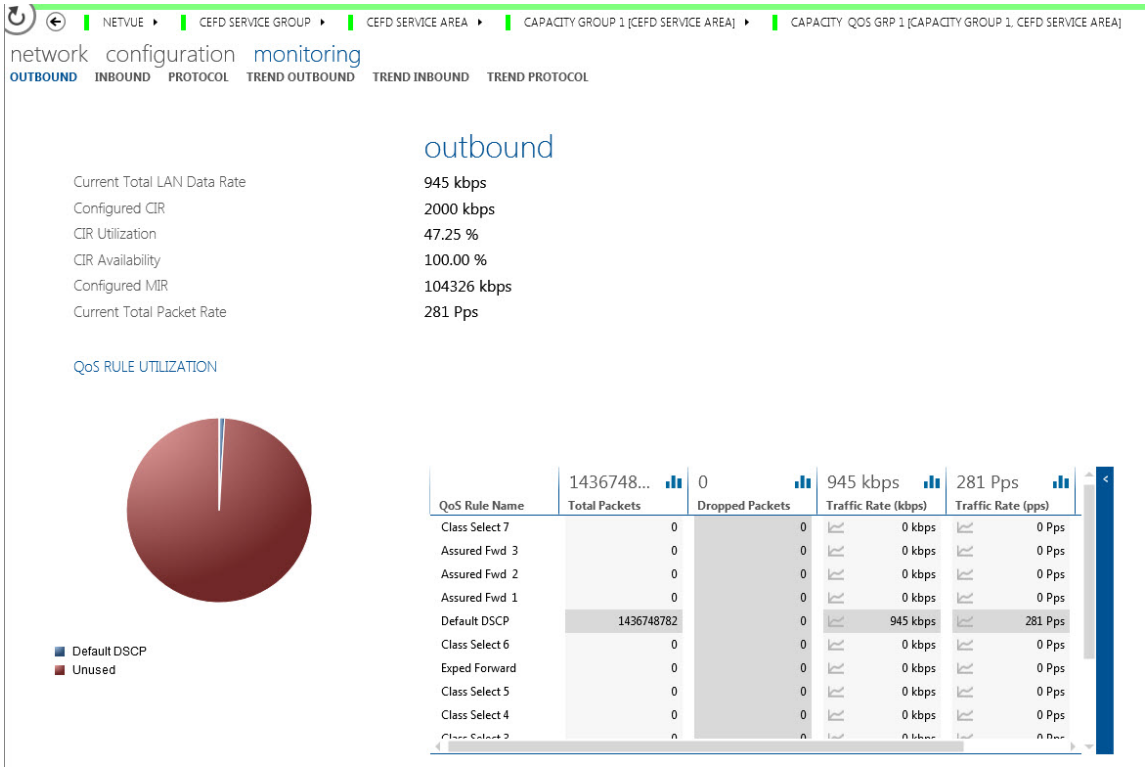


Figure 3–85. Capacity Group Report

The top half of the report page for the QoS Group shows key statistics for the Outbound. The bottom half of the report page shows the rule usage in a pie graph, and a table with each rule.

Any parameter showing this icon:  ***means that this value is being trended.***

Table 3–12. Capacity Group Report Type and Description

Type	Description
Current Total LAN Data Rate	Total Occupied LAN Data Utilized by the Outbound
Configured CIR	The Configured Committed Information Rate for the specific QoS Group
CIR Utilization	The Utilization of the Committed Information Rate in percentage
CIR Availability	The Availability of the Committed Information Rate in percentage
Configured MIR	The configured Maximum Information Rate (MIR) for the specific QoS Group
Current Total Packet Rate	The current Packet Rate for the specific QoS Group

3.8.6.3.4.2 Inbound

The QoS Group Monitoring Inbound page shows the aggregated statistics for all remotes or for a single remote.

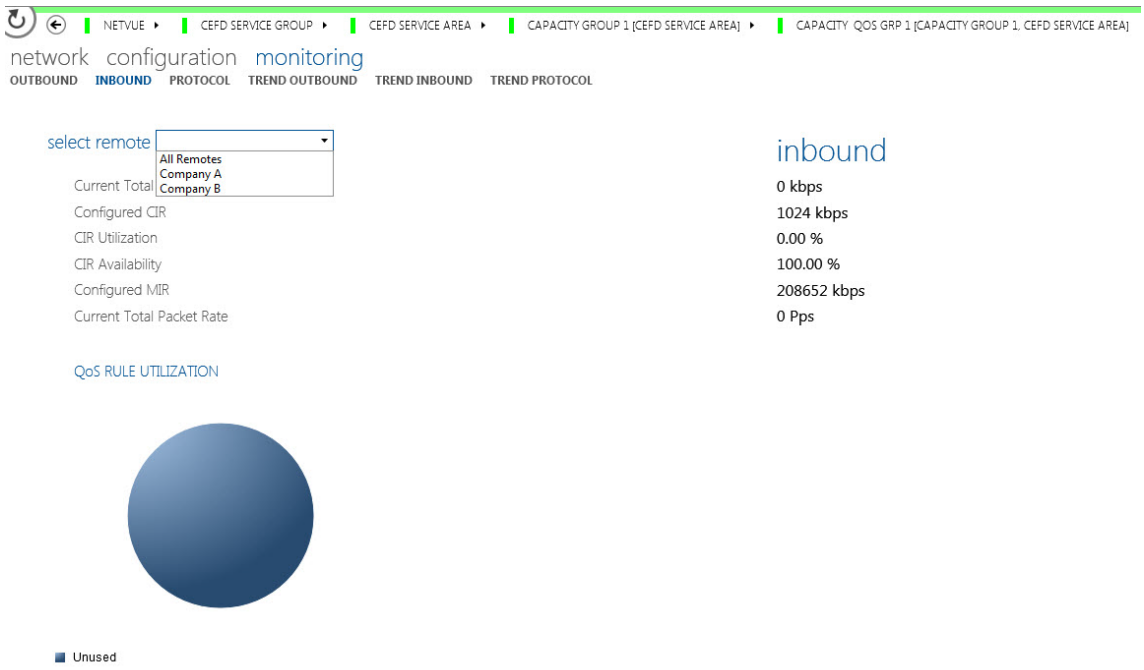


Figure 3–86. QoS Group Monitoring Inbound

The top half of the monitoring page for the QoS Group shows key statistics for a selected Inbound or for all inbounds. The bottom half of the report page shows the QoS Rule utilization.

Table 3–13. QoS Group Monitoring Inbound Type and Description

Type	Description
Current Total LAN Data Rate	Total Occupied LAN Data Utilized by the specific Remote Inbound or All Remote Inbounds
Configured CIR	The Configured Committed Information Rate for the specific Remote Inbound or All Remote Inbounds
CIR Utilization	The Utilization of the Committed Information Rate in percentage
CIR Availability	The Availability of the Committed Information Rate in percentage
Configured MIR	The configured Maximum Information Rate (MIR) for the specific Remote Inbound or All Remote Inbounds
Current Total Packet Rate	The current Packet Rate for the specific Remote Inbound or All Remote Inbounds

3.8.6.3.4.3 Protocol

The Protocol page is a display of the aggregated statistics for all of the Remotes that is QoS Group contains.

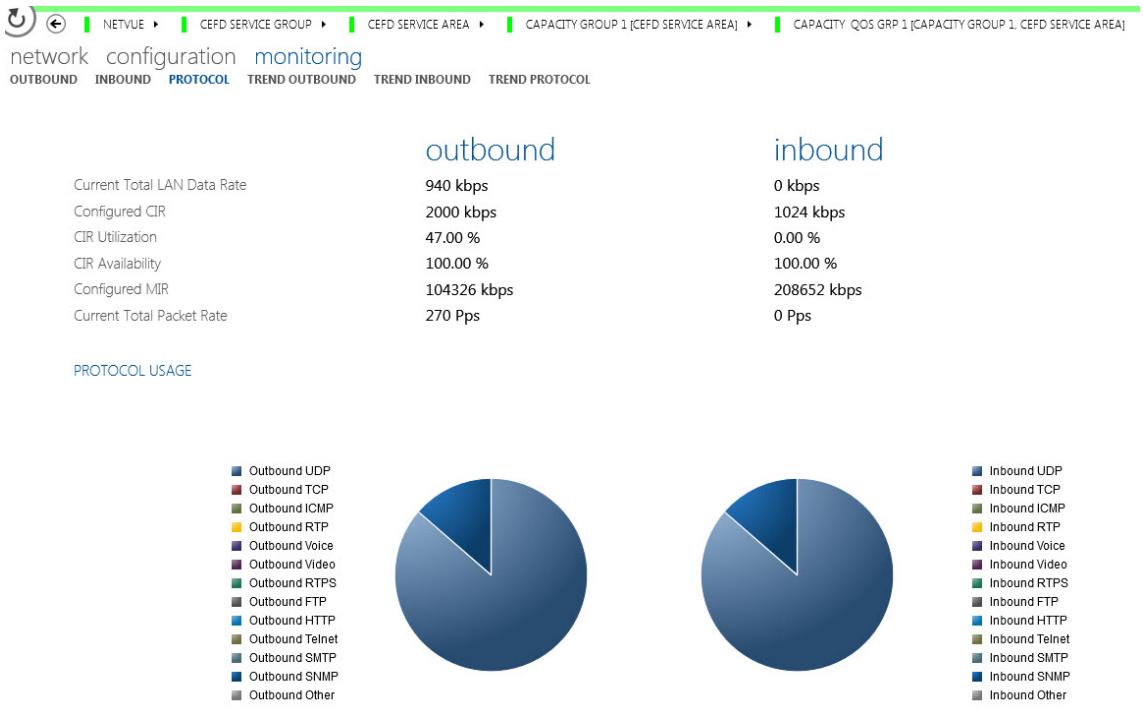


Figure 3–87. QoS Group Monitoring Protocol

The top half of the protocol page for the QoS Group shows key statistics for both the Outbound and Inbound. The bottom half of the report page shows pie graphs of the protocol usage.

Table 3–14. QoS Group Monitoring Protocol Type and Description

Type	Description
Total LAN Data Rate	Total Occupied LAN Data Utilized sorted by Outbound and Inbound for the individual QoS Group
Configured CIR	The aggregated Configured Committed Information Rate for the QoS Group
CIR Utilization	The aggregated Committed Information Rate (CIR) for the QoS Group
CIR Availability	The aggregated available Committed Information Rate (CIR) for the QoS Group
Configured MIR	The configured Maximum Information Rate (MIR) accumulated for the QoS Group
Current Total Packet Rate	The current Packet Rate accumulated for the QoS Group

3.8.6.3.4.4 Trending

Use the QoS Group Trending tab to see the Traffic Utilization and CIR Availability for the Outbound and Inbound, as well as the protocol usage for the Outbound and the Inbound. The default view is the Last Day, with options to see the Last Hour, Last Week or Last Month. Manipulate the Trend Graphs to see a specific area of interest.

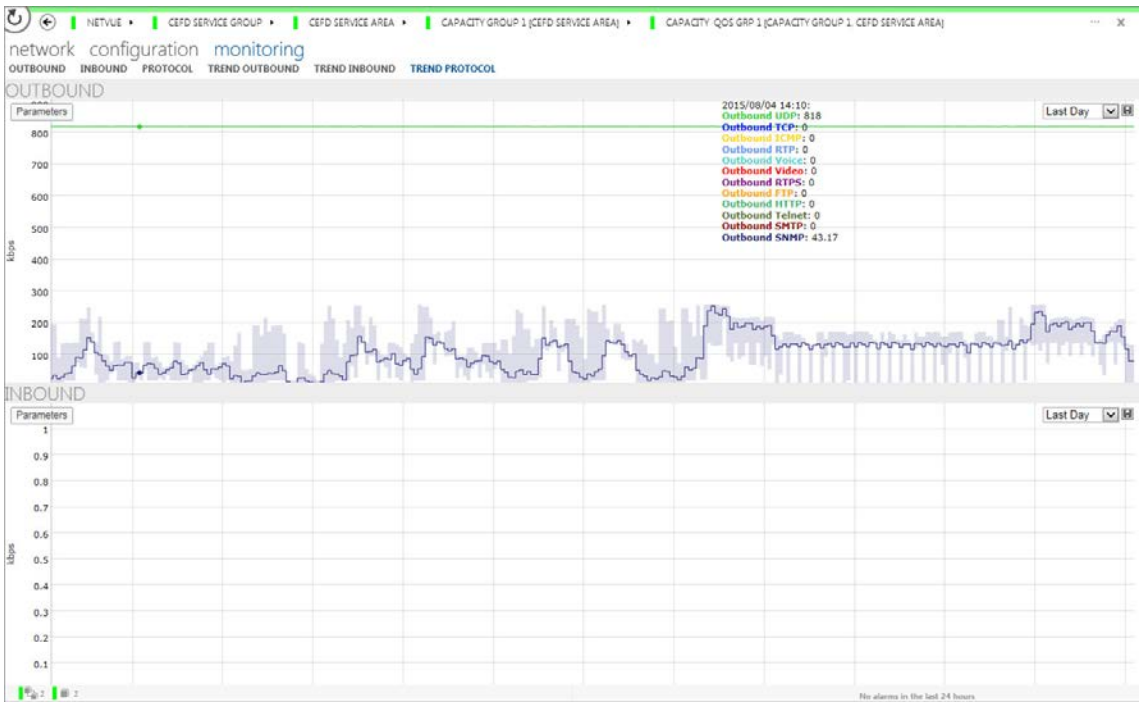


Figure 3–88. QoS Group Trending Protocols

3.8.6.4 Carrier

The Carrier View is located at the Service Area Level. It gives a synthetic view of the return carriers and ECM placement.

The Carrier View is a synthetic view of the return carriers. It does not replace an actual Spectrum Analyzer.

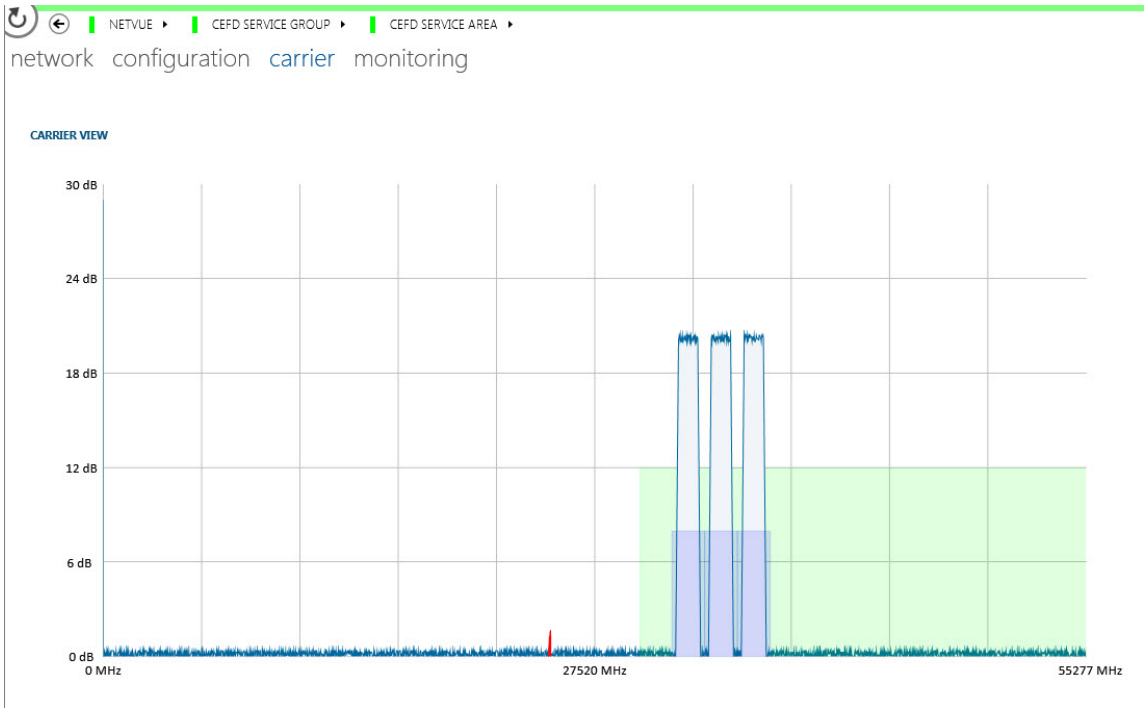


Figure 3–89. Carrier View

3.8.6.4.1 Hub View

The Hub is the location of the NetVue Server. The Hub inventory list shows the common or hub gear installed at the hub location.

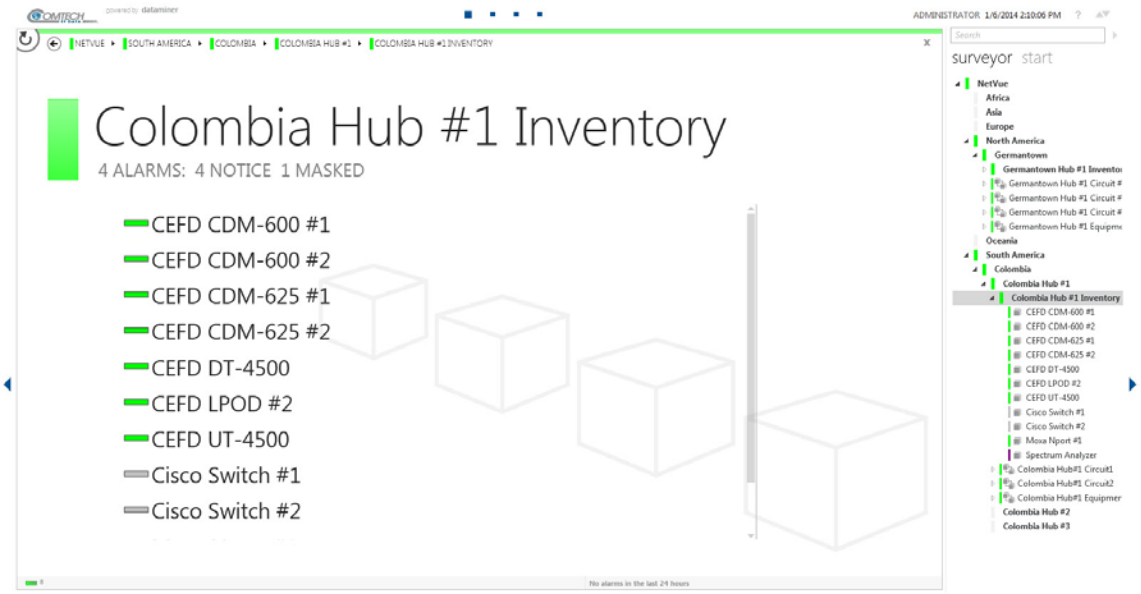


Figure 3–90. NetVue Cube Hub View

3.8.6.4.2 Circuit View

The Circuit View is a link between the Outbound and Return Link for a specific site. The Circuit View has three tabs: Circuit, Network and Monitoring.

The Circuit View tab shows equipment at both the local and remote ends of the circuit, as well as key performance indicators.

The Network tab gives the geographical location of a specific remote site.

The Monitoring tab gives you the means to trend the Outbound and Inbound Link Rate and ES/No, as well as the performance of the hub and remote equipment.

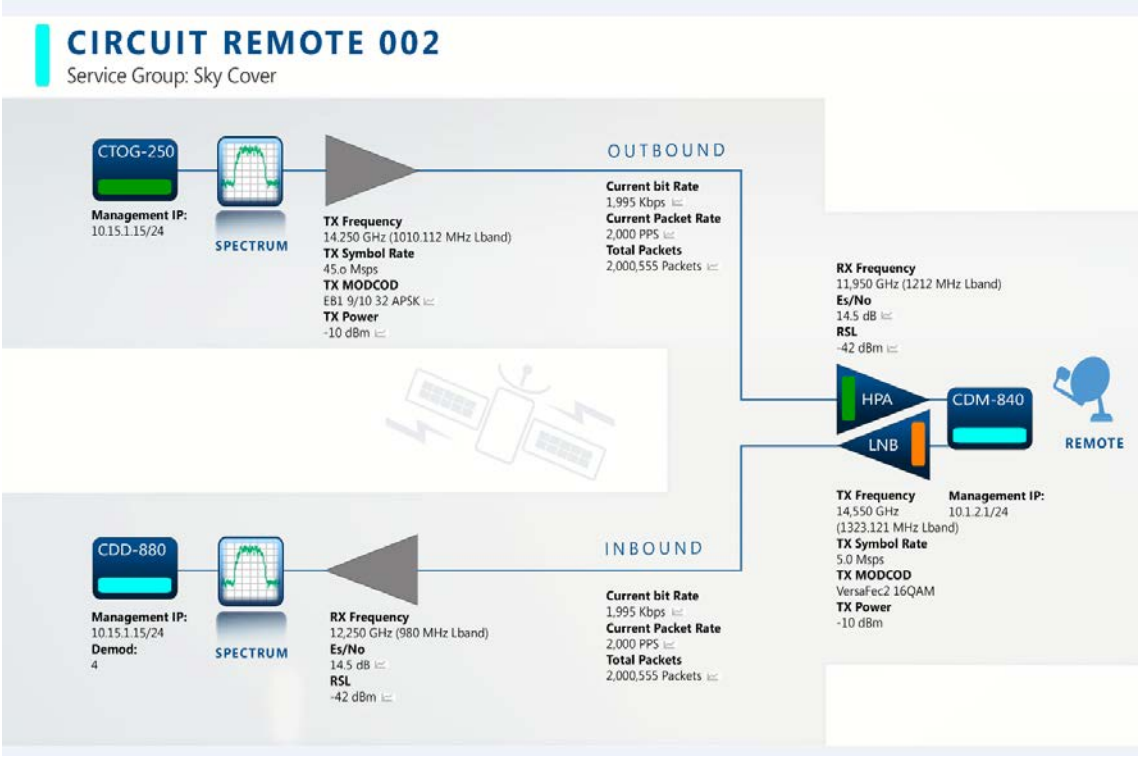


Figure 3–91. NetVue Cube Circuit View

3.8.6.5 Device

The Device View shows specific details for the selected equipment. Rotate the Card to configure specific parameters for the selected device.

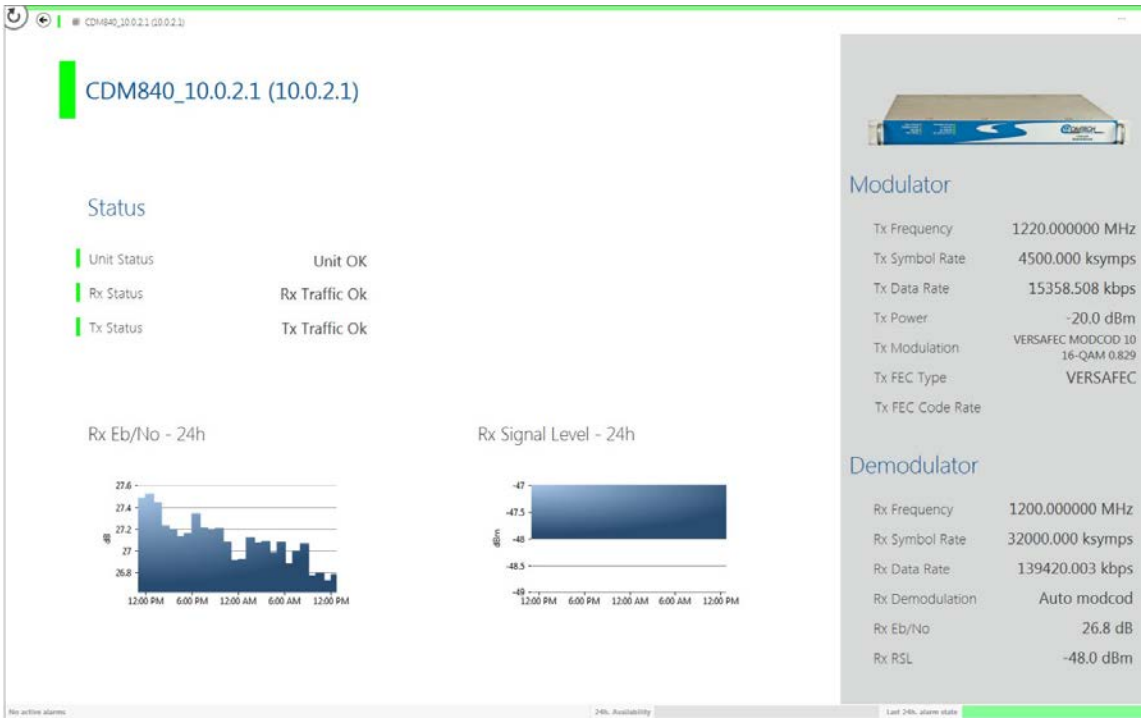


Figure 3–92. NetVue Cube Device View

3.8.7 Events/Alarms

Use the Alarm console to examine, manage and process Alarms.

Only users with the* Alarm console Access *permission have access to the Alarm console.

3.8.7.1 Open and Close the Alarm Console

When you open NetVue, the Alarm console is collapsed. The collapsed Alarm console is also called the *Alarm bar*.

The Alarm bar shows the total number of active alarms, and the numbers of active alarms grouped by severity.

- To open the Alarm console as a *temporary pane*, click the left–hand side of the Alarm bar.
- To close a temporary Alarm console pane, click anywhere in the NetVue interface, but outside of the Alarm console pane.
- To open the Alarm console as a *fixed pane*, double–click the left–hand side of the Alarm bar, or click the *Expand* button at the right.

3.8.7.1.1 Fixed Pane Icons

The fixed–pane Alarm console has three icons in the top right corner:

- Undock
- Maximize/Restore
- Collapse

These icons control the views of the fixed–pane Alarm console.

- **Undock** – opens the Alarm console in a separate browser window; close this window to restore the docked view

  If you change the size of the undocked Alarm console, the change occurs across sessions.

- **Maximize/Restore** – maximizes the Alarm console to a full screen view, or restores the previous view

  While the Alarm console is maximized, every Element card opened from within the Alarm console is undocked in a separate browser window.

- **Collapse** – minimizes the Alarm console to hide it from view; restore the Alarm console view with the **Expand** button at the right of the Alarm bar.

3.8.7.2 Alarm Tabs

The Alarm console has three tabs in the default layout:

- Active Alarms
- Information Events
- Masked Alarms

You can open new tabs and rename or close existing tabs as necessary.

If NetVue detects an Alarm storm (an unusually large amount of Alarms entering the system), then Alarm tab sorting and grouping is delayed until all Alarms have entered the Alarm Console.

3.8.7.2.1 Open a New Tab

1. Click the + (plus) button on the rightmost tab to open a new tab.
2. On the new tab, select the type of information you want to see:
   - **Reopen Closed Alarm Lists** – Click one of the listed items to reopen a recently closed tab.
   - **Show Current** – Click one of the listed options to open a predefined tab, or click *Apply Filters* to refine the list.
   - **Show History** – Click one of the listed items to see the Alarms of the last hour/day/week/month. Use the checkboxes or *Apply Filters* to refine the list as necessary.

3.8.7.2.1.1 Apply Filters

Click **Apply Filters** to select predefined Alarm filters, or to specify a custom time frame. You can combine these selections into a single query using logical operators.

3.8.7.2.1.2 Reopen Closed Alarm Lists

When you add a new tab to the Alarm Console, you will see a list of recently–closed Alarms listed under the **Reopen Closed Alarm Lists**.

This list can have a maximum of ten items. When the maximum is exceeded, the oldest items in the list are deleted automatically.

Protect an item from deletion by clicking the *Pin* icon beside it. A horizontal rule separates the pinned and unpinned items.

3.8.7.2.2 Close a Tab

Click the **X** button on the tab to close it.

3.8.7.2.3 Rename a Tab

Alarm tabs named *new tab* cannot be renamed, unless you apply an Alarm filter. You can specify a new Alarm tab name after a filter is applied.

1. Right–click the name of an Alarm tab.
2. Click **Change Tab Name**.

3.8.7.3 List Columns

If NetVue detects an Alarm storm (an unusually large amount of Alarms entering the system), then Alarm tab sorting and grouping is delayed until all Alarms have entered the Alarm Console.

3.8.7.3.1 Sort a List by a Specific Column

You can sort a list according to the contents of a selected column. A small *Up* or *Down* arrow to the right of the column header shows the sorting order.

1. Click a column header to sort the list.
2. Click the column header again to reverse the sort order.

3.8.7.3.2 Show or Hide a Column

1. To open the **Add/Remove Column** submenu, right–click any column header in the list.
2. Find the name of the column to show or hide, and check or clear the check box next to it.

3.8.7.3.3 Change the Position of a Column

Drag the column header to a different position.

3.8.7.3.4 Reset the Column Layout to the Factory Default

1. To open the *Add/Remove Column* submenu, right–click any column header in the list.
2. Click *Set Default Columns*.

3.8.7.4 Filter Alarms and Information Events

Use these *Filter* options to refine and focus the Alarms or Information Events that are listed on a tab.

3.8.7.4.1 Filter with Content

Enter text into the **Filter** box. As you enter text, results are filtered progressively, and shown in the suggestion box. For example, if you type "fra", the suggestion box shows all parameters having “fra” in the name (“frame rate,” etc.).

To clear the **Filter** box, click the red *X* on the right.

3.8.7.4.2 Filter with Special Syntax

Search the contents of a specific column – In the **Filter** box, enter the column name, a colon and the search value. Example: Enter “Value:50” to see all Alarms or Information Events that have “50” in the Value column (250, 7500, 2.50, etc.).

Search the contents of a specific column using a comparison – In the **Filter** box, enter the column name, a comparison operator and a value. Example: Enter "Service Impact"<2 to see all Alarms that have a service impact less than 2.

3.8.7.4.3 Filter with RCA Level

At the left of the **Filter** box, click the **Up** arrow, and move the RCA slider up or down.

3.8.7.4.4 Filter with the Active Alarms Time Line

The **Active Alarms** tab lists the active Alarms at this moment, by default.

To see Alarms that were active at a specific time in the past, use the time line at the bottom of the tab.

3.8.7.4.4.1 See Past Active Alarms

The time line is set to **Now** by default. Use one of these methods to see past Active Alarms:

- Move the white *point in time indicator* to the left, or
- Click the small clock icon on the right of the time line, then specify a date and time.

3.8.7.4.4.2 Change the Time Line Scale

At the right of the time line are small plus and minus icons. To change the amount of detail in the time line scale, click these icons.

3.8.7.4.5 Filter with the History Page Time Line

The **History Page** tab lists the Alarms that occurred during the last hour, day, week or month. The black bars in the time line show the quantity of alarms for a particular time.

You can customize the time period using the time line at the bottom of the **History Page** tab. Use one of these methods to change the time period:

- Change the time period start or end point: move the boundary indicator right or left.
- Specify dates for the time period: click the **From** or **To** time on the time line, and use the date chooser to set the dates.
- Select a preset time period: last hour, last day, last week or last month.

3.8.7.5 View Alarms and Information Events

3.8.7.5.1 Current Value

Click an Alarm listed in an Alarm console tab, and the **Current Value** box shows the current value of the Parameter that caused that Alarm. Click the ***Current Value*** box to open an Element card that shows more details about this Parameter.

3.8.7.5.2 More Details

The **More Details** function shows the complete life cycle of a listed Alarm. The evolution of the Alarm State over the last 7 days is represented graphically by a color bar. Hyperlinks are available for you to go to the related Element, and to see other Parameters of that same Element that are also in Alarm.

Use one of these methods to see *More Details* about a listed Alarm:

- Click the *More Details* button, or
- Double–click the Alarm in the list

3.8.7.5.3 Less Details

The *Less Details* function closes the More Detail view and restores the Alarm list view.

- Click the *Less Details* button, or
- Double–click the Alarm in the list

3.8.7.6 Manipulate Alarms and Information Events

Select a listed Alarm and choose from several possible commands and actions.

3.8.7.6.1 Command Menu

Frequently used commands are available in a menu on the right of the Alarm list.

- **Mask Alarm** – Masks the selected Alarm(s) or the associated Element(s); starts the **Mask** wizard.
- **Unmask Alarm** – Unmasks the selected Alarm(s) or the associated Element(s); starts the **Unmask** wizard.
- **Clear Alarm** – Clears the selected Alarm.
- **Copy Full Alarm** – Copies the details of the selected Alarm to the Windows Clipboard, ready for you to paste into other applications.

3.8.7.6.2 More Actions

Click the *More Actions* button to see more commands.

- **Take Ownership** – Declare yourself the owner of the selected Alarm.
- **Release Ownership** – Release your ownership of the selected Alarm.
- **Forced Release Ownership** – Release another person's ownership of the selected Alarm.

You must have the necessary rights to force the release of ownership.

- **Add Comment** – Add comment information to the selected Alarm.
- **Send by SMS** – Send someone a text message containing key information about the selected Alarm.
- **Set Alarm as Unread** – Mark an Alarm as unread.
- **View Connectivity** – See the RCA chain of the selected Alarm.

3.8.7.6.3 Right–click Menu

Right–click an Alarm in the list to open a shortcut menu showing these additional commands:

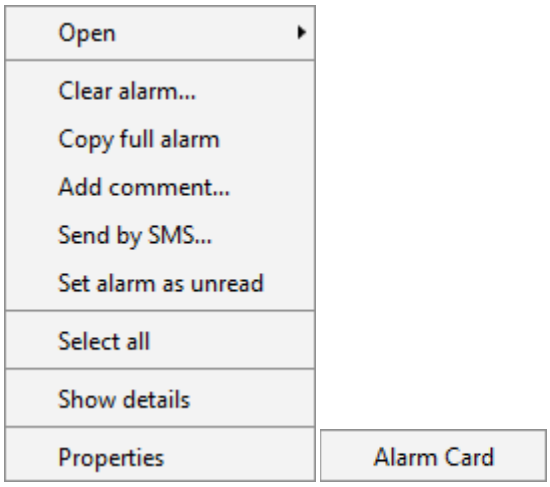


Figure 3–93. Right Click Menu

- **Open** – Opens a submenu with several items:
  - All Elements associated with the selected Alarms
  - All Views in which those Elements can be found
  - All Services containing those Elements
- Click a submenu item to open it in a new card.
- **Set Element State** – Sets the state of the Element associated with the Alarm.
- **Select All** – Selects all rows in the current Alarm console tab.

3.8.7.7 Configure the Alarm Console Tabs

The Alarm console tabs have several functional *Settings* that you can activate or deactivate with check boxes:

- **Auto Clear** – If checked, each cleared Alarm is automatically removed from the list.
- **History Tracking** – If checked, Alarm life cycles are not available to view.
- **Text to Speech** – If checked, new Alarms are audibly announced with a spoken message.
- **Freeze** – If checked, the Alarm list is *frozen*. Incoming Alarms and Information Events are not visible. While an Alarm list is frozen, incoming Alarms are stored. When the *Freeze* option is unchecked (deactivated), stored Alarms are immediately displayed.

  The Freeze option deactivates automatically after a specified period of time. By default, this period is 60 minutes.

- **Full Alarm Coloring** – If checked, the rows in the list are shown in colors related to the severity of the Alarms they represent.
- **Default Alarm List** – If checked, the current tab becomes the default Alarm list.

  When you collapse the Alarm console, the Alarm bar shows a summary of the data from the default Alarm list.

3.8.7.7.1 Activate or Deactivate the Settings

At the bottom of a tab, click the *Settings* button to see the list of available settings. The button has a small wrench icon.

Click the check boxes to activate or deactivate the settings as necessary.

3.8.8 NetVue Applications

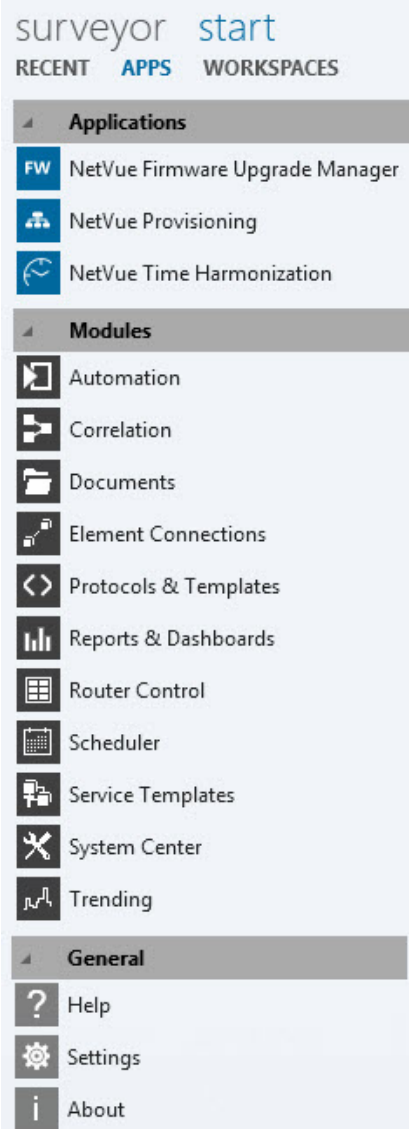


Figure 3–94. NetVue Applications

3.8.8.1 Modules: Extensions of NetVue

3.8.8.1.1 Automation

Automation lets you create scripts that can automatically take care of backup routines, system configuration, channel selection, report generation, notification via email or SMS, etc.

3.8.8.1.2 Correlation

Based on the rules set by the user, Correlation can create correlated alarms or send notifications via SMS or email to inform operators of certain events. It can trigger Automation scripts also, so that automatic countermeasures occur in case of emergency, or preventive actions occur in case of emerging problems.

3.8.8.1.3 Documents

Documents app lets you see all available documents stored on the NetVue Server. Any type of document can be stored within a 20Mb file size limit. Email addresses and Hyperlinks can be stored as well.

The client PC must have the application installed to open the document type.

3.8.8.1.4 Element Connections

Element connection app lets you define a connectivity change, which can be used for Root Cause Analysis.

The Connectivity tab is available only for elements that have in/out interfaces defined in their protocols.

3.8.8.1.5 Protocols & Templates

This is the interface to manage protocols for supported Devices in NetVue. Create, maintain and adjust Alarms and Trending Templates (see Chapter 8, Protocols in NetVue).

3.8.8.1.6 Reports & Dashboards

Manage the NetVue Reporting tool here. Collect Reports and create Dashboards. Dashboards are a collection of Reports organized on the same virtual page to be included/exported as part of the same view/document.

NetVue gives authorized users Dashboards for access to both real–time and historical NetVue System information. These customizable Dashboards combine critical information and key performance indicators (KPI) from many sources. Data sources include devices, locations, services and SLAs available in the operational environment.

Dashboards give authorized users a detailed view of operations. The intuitive Dashboard web interface is available directly through a web browser, or from within other NetVue applications. In NetVue applications, the information feeds into the selected Dashboard layout automatically.

Examples of some of the many Dashboard applications are:

- List of real–time amplifier KPI.
- Collection of data from different devices in a satellite uplink site to provide a single real–time overview of the key parameters.
- Compact real–time view on the status of all ports on a Cisco switch.
- Aggregated view for Service(s) and their statuses.
- Consolidated overview of all business SLAs, with key parameters.
- A collection of spectrum thumbnails for an overview of RF integrity for incoming satellite feeds and uplinks, HFC return paths, etc.
- A real–time overview of all KPI supplied by test and measurement solutions distributed in the operational environment.
- A list of all business high speed data connections and their key readings.

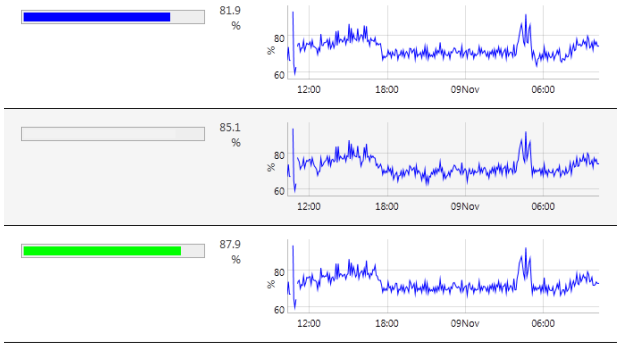


Figure 3–95. Example views from the Dashboard

Examples of Dashboard Components:

- Alarm indicator for Elements/Services/SLAs
- Real–time data
- Fixed text or titles
- Alarm indicator for Parameters
- Trend graph or values for Parameters
- Alarm quantity pie diagram
- Percentage of time in Alarm pie diagram

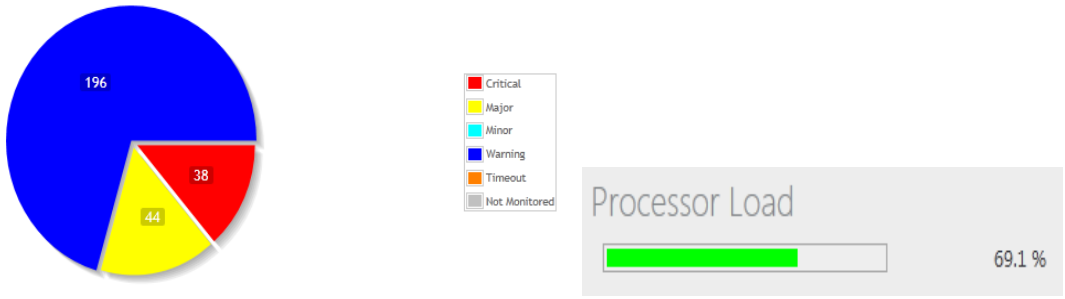


Figure 3–96. Dashboard Component Examples

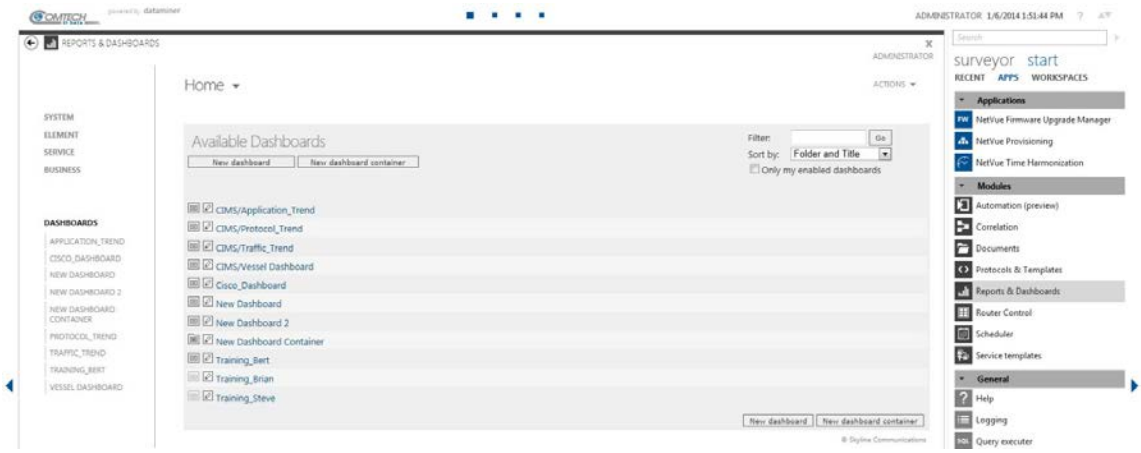


Figure 3–97. NetVue Report/Dashboard

3.8.8.1.7 Router Control

Router Control is a NetVue application that allows you to configure all matrices in your NetVue system in a single, customizable user interface.

When you open the app for the first time, you will find a default user interface (called a configuration) that contains a tab for every matrix found in your NetVue. Next to that default configuration, you can create additional configurations. All configurations can be customized, including the default.

3.8.8.1.8 Scheduler

Scheduler allows you to manage a list of scheduled tasks that you want the NetVue System to execute automatically.

3.8.8.1.9 System Center

System Center is the administrative control area. From within System center an authorized user can make modifications to the NetVue system.

3.8.8.1.9.1 System Center – Overview

System Center Overview gives an overview of your NetVue Servers. It shows information about the Agents Server Performance, Server Database, Server Backup Schedule, Trap Forwarding information, mobile gateway information (Not Supported in This Release), Users/Groups, who is online, as well as logging and tools.

All icons in the overview are selectable. Click any icon to go directly to the individual module for more specific information.

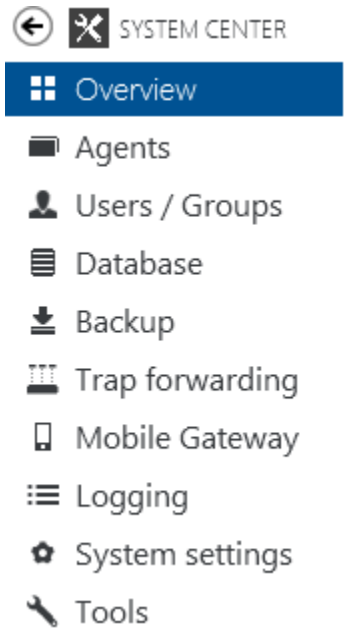


Figure 3–98. System Center

3.8.8.1.9.2 System Center – Agents

System Center Agents lets you see the server performance, such as processor load, free memory, free disk space, server uptime, DMA uptime and the number of elements contained for each NetVue server. You can manage each NetVue server and configure 1:1 NetVue redundancy within System Center Agents.

3.8.8.1.9.3 System Center – User/Groups

System Center Users/Groups is a fully integrated security module that lets you configure which users and groups have access to what parts of the system. Manage users with user profiles to set which actions they can perform, and to keep a detailed log of all user activity.

3.8.8.1.9.4 System Center – Database

System Center Database allows an authorized user to configure or modify the database to be local or central, or to add an additional database.

3.8.8.1.9.5 System Center – Backup

In the System Center Backup app, you can configure automatic backups that will run at regular intervals, and you can run an immediate backup when necessary.

3.8.8.1.9.6 System Center – Trap Forwarding

In your NetVue System, you can define a list of SNMP managers. These are third–party platforms, to which NetVue must forward SNMP traps.

3.8.8.1.9.7 System Center – Mobile Gateway

Not supported in this release.

3.8.8.1.9.8 System Center – Logging

In the System Center Logging app, the *Logging* page gives access to the various log files available in the NetVue System. On this page, you can examine log files to check the system health and troubleshoot any problems.

3.8.8.1.9.9 System Center – System Settings

In the System Center System Settings App, there are three subpages: *Upgrade*, *Logging* and *Notification Alarm Storm Prevention*.

The Upgrade subpage defines what actions must occur during the upgrade process, and defines the failover policy if 1:1 NetVue redundancy is used.

The Logging subpage lets you set the maximum size of the log files on this NetVue Agent.

To avoid flooding Cube with a large number of similar alarms, you can enable alarm storm prevention. When this function is enabled, set an *alarm storm start* threshold. This is the number of alarms with the same parameter description that will start the alarm storm mode. In addition, set an *alarm storm stop* threshold. This is the number of alarms with the same parameter description that stops the alarm storm mode. This way, alarm storm mode activates as soon as a quantity of alarms with the same parameter description exceeds the *alarm storm start* threshold. Alarm storm mode deactivates when the last quantity of alarms with the same parameter description is less than *the alarm storm stop* threshold.

3.8.8.1.9.10 System Center – Tools

In the System Center App Tools, you can do these tasks:

- Run queries on the NetVue Agent
- Synchronize the NetVue Agent
- Clean up unused protocols, alarm filters and Visio files

3.8.8.1.10 Trending

With trending, you can see and compare trend data logged by the NetVue System. With the trending App, you can see the trending information for one parameter, or for groups of parameters.

3.8.8.2 General: Help and Troubleshooting Section of NetVue

3.8.8.2.1 Help

Shows content of this document in HTML format.

3.8.8.2.2 Settings

User Account Settings, same as in the Header bar.

3.8.8.2.3 About

Contact information, software versions of the NetVue/NetVue modules and upgrade history.

Chapter 4. Bandwidth Manager

4.1 Bandwidth Manager Overview

NetVue communicates with the Vipersat Management System (VMS) through an interface that is proprietary to Comtech EF Data.

Once you configure NetVue and VMS to communicate, NetVue becomes the central command and controller while all the autonomous operations are managed by the VMS. The exchange between the bandwidth manager and NetVue is a partnership, where the NetVue asks the VMS for specific information and then builds a database structure of the required network components in the VMS.

This exchange can build the entire VMS database while providing complete control over the autonomous or manual operations.

Through the VMS, the NetVue Integrated Management System can configure and operate these parts of the system operation:

- System Configuration
  - VMS Manager
  - Redundancy (VMS)
  - Equipment Inventory Lists
  - Service Area
  - Sites
- Switching Operations
- Dynamic Bandwidth Management
  - Load
  - ToS (Application)
  - Diagnostic
    - Revert
    - Reset
- Guaranteed Bandwidth & Reservations

4.2 Introduction

In relationship to NetVue, the VMS server is a network element that gathers and processes information it receives from the hub apparatus and Remote Gateways that comprise an AdvVSAT or Heights satellite network. The Comtech EF Data Satellite Gateways measure, capture and transmit real-time network operating parameters to the VMS via unsolicited status messages or extended queries for more details.

The VMS receives, stores, and processes this data, and is used to update the NetVue configuration and status information, providing the intelligence for management of satellite bandwidth resources and dynamic switching operations. The NetVue client then shows the network data in an easy-to-interpret, graphic presentation.

Through the VMS proprietary interface, NetVue can customize each satellite network for controlling bandwidth resources and limitations associated with each service area by modifying system properties and site policies.

As the VMS receives a switching request from a Remote Gateway, it uses sophisticated algorithms to evaluate the request against available network resources and service area policies before sending a switch command back to the requesting remote to provide a new frequency and bit rate change. If the switch request is denied because of lack of available service area resources, for example; the remote will remain at its current state until the necessary resources become available.

4.3 System Configuration

4.3.1 Vipersat Manager

Vipersat Manager is used to configure the necessary addresses and timeout parameters. After the Vipersat server is activated, the VMS can establish communications with, and register, the apparatus in the network. The Vipersat Manager is the landing point where new devices, hub and remote units are categorized through a registration process, thus building inventory lists. The lists are autonomously formed as each unit reports in with a Resource Sharing Group ID, IP address and type of device; i.e., HTO-1, HRX-16, H8, H16, CDM-840…

Initially, this manager requires configuration of network parameters to allow IP communications. Several parameters provide the necessary addressing and timing for the overall networks available.

4.3.1.1 Parameters

In the General Tab shown in Chapter 5, figure 5-7, is the Management Multicast address of the VMS. It must match the Receive Multicast Address of the hub outbound(s). This address is used to propagate managing multi-command messages from the VMS to all receiving network units.

The Management Interface address is defaulted to 0.0.0.0 on new installations. You must change it to reflect the IP address of the NIC that connects the VMS server to the equipment LAN. This address configuration is necessary because of multiple LAN ports on the server.

The Base Port sets the starting IP port addressing for all VMS messages. Changing this address base affects the entire network, requiring configuration changes to all modems. Leave this setting at default C000 (49152) to avoid unnecessary configuration changes. Change this setting only if network port addressing is in contention.

The Type of Service (ToS) Value provides prioritization of VMS messages in cases where the forwarding router is congested or overloaded. Typically, the value is set to Class Selector 6 or 192 for priority queuing to make sure management/signaling messages are granted the highest passage level.

The Streamload Data Rate values control the amount of bandwidth required to GET and PUT unit firmware files. Set the rates not to exceed the network's forward transmission change bandwidth rates. These values are set low because the file transferred is small and requires little overhead. Default settings are usually acceptable.

The Timeouts tab shown in Chapter 5, are adjustable parameters to accommodate communications that require additional time because of network congestion. The default settings are suggested and should be sufficient for all conditions.

The Communications timer values set timeouts for command messages. The Retry Timeout is the wait between messages, which works with Retry Count. A retry count of three and a timeout of five seconds would set the message failure at a total timeout of 15 seconds with three attempts to command the managed unit.

If communication latencies are greater than default settings (command communication failures), increase the Retry Timeout value.

The Status Update Messages (SUMs) values set the dual timeouts and debounce for Remotes that are in SCPC mode or ECM.

- The SCPC Timeout parameter is the time interval between the sending of SUMs to the VMS by Remotes that are in SCPC mode.
- The ECM Timeout is the time interval between the sending of SUMs to the VMS by Remotes that are in Entry Channel Mode.
- The Debounce is a counter setting for the number of consecutive time intervals that can pass without the VMS receiving a SUM for a particular Remote unit, before a switch failure occurs for that Remote.

Generally, the SCPC Timeout is set to a relatively short interval to provide timely responses to switch requests. These requests can be caused by variations in load for Load Switching applications. For networks that support large numbers of Remotes that are often operating in ECM, a longer interval setting for ECM Timeout will reduce contention for shared bandwidth usage.

- The Heartbeat timer settings include the Interval, Timeout and Debounce values for Hub device redundancy messaging.
- The Interval parameter updates the modem to send its heartbeat message to the VMS at the set rate.
- The Timeout is how long the VMS will wait before finding communications failure and commanding a device redundancy switchover.
- The Debounce is a counter setting for the number of consecutive alarmed messages the VMS will receive from a Hub unit before a redundancy switch activates. This parameter setting is useful for reducing or eliminating unnecessary redundancy triggers caused by spurious alarms.
- The Announcement Period is the interval at which the VMS multicasts its management IP address to all listening units within the network(s).

The default value (15 seconds) enables the VMS to send the update message on a 15-second interval to establish the current managing address in all units set to receive the message.

4.3.1.2 Global Commands

NetVue provides the capability to perform global commands that are specific to the bandwidth manager and its interaction with the devices. The global commands are located in the **Bandwidth Manager->Details View** under the **Devices View**.

- Global Re-init – Forces the Bandwidth Manager to poll the network for device updates.
- Soft Reset – Causes the selected device to refresh all latched alarms.
- Hard Reset – Causes the device to reboot.
- Force Registration – Attempts to force the device to register with the Bandwidth Manager.

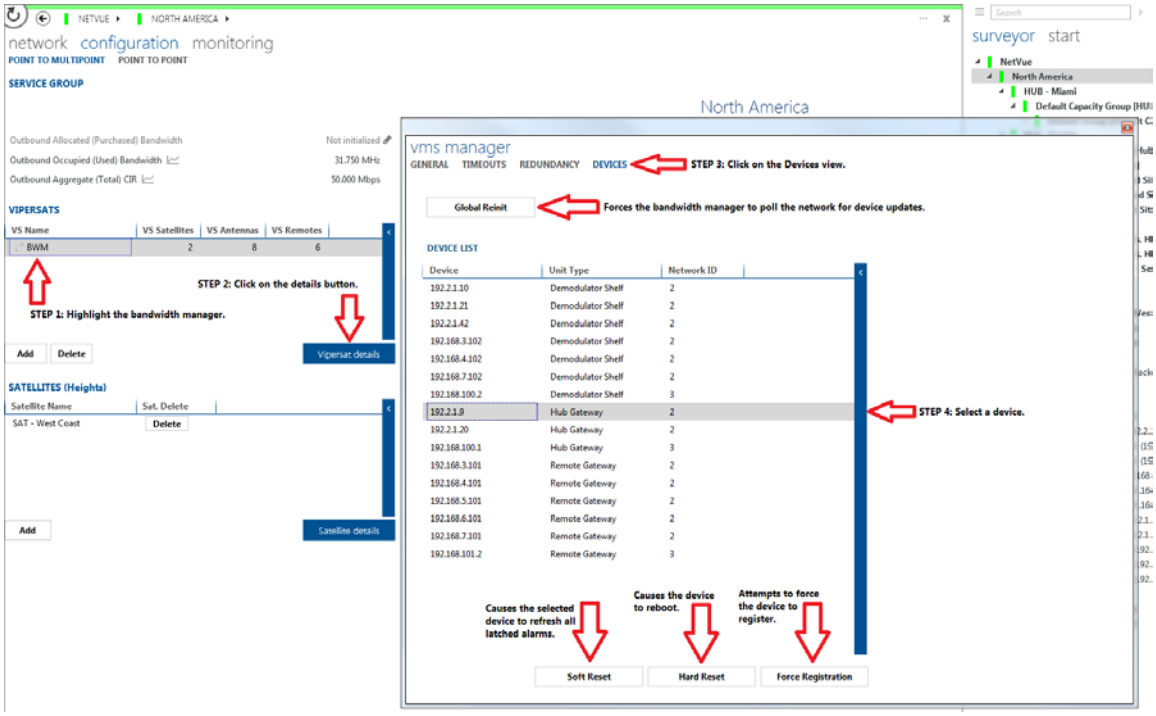


Figure 4-1. Bandwidth Manager Global Commands

4.3.1.3 Auto-learning Bandwidth Manager Configuration

Auto-learning the bandwidth manager configuration greatly reduces the burden on the user when re-building or upgrading the system. NetVue can take the existing configuration of the bandwidth manager (RF, devices, Sites, Hub Redundancy) and import it into NetVue. There are some restrictions that need to be followed, otherwise the import may fail or improperly import.

- The Service Area name will use the name of the Hub Site because the bandwidth manager doesn't have the concept of a service area, so name the Hub Site accordingly.
- Site names need to be unique. This is especially important for Hub Sites because it is used as the Service Area name.
- The Hub Redundancy container name needs to match the Hub Site name in order to ensure proper importing.

  To use auto-learning, it is assumed that the NetVue configuration is blank no elements exist (other than the root and NetVue Info elements).

4.4 Learn an Existing Bandwidth Manager Configuration

Click on the root level and Create a Service Group.

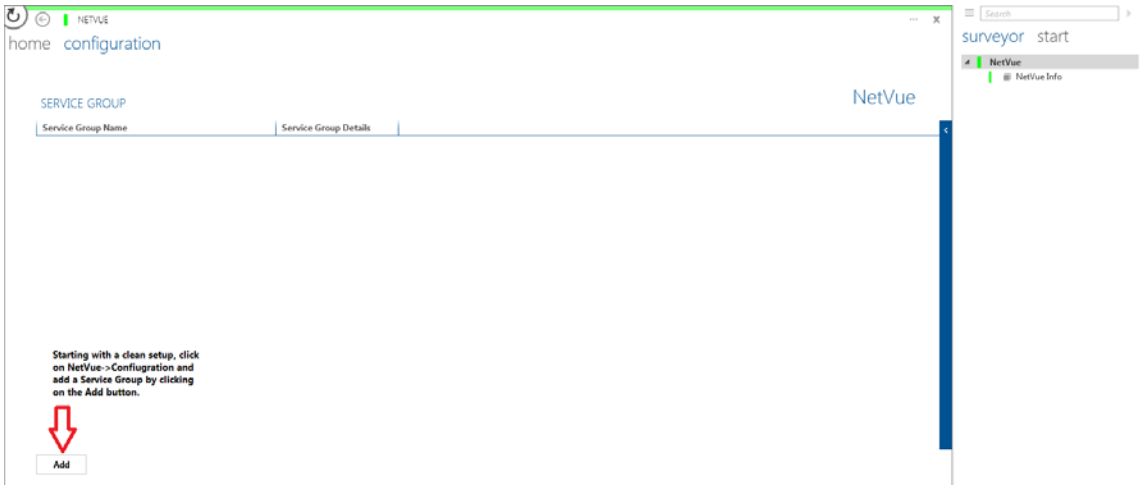


Figure 4-2. Creating a Service Group

Next, create a bandwidth manager and open the details view and click on the "Auto-learn" button.

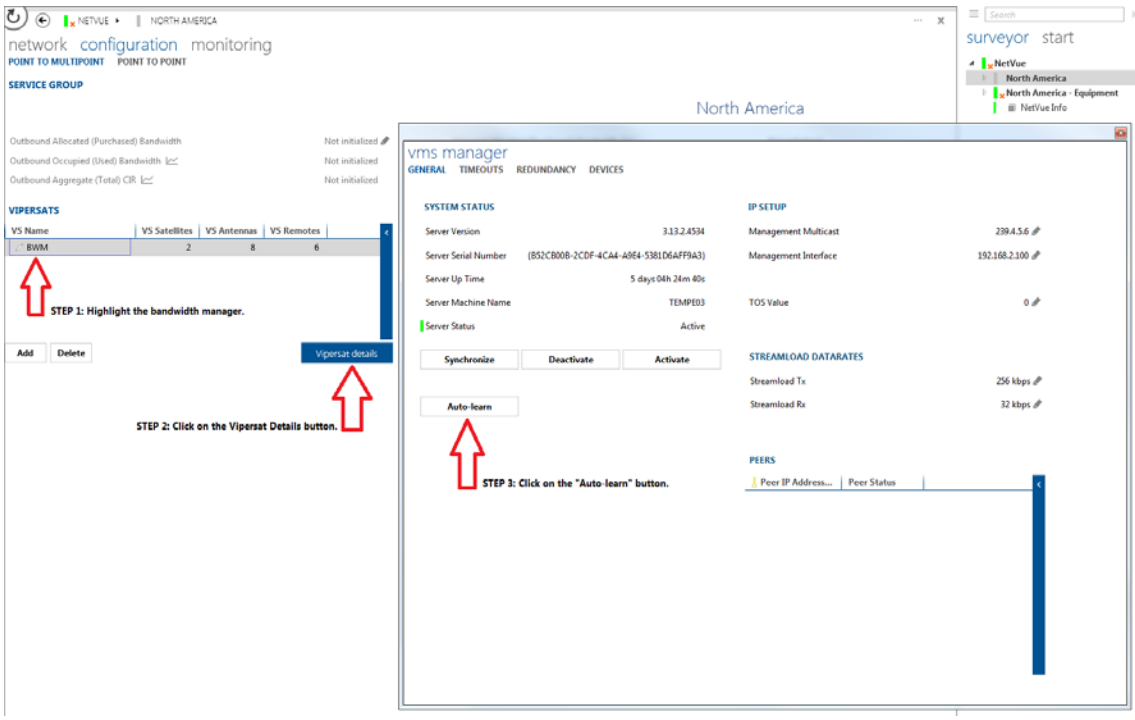


Figure 4-3. Bandwidth Manager Auto-learn

Once NetVue has finished importing the bandwidth manager configuration, the system is ready for use.

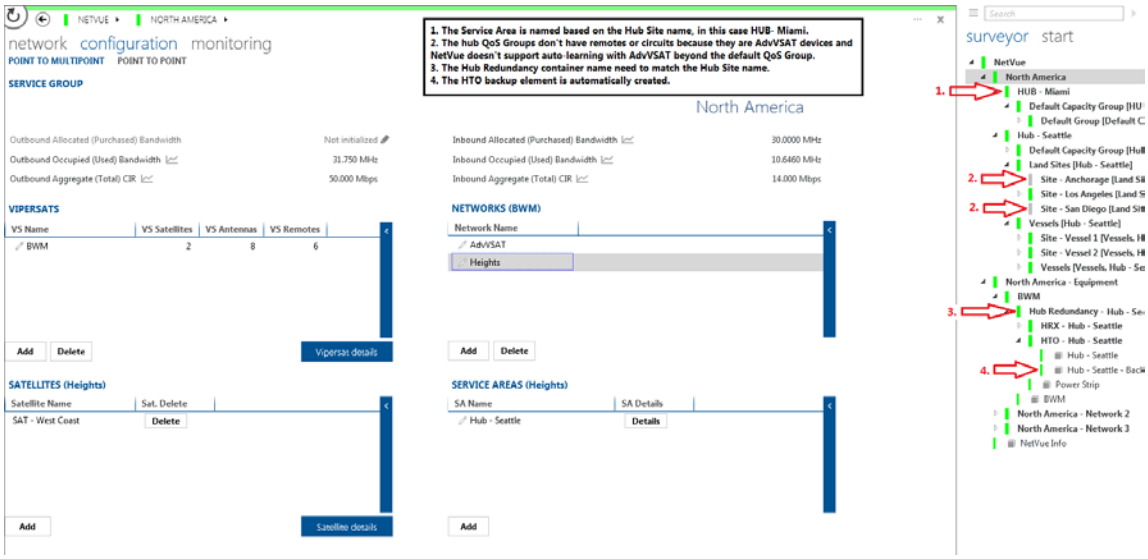


Figure 4-4. NetVue System After Bandwidth Manager Auto-learn

4.5 Re-import a Bandwidth Manager Configuration

If for some reason, the NetVue configuration needs to be re-built, it first needs to be cleaned of all non-NetVue elements before a new import can be performed. Cleaning NetVue of its configuration will destroy all circuit names, linkage, and any manually added linkage (RF devices for example). Any manually created linkages and user-defined circuit names will need to be re-done after the import.

4.5.1 Delete the NetVue Configuration

Clean up NetVue by deleting all non-NetVue elements in the following order:

1. Delete all Service Area elements.
2. Delete all Bandwidth Manager elements.
3. Delete all Service Groups elements.
4. Delete all device and circuit elements.
5. Delete the configuration from the database.
6. Restart NetVue.
7. Create a Service Group.
8. Create a bandwidth manager.
9. Click on the “Auto-learn” button in the bandwidth manager’s details view.
10. Add back any manually created elements and linkage.
11. Rename circuits as needed.

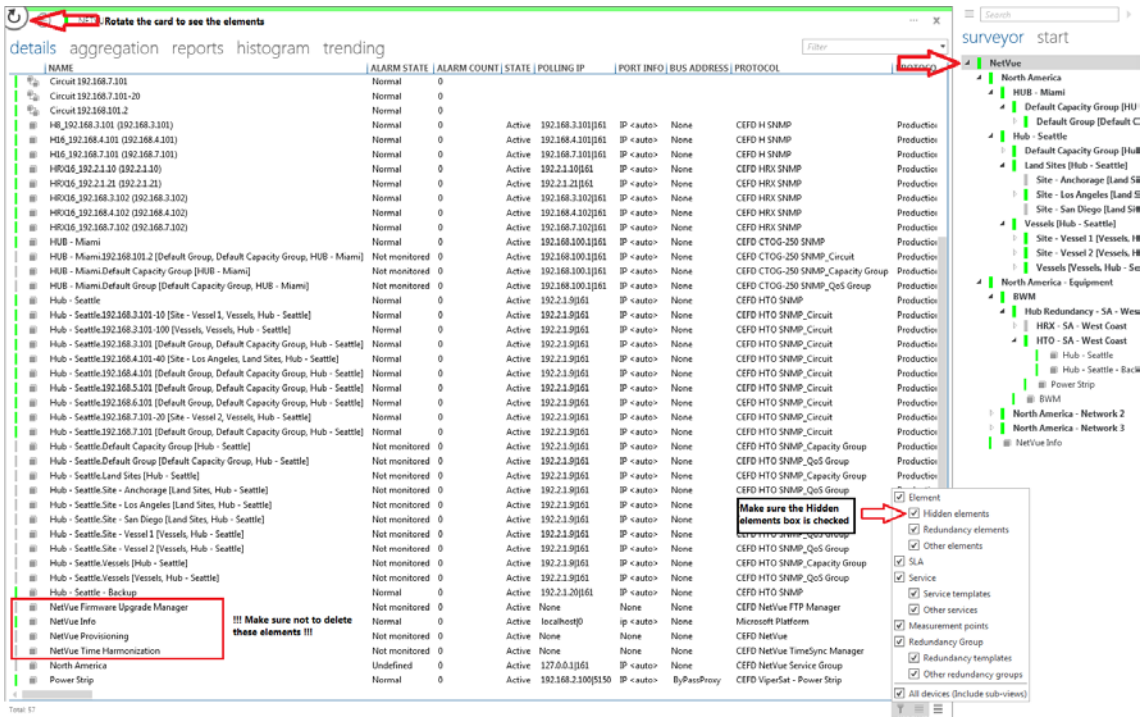


Figure 4-5. Remove All Elements

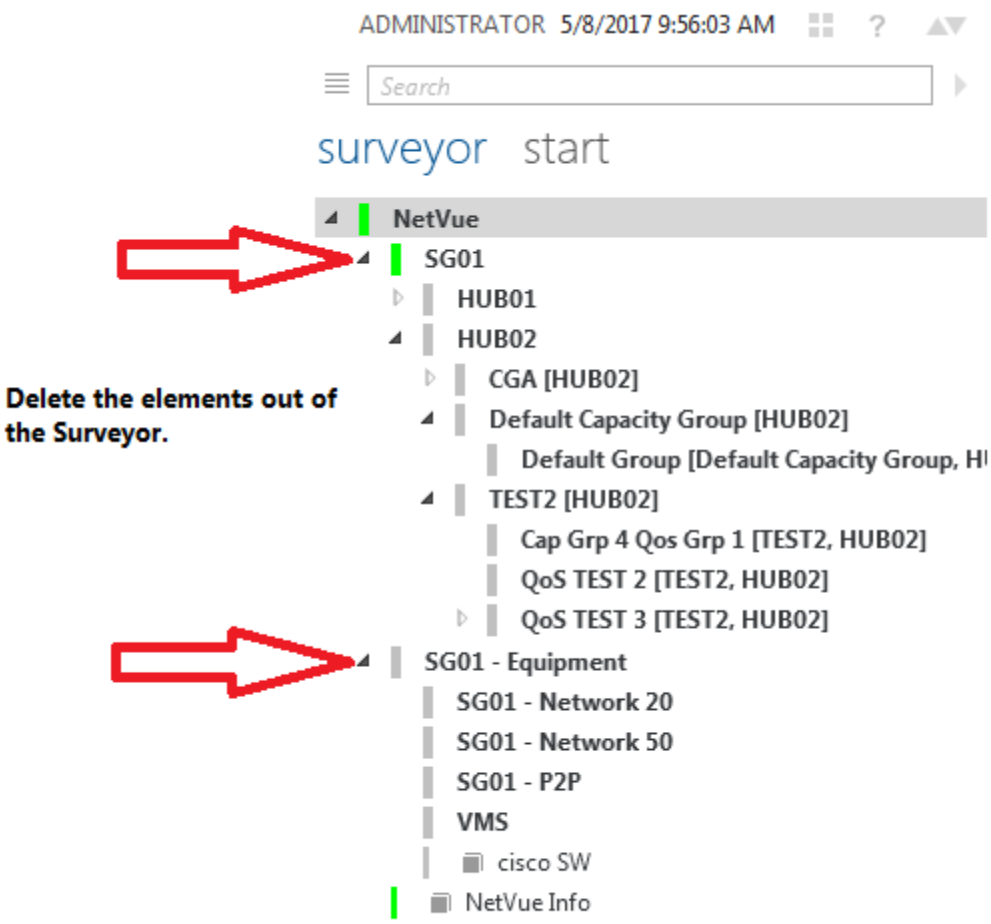


Figure 4-6. Delete Elements from Surveyor

Once all of the elements have been removed, close the card and clear the database configuration tables by going to the NetVue Provisioning App and clicking on the “Clear All Tables” button.

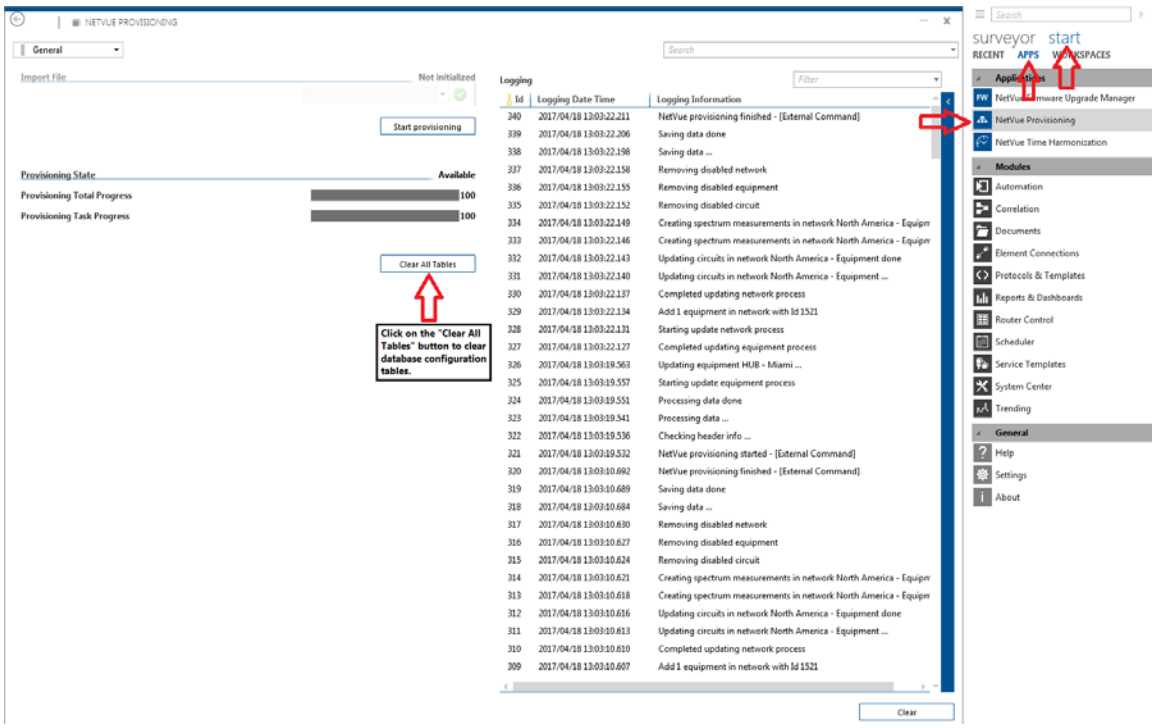


Figure 4-7. Remove Configuration from Database

Restart NetVue and follow the steps in section 1.1 to re-import the bandwidth manager's configuration. If the QoS configuration was properly setup to use pairing IDs, NetVue will also auto-learn the QoS configuration during the re-importing of the bandwidth managers configuration.

4.5.2 Redundancy (VMS)

VMS redundancy increases the system availability in a network by protecting the network from a VMS server failure. Redundancy is a monitored, hot-standby configuration with 1+1 VMS servers running in parallel.

4.5.2.1 Redundancy Mode

The redundancy mode provides the status of VMS redundancy configuration. If redundancy is not enabled, the status is standalone, or else redundant.

Hardware configurations can vary between separate servers, NetVue and VMS, or combined (DUO), which both services are running on a single server unit.

In either case, each VMS server can switch between two mutually exclusive modes of active or standby. The active/standby hierarchy is specified through the assignment of a priority level attribute. If the active server fails, the backup server with the highest priority is hot-switched to assume control of the satellite network, replacing the failed server.

In a redundant configuration, the VMS servers run in parallel. The VMS database on the standby server is maintained in real-time, as a mirror image of the VMS database running on the active server.

It is recommended that all servers be co-located at the same site and be connected to the same Ethernet LAN segment.

4.5.2.2 Redundancy Local

If the active server fails, the VMS that is protected by 1:1 redundancy switches to a standby server immediately. The VMS running on the standby server picks up and executes the ongoing network management tasks until the failure in the active VMS server is resolved by human intervention.

Both the active and standby servers operate in a query-peer mode to control which server is to be the active VMS server in the network.

For example, if the active VMS server fails, causing a protection switch, a standby VMS server assumes control of the network. While the standby server is actively managing the live network, a previously active server that is restarting cannot assume the active server role without first checking for the presence of an active VMS server already managing the network.

The process for starting and managing the transitions between active to standby modes occurs whenever:

An automatic switchover is caused by the failure detection mechanism activated by active VMS failure, or

A manual switchover is started from the active console by shutting down the active server, for maintenance, for example.

A switchover from the active server to the server with higher priority (once recovered) is not automatic. An operator must cause the switch manually at the active server's console.

When a server with a higher priority is restarted, the VMS on the server detects an active peer on the network (a previous standby server), and enters standby mode automatically. It remains in standby mode until an operator switches the server back to active mode manually, or a failure occurs that causes an automatic switchover.

4.5.2.3 Active Server Role

The active VMS server has specific privileges that differ from a standby server:

- Only one (1) VMS server can manage the network actively.
- The active server is considered the default VMS server for configuration and network topology purposes.
- The active server's database is considered the master copy. The standby server(s) receives a copy of the master database from the active server as a part of its start-up process and automatic synchronization.
- The first VMS server to come on-line assumes the active mode, if all redundant servers are online and no other server is operating in active mode.
- The active server is the only unit that may initiate a manual protection switchover (a transition from active-to-standby mode or standby-to-active mode). This is a two-step event controlled by the operator/administrator: the active server is deactivated first, and then a standby server is activated.

4.5.2.4 Standby Server Role

A VMS standby server has specific functions that differ from the active VMS server:

- Upon startup, a standby VMS enters a query-peer mode, where it attempts to discover a peer VMS in active mode. The VMS enters a standby mode when an active VMS is discovered.
- A standby VMS server's default mode is standby. It can enter active mode only as the result of a protection switch, either automatic or manual.

4.5.2.5 Redundancy Auto Activate

An Auto Activate function is available to resolve any activation conflicts if all servers go offline temporarily. After the servers return to online status, the server that was the last active will reactivate automatically and assume the active role.

4.5.2.6 Server Synchronization

Server synchronization is always executed by/from the active VMS server, and is done to make sure that all standby servers receive any necessary updates because of changes in the master database that resides in the active server. Two types of server synchronization occur with a redundant VMS configuration, automatic and manual.

4.5.2.7 Automatic Synchronization

Automatic synchronization occurs automatically by the active VMS. It occurs whenever any changes that are associated with automatic system functions happen, such as automatic switching, device redundancy, etc. The active server maintains a memory cache that holds the updates until they can be pushed out to the standby servers by an automatic synchronization occurring during the VMS heartbeat. The updates are tagged onto the heartbeat message that is sent by the active server to the standby servers.

4.5.2.8 Manual Synchronization

Manual synchronization, also called full synchronization, must be done by administrator/user command for any changes not related to automatic VMS functions, such as whenever any database configuration changes are made to the server. If a standby server is restarted, when it rejoins the redundancy group, the sequence of updates can be lost and a manual synchronization is required to make sure that the standby receives the most current database from the active server.

This operation can be automated on a 24-hour basis with the Auto Synchronize.

During a full synchronization, the active VMS service is taken down temporarily, to avoid any changes occurring during the synchronization process. The active server sends the contents of the temp file holding the entire database backup to each standby server via simultaneous unicasts. If there is any failure with this update process, a notification is saved in the windows log.

Server contention is a built-in protection mechanism for redundant VMS operation. A situation can occur where the active server loses network connectivity briefly, before communications are restored. The first priority standby becomes active because of the lost heartbeat of the former active server. When the former active server returns, it detects that another active server is operating, and enters the contention state.

When the active server senses this, it enters the contention state also. In such a situation, there is no way for the system to know which server has the most current up-to-date database, and both servers will de-activate immediately to protect the status of the network. A generated alarm, both visually and audibly activated, occurs on each server. In addition, an SNMP trap is generated.

In this condition, VMS services are still running, but no changes of state can happen in the network until the condition is cleared.

4.5.2.9 Redundancy Local Status

The VMS Redundancy Status shows the local server state. The screen in Chapter 5, Figure 5-9 VMS Manager, Redundancy Local, shows the current state.

There are four possible server states:

- Active
- Standby
- Contention
- Disconnected

4.5.3 Equipment Inventory Lists

The Vipersat Manager builds lists of groups that are created autonomously as each unit reports in for the first time. After Vipersat Manager is configured and the server is activated, communications between the VMS and live network units at Hub and Remote sites are established, and the auto-discovery process begins. This important process allows NetVue to choose devices that were previously discovered, automatically identified, and added to the VMS database.

When a new unit is added to the network and IP communications are established to the hub LAN, the VMS will start receiving autonomous registration messages. These messages provide particular indentifying information about the device, allowing it to be categorized and assigned to a resource sharing group list initially.

The Resource Sharing Group ID number (1 – 255) is set and managed by the outbound hub traffic optimizer. Any remote gateway or receiving hub unit that is assigned to this outbound are synchronized to this number, identifying a physical Service Area at hardware level.

4.5.4 Service Area

The Service Area is a hierarchy comprised of many different levels within the system architecture. The example hierarchy in Figure 4-8 shows the framework and where each element resides.

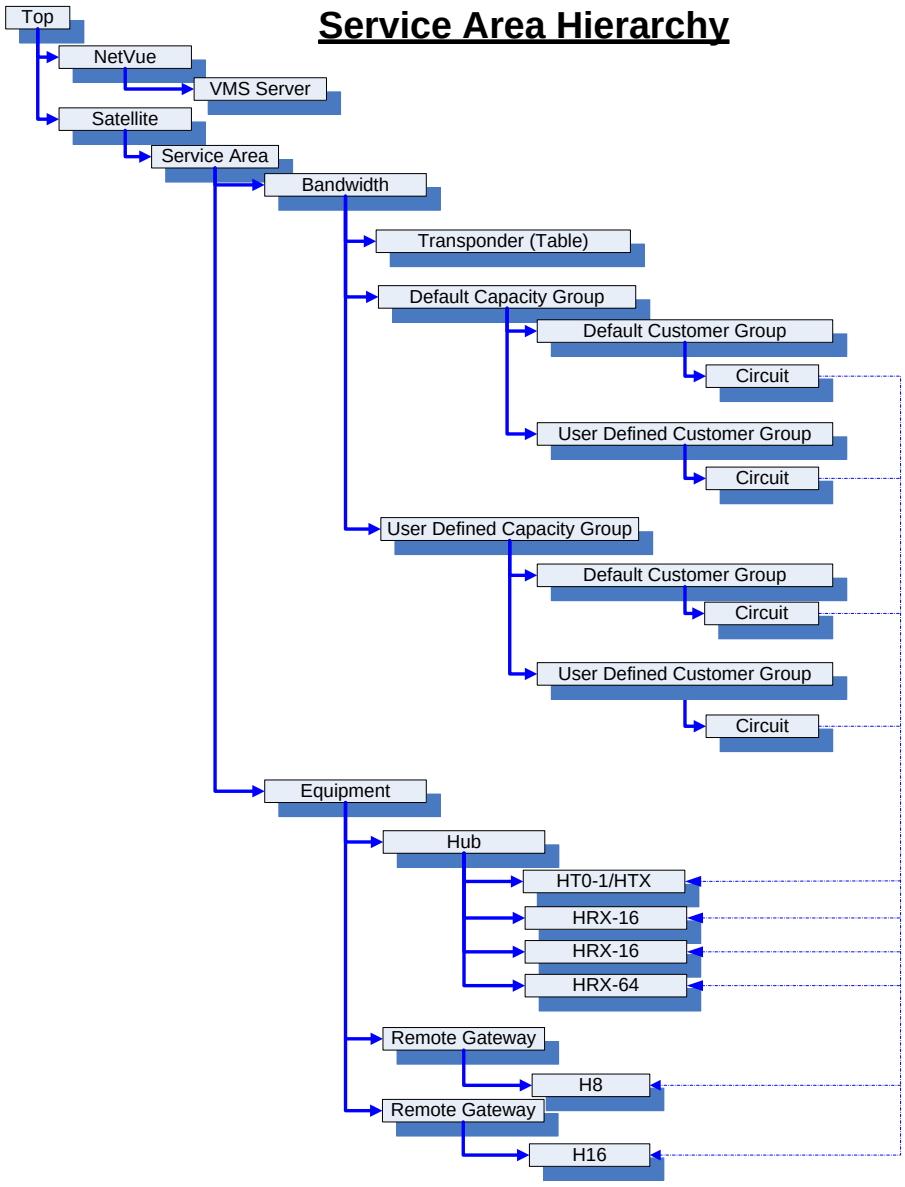


Figure 4-8. Service Area Hierarchy

At this level in NetVue, the service area is a container that stores specific and unique information that defines the communication structure. Each block represents a set of configurable components in the hierarchy, which classifies the flow for provisioning.

Each block has list of parameters that build the bindings linking each of the devices through configuration policy settings.

4.5.5 Sites

The equipment within the system architecture has two different roles, hub or remote. The hub site units are the foundation and the central point for all remotes within the service area group. The key element in the service area is the outbound hub traffic optimizer. The outbound is the focal point in which all traffic and management information is disseminated. Many of the network identification parameters are broadcast using a special WAN Universal Announcement message to all listening remotes updating Resource Sharing Group ID, VMS management multicast address and routing information.

As part of the configuration management, the hub site is first to be constructed after defining the satellite frequency domain, satellite characteristics, transponder(s) and dynamic bandwidth pools.

4.6 Switch Operations

To understand the dynamic switching processes, it is important to review the different states required to process a request for capacity changes. The Bandwidth Manager (engine) is a core component of the switching subsystem in the VMS, responsible for accepting data-rate change requests from remotes, finding resource availability and coordinating the reconfiguration of devices to fulfill those requests.

The engine interacts with its environment through a set of stateless interfaces. This allows the engine to work with different types of carriers and hardware devices without specific knowledge of those components.

4.6.1 Components

The engine depends on other components of the system in order to fulfill its role. It depends on device drivers to provide information about limits to perform operations based on device specifications (i.e. calculating bandwidth or power required given a set of transmission parameters). It depends on the bandwidth manager (RF manager) to perform frequency calculations and track device visibility. It also depends on switching state objects to interface with external clients, and translate results of solutions into switch type specific command structures for the modem drivers to use for sending commands to the actual hardware.

4.6.2 Allocation Space

The allocation space is the component that manages the switching functionality for a particular satellite. It maintains the satellites available resources. It tracks allocations and pre-allocations. It hosts all the queuing functionality and it is the entry point for switch requests to be processed by the engine. Each allocation space executes operations in parallel (assuming available processing resources).

4.6.3 Queuing Structure

The queuing structure refers to the mechanisms necessary to prevent incoming requests from conflicting with each other. In addition to preventing conflicts, it will group and/or skip requests to improve performance in active networks. Request sets combine to form problems that are fed to the solver to generate solutions, which are then implemented (sent to hardware). The queuing structure is multiple layers that track different aspects of the pending requests.

4.6.4 Allocation Process

The allocation process operates in three broad phases. The first phase checks whether the request must be pursued. The second phase consists of a series of passes over the problem, attempting to place the requests in a manner that minimizes impact on existing carriers. In the final phase, the system falls back to a known solution that provides, at minimum, the configured guaranteed data-rate (CIR).

Allocation always attempts to affect the carriers in the bandwidth pools minimally. It does this by using a Minimal Impact Solver. The goal of the minimal impact solver is to produce a solution that has the least impact on the system. Generally, minimal impact means fewest additional carriers involved, through a carriers priority, and the amount that it is over its guaranteed rate is a factor.

During evaluation, the rule for reducing a carrier's bandwidth involves priorities and the guaranteed-rate for the involved sites. Given two carriers, the carrier with the highest priority will reduce the lower priority carrier as far as needed for the higher priority carrier to fulfill its needs to the extent that the lower priority is using bandwidth above its guaranteed rate. Therefore, if a higher priority carrier requires the lower priority carrier to be reduced below its guaranteed rate to fulfill its request, the higher priority carrier's request rate will be reduced enough to allow the lower priority carrier to maintain its guaranteed rate.

4.6.5 Communication Failure

If communication failures occur (e.g., environment, interference and hardware breakdown) within the network, the rate guarantee cannot be maintained. When the system detects failures it enters into a state of recovery that attempts to return faulting remotes to a known state removing possible contention within the resource pool or a better term physical carrier level. During this recovery mode, normal switching is allowed to continue. Resources occupied by faulting remotes are unavailable, and, potentially, rate guarantees are not honored. Once all faulting remotes are recovered or identified through failure state analysis, the rate guarantees are once again honored. The bandwidth from this point is once again available for continued allocations.

4.7 Dynamic Bandwidth Management

Dynamic switching provides autonomous operation of network demands, based on either site traffic loads or applications requiring immediate change in return transmission bandwidth.

These automatic switching types are presented in each of the unit manuals, AdVSAT and Heights, which provide more detail on the configuration and mechanics of operation. However, for simplicity, this section will cover a system level exchange between remote gateways and bandwidth manager with reference to each type.

The basic signal topology in the bandwidth-managed network is a fixed outbound and proprietary return path.

When required, a network is switched from shared entry channel to dynamic SCPC. The dSCPC bandwidth is allocated from a bandwidth pool by the VMS to meet QoS or other requirements for the duration of a connection. When the dSCPC connection is no longer required, the bandwidth returns to the pool for use by another client through carrier reduction or by removal.

This basic structure gives the VMS controlled network its flexible, automated network usage and optimization capability.

The VMS has the intelligence to interpret the constantly changing statistics gathered by the remote gateways and use this data to issue commands back, effectively managing the network operation in real time, and optimizing each site's bandwidth usage to meet their QoS and cost requirements within their bandwidth allocation or SLA. The result is a stable satellite network connection that responds to the customer's requirements automatically, while monitoring and reacting to changing load, data type, and QoS requirements continuously.

VMS is the engine that provides dynamic bandwidth management of space segment. When a remote gateway in the network has an application to transport over the satellite link, dynamic technology provides the mechanism to establish the SCPC carrier for that transmission automatically. The dSCPC resizes the carrier based on the increase or decrease in data being sent over the link. Finally, dSCPC technology returns the remote gateway to its minimum transmission state once the application or load condition has subsided. The dSCPC yields true bandwidth-on-demand providing low latency, low jitter, lossless dedicated SCPC connection needed for real-time applications.

4.7.1 Entry Channel Switching

Entry Channel Mode switching allows the remote gateways to switch into dSCPC immediately after completing boot and registration into the network.

Once the remote indicates that registration with VMS is complete, the hub entry channel controller on behalf of the remote terminal will request dSCPC assignment by placing the address of the remote into the list: "switch pending", and sending an ECM type switch request message to the VMS. Upon receipt, VMS will grant the request and signal the hub controller to remove the remote from its list, or ignore the request, leaving the remote in switch pending list. The hub controller will repeat the request every 12 seconds up to 5 times, and then remove the remote from the pending list. While the remote is in this "pending" state, it continues to send Status Update Messages (SUM) to the VMS indicating its health. Because all ECM transmissions from the remote contain a Remote ID, this will cause the remote to be put back in the pending list. This cycle continues until the remote is either switched, set to wait state or goes offline.

The VMS is the last step in the entry process providing network registration and granting dSCPC resources or not, and if resources are limited because of bandwidth, hardware or completely unavailable, remotes will remain in the entry channel awaiting next assignment.

The VMS has no role in ECM timing or control.

4.7.2 Load Switching

Load Switching is a mechanism in the remote gateway by which the bandwidth manager receives remote terminal's capacity change based on traffic QoS levels measured at the remote.

Load switch configuration changes are set in the Remote Gateway.

There are two components of load switching, bandwidth manager and the remote gateway. The bandwidth manager component receives switch requests from the remote. Based on policy settings and available resources, it grants or denies the request. The remote requests can increase or decrease bandwidth based on the amount of data in its queues.

The basic concept for all load switching is that a running average of current usage is maintained, and when that usage exceeds a preset threshold, a switch is initiated. The data rate for the switch is computed by finding the current bandwidth requirement of the remote and adding a small percentage of excess margin.

Load switching is accomplished by maintaining a running average of the data traffic passing over the WAN. The running average is maintained as a percentage of the current Data Rate. Whenever a switch in data rate occurs, that running average is cleared and must accumulate for at least the specified delay period before another switch can occur. After the specified delay period is reached, the system checks the current usage against the step up and step-down thresholds once per second, and if the usage is outside the desired range, the system requests a switch with the new calculated rate. After the request is granted, the running average is reset and accumulated for the specified period. At the end of the delay period, if the usage is still out of range, a switch is requested again, using the re-computed usage adjusted by the excess capacity.

We define both Step Up and Step Down threshold in terms of percent usage, a bandwidth margin value and a latency or averaging period. Once per second, the modem software finds the current percent usage by dividing the bits transmitted by the current transmit data rate. If the percent usage exceeds the step-up threshold, or is less than the step-down threshold for the entire latency period, then an Automatic Switch Request (ASR) is sent to the VMS. The bandwidth requirement for the ASR is computed by taking the average percent usage over the latency period and multiplying that by the current data rate to find the actual data rate used over the measured interval. This number is multiplied by the margin value and rounded up to the nearest 8K to calculate the requested bandwidth.

4.7.3 ToS Switching (Application)

The Type of Service (ToS) or Differentiated Services (DiffServ) field in the IP header is used to classify IP packets so that routers can make Quality of Service (QoS) decisions about which path the packets should travel across the network. This type of classification mechanism is configurable through the application interface typically, or the next hop service connection. When applying encryption to the applications, some IP Sec routers can provide packet classification or preservation. In either case, the ToS value is useful information to the bandwidth manager.

Applying a ToS value to an application such as VoIP, IPVC or priority data, through preservation or classification packet stamping, allows the bandwidth manager to even function in an encrypted network.

Because each packet is marked with the ToS value, it is not possible to miss setting up a switch. If the ToS stamping is done by a router, or by a gateway that allows for marking the signaling packets with a different ToS or DiffServ value, it is possible to configure the remote gateway to switch only on the RTP, thereby preventing a ring-no answer for voice calls.

ToS switch configuration changes are set in the Remote Gateway. Any classification of packets is managed by applications or front-end routers.

4.8 Manual Switching

Sometimes you want to set up dSCPC carriers manually. The system provides for two types of manual switching: Diagnostic, or Applications Sessions.

4.8.1 Diagnostic Switching

Diagnostic switching is used mostly for troubleshooting problems with other types of automatic switching. It has special rules. The VMS will not downsize or revert a diagnostic switch. Therefore, while diagnostic switches are in the allocation space, guaranteed bandwidth is disabled. Do not leave diagnostic switches up in the bandwidth pool for this reason.

To set up Diagnostic switches, select Setup under DIAGNOSTICS. A dialog box opens, in which you can select a bit rate for the switch, and select the MODCOD by clicking the dropdown under Modulation and Coding.

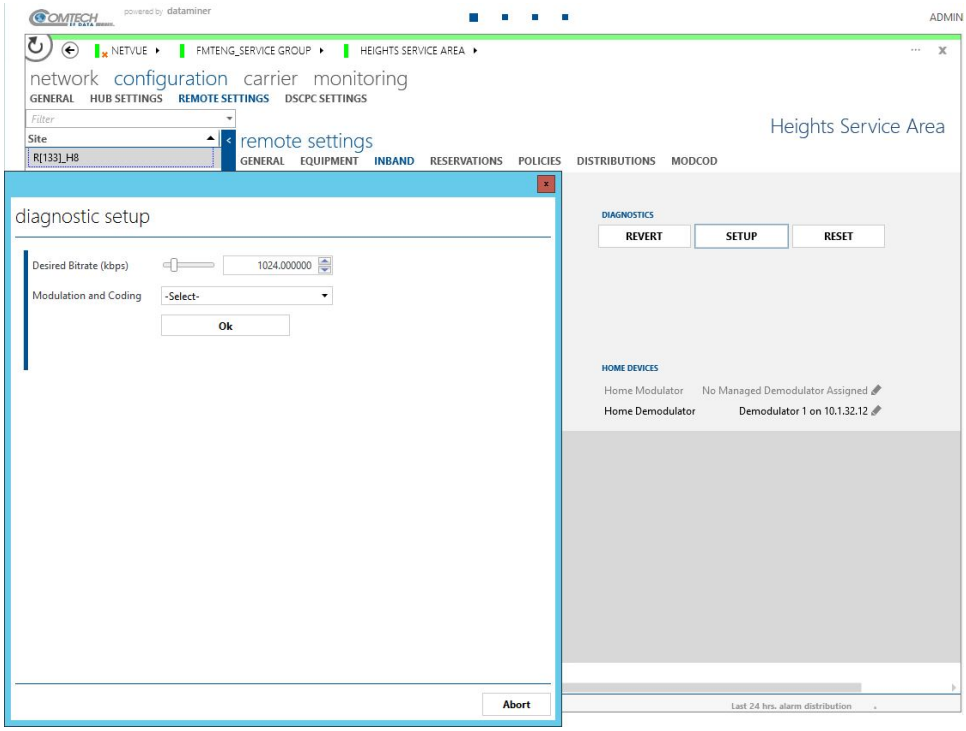


Figure 4-9. Diagnostic Switching

4.8.2 Revert

The Revert command returns the remote gateway to its home state settings. Use this command when SCPC transmission is no longer required, switching back to Entry Channel Mode, or when communications with the remote have been lost and it is unknown if the remote gateway is still transmitting. Unlike the Reset command, the bandwidth slot is retained in case the communications are restored.

4.8.3 Reset

As with the Revert command, the Reset command returns the remote gateway to its home state settings. However, use this command to prevent the occurrence of an interfering carrier when communications with the remote have been lost and it is known that the remote is not transmitting. The bandwidth slot and associated hardware (demodulator) are freed for use by another network device.

If the remote is still transmitting, an interfering carrier can be created. Thus, the selected Diagnostic Reset command shows the reset uplink warning.

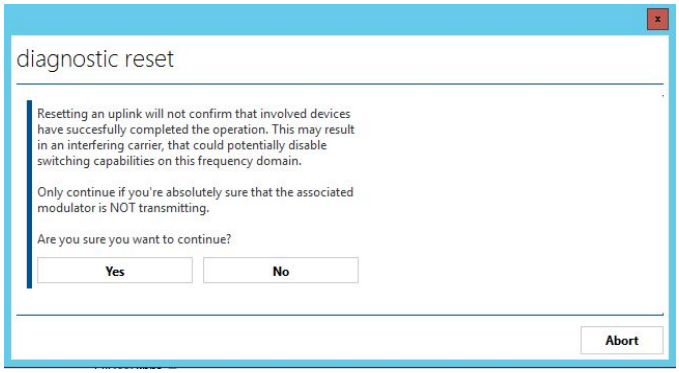


Figure 4-10. Reset Uplink Warning

4.8.4 Guaranteed Bandwidth & Reservations

Premium services offered by satellite service providers are far more attractive if Service Level Agreements (SLA) can be arranged to guarantee bandwidth. A common business model is to offer quality of service in the form of a Committed Information Rate (CIR). Customers are willing to pay a premium for service where their access and experience will meet or exceed their expectations. Low latency and low jitter connections are the hallmark of SCPC links. The drawbacks have always been the bandwidth wasted when the links are lightly loaded, or are offline, and the inability to offer Maximum Information Rates (MIR) that exceed the guarantee on a best-effort basis. This has been a feature of TDMA solutions, but they do not provide the quality or efficiencies of SCPC circuits.

The guaranteed bandwidth algorithm provides operators with a flexible solution for offering the highest quality communications links, which can be sized dynamically based on instantaneous usage.

Service providers can now announce a service that guarantees bandwidth on a site basis, but can fall to an Entry Rate (ER) if the site is lightly loaded. If the site is offline, it consumes no bandwidth, thus providing the remaining for other sites. However, as soon as there is a need, VMS will resize other carriers (with as little network disruption as possible) to make sure the site gets its guarantee.

In addition, system operators can provide their users with priority within the dynamic allocation of bandwidth. On a site-by-site basis, you can assure users that their most important links get the bandwidth they need as soon as they need it.

There are three levels of service:

- Entry Rate (ER) – A level of service always available to the customer, making sure they have the ability to enter a clear channel dSCPC circuit.
- Committed Information Rate (CIR) – Bandwidth guaranteed to be available instantaneously, based on the users' demand or contention.
- Maximum Information Rate (MIR) – Bandwidth that can be used by any site on best effort availability, and categorized through multilevel prioritization.

4.8.5 Guaranteed Bandwidth Description

With dSCPC, when a remote gateway detects a QoS load or ToS-stamped traffic, the remote gateway requests inbound (remote to hub) bandwidth from the VMS. The VMS then allocates inbound bandwidth for the site, and reconfigures modulator and demodulators to support the request.

Each remote site can be configured with a minimum entry rate, a guaranteed SCPC inbound data rate and a maximum SCPC inbound data rate. The minimum rate provides connectivity and service when the link is lightly loaded. When necessary, the VMS makes sure that a remote can receive at least its guaranteed rate (CIR), regardless of network usage. A remote's maximum rate is calculated on a site-by-site basis using the site's link budget, the remote configuration options purchased and the actual service offering.

The remote settings show site policies, see Figure 4-11. This is where the Minimum and Maximum bit rates and the site priority are set.

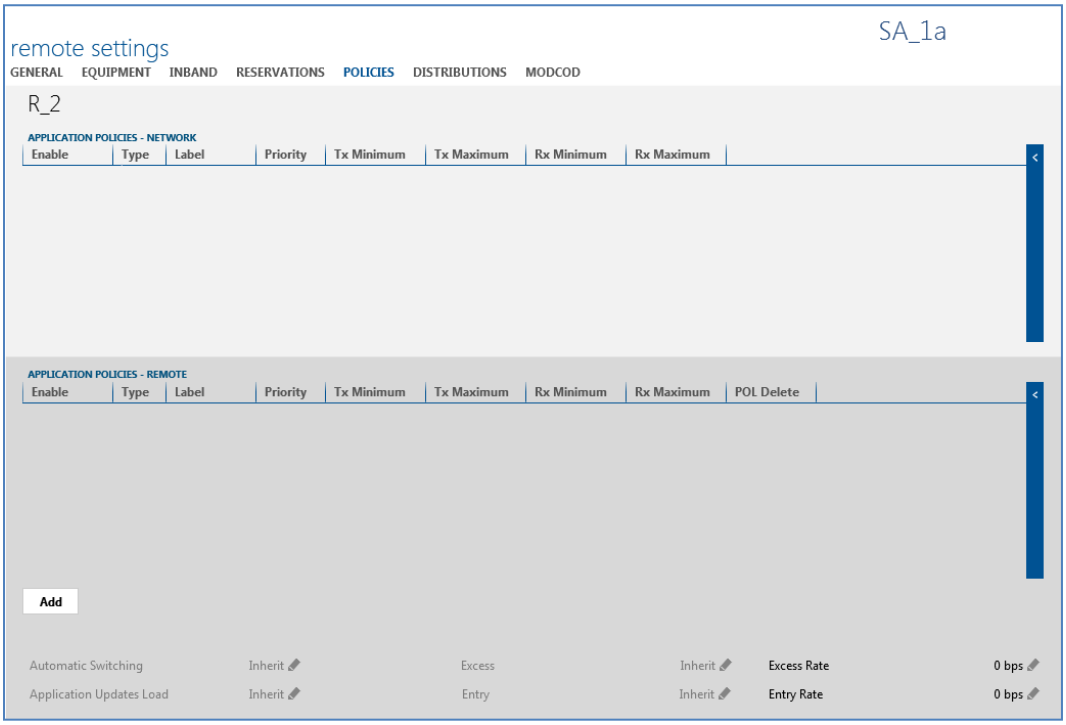


Figure 4-11. Site Policies

Figure 4-12 shows the bandwidth reservation page. All the satellites configured in the network are listed here, providing the assignment guarantees. You can select the current satellite, set the data rate for the reservation and select the Modulation, FEC Rate and FEC Type. An Active Status means the VMS is configured to provide the guaranteed rate. If the site is roaming and transitions to another satellite, the VMS will switch to the other satellite automatically, providing the next level of guarantee.

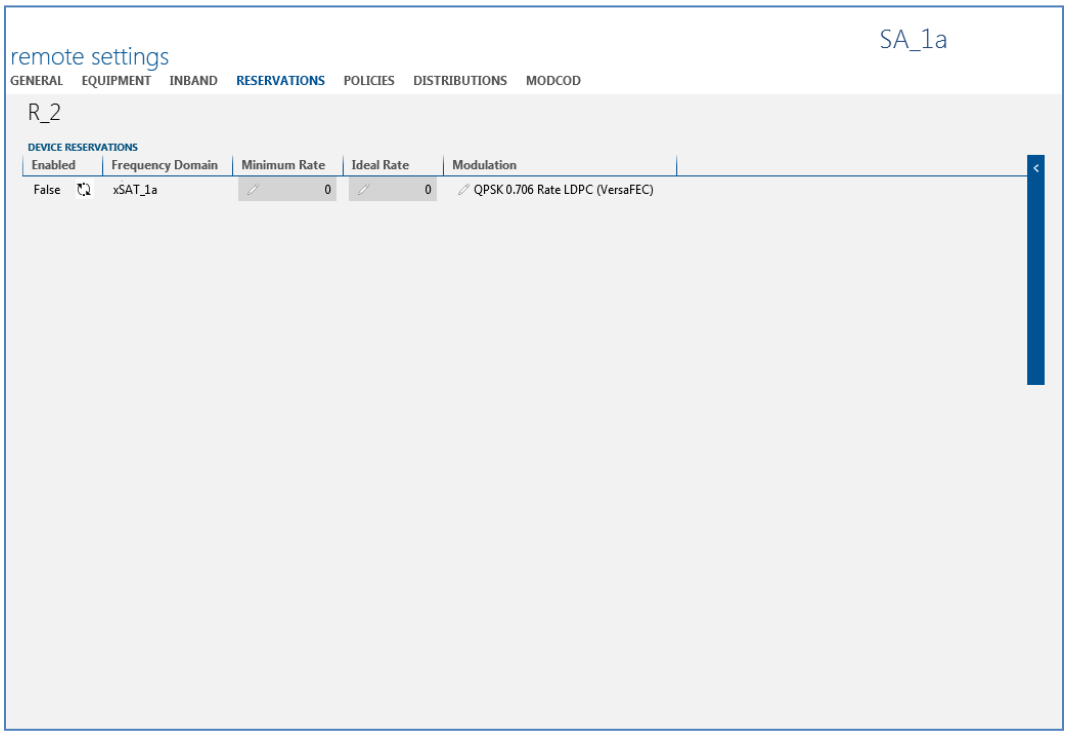


Figure 4-12. Reservations

The VMS allocates inbound bandwidth automatically for sites from one or more satellite capacity pools. When a site is using less than its guaranteed rate, the unused bandwidth is available for other sites.

In certain cases when providing a remote site with its guaranteed rate, the VMS can move other carriers in the satellite capacity pools, or resize carriers that are larger than their site's guaranteed rate.

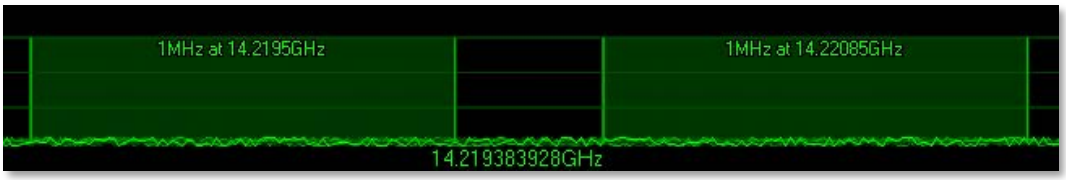
A key objective in the VMS guaranteed bandwidth algorithm is to minimize the movement and/or resizing of existing carriers in the satellite capacity pools when a remote site requests a data rate greater than or equal to its guaranteed rate.

4.8.6 dSCPC with Guaranteed Bandwidth Illustrated

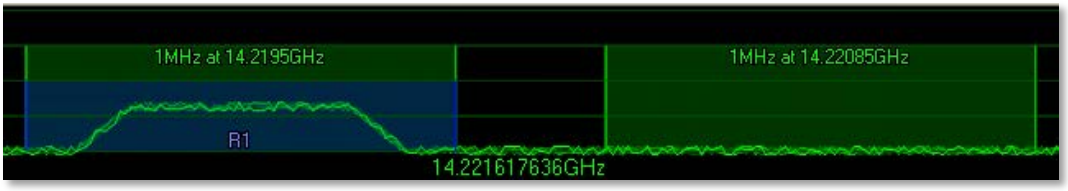
The scenarios show how the guaranteed bandwidth algorithm operates. The scenarios were selected for simplicity, but demonstrate the concept fully.

4.8.6.1 Scenario 1

1. Each site is assigned a CIR of 512 Kbps with a transmission waveform of QPSK ¾, using a 30% allocation factor equaling a bandwidth guarantee, per site, of 443.733 KHz.
2. R1 is configured with the highest priority over R2 - R4, which are equal in priority.
3. Each site is allocated SCPC bandwidth dynamically, occupying well above their guarantee.
4. There are two 1MHz bandwidth pools.

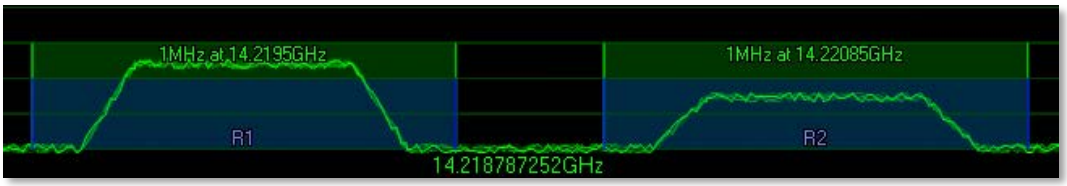


The first remote (R1) transmits requesting bandwidth that exceeds the size of either pool. Even though the request exceeds the site guarantee, the VMS gives it the maximum amount of bandwidth available, or equal to the site maximum (an example of moving toward MIR).



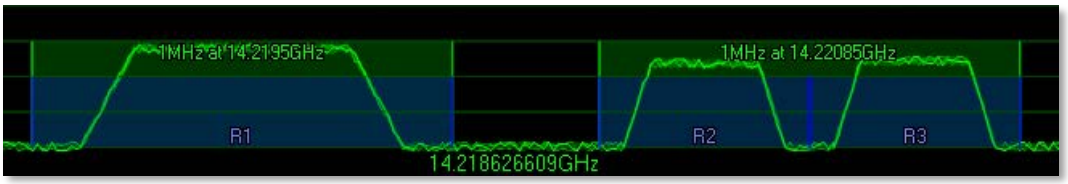
The image above shows that R1 switched to a carrier size of 1.15 Mbps, which fills the pool.

When R2 switches into SCPC, requesting bandwidth that also exceeds the total available in this scenario, the VMS assigns the same bandwidth as R1 as shown in this graph:

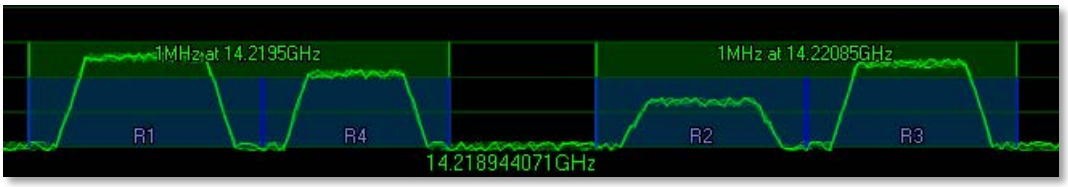


From the spectrum view, we can see that all the bandwidth in both pools is occupied equally by R1 and R2.

Thus, when R3 requests SCPC bandwidth, the VMS must make a decision as to which of the two carriers to downsize before allocating bandwidth to R3.



Through the reassignment as shown above, R2 and R3 split the bandwidth evenly in the second pool; this is because R1 has a higher priority. VMS deduced not to reduce R1's bandwidth, maintaining quality of service during increased capacity loading. However, when R4 requests bandwidth, we end up with the final solution, giving R4 its CIR as shown by the next graph.

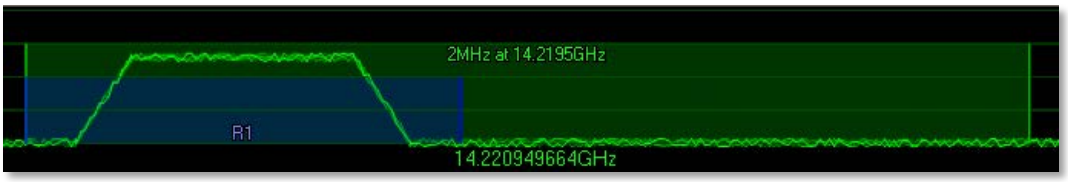


The VMS had to reduce R1 to provide R4 with its CIR guarantee. However, the bandwidth did not split evenly, as it did when R2 was reduced to accommodate R3. This is because R1 is still the dominating priority, whereby any excess bandwidth is provisioned over the R4 guarantee.

4.8.6.2 Scenario 2

1. Each site is assigned a CIR of 256 Kbps with a transmission waveform of QPSK ¾, using a 30% allocation factor equaling a bandwidth guarantee per site, of 221.866 KHz.
2. R1, R3 and R4 have equal priority. R2's priority is lower.
3. Each site is requesting a rate greater than their CIR of 1Mbps.
4. There is a single 2MHz pool.

R1 generates a request for a rate of 1Mbps of bandwidth. The VMS evaluates the request and sets up the SCPC transmission.

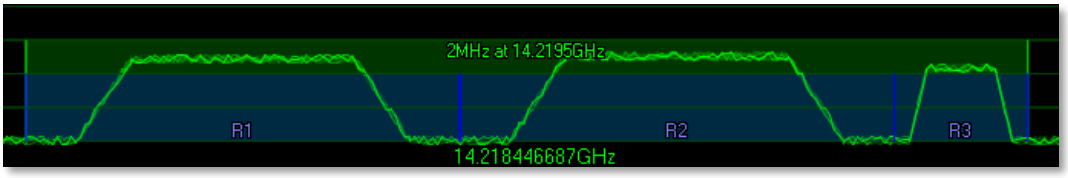


R2 then generates a request for rate of 1Mbps of bandwidth. There is enough space to grant the second request, so both sites are allocated bandwidth greater than their CIR. Note that the 1Mbps carriers occupy less than half of the 2MHz pool, because this is a factor of modulation and coding gain.

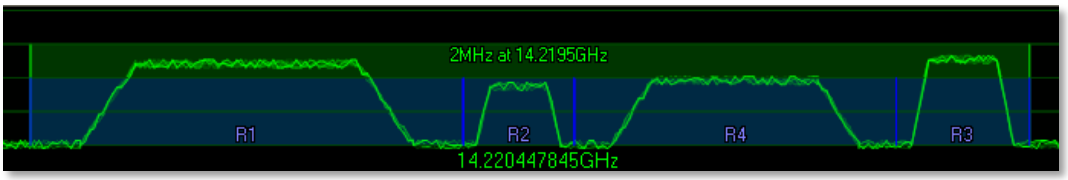
R3 then generates a request for a rate of 1Mbps of bandwidth. The VMS considers these factors:

1. The amount of contiguous bandwidth remaining in the pool
2. The guaranteed CIR rate configured for R3 (256 Kbps)
3. The maximum amount of bandwidth requested from R3 (1 Mbps)

There is enough contiguous bandwidth in the pool to support R3's guaranteed rate (256 Kbps), but insufficient amount to support the total requested. Because the VMS guaranteed bandwidth algorithm is designed to minimize the impact on existing carriers when providing a remote with its guaranteed rate, in this case, the VMS assigns as much bandwidth (greater than its guarantee) as available to R3 without affecting the existing R1 or R2 carriers.



R4 then generates a request for 1Mbps. There is no available capacity, so the algorithm must reduce one of the carriers in the pool. At this point, R2 is affected because it has lower priority, allowing all other sites to take precedence, resulting in carrier reduction.



Neither R1 nor R3 were touched, because they were of equal priority with R4. Because R2 had to be reduced, the VMS provided the site with its guarantee and gave the excess to R4, the higher priority carrier.

4.8.7 Bandwidth Capacity Considerations with Guaranteed Bandwidth

The VMS guaranteed bandwidth algorithm does not support the oversubscription of CIRs. Therefore, the minimum amount of bandwidth required is the aggregate of the bandwidth reservations. Excess bandwidth is available only if remotes were off line, or operating between their ER and CIR.

Carrier reductions, or movement, occur only when the VMS cannot fulfill a bandwidth request involving a site with a bandwidth reservation. To provide a premium experience to your customers, a minimum of 10% excess capacity over the aggregate of the bandwidth reservations is recommended.

Chapter 5. PROVISIONING

5.1 About Provisioning

Provisioning equipment and circuits is how NetVue creates the user network. Within NetVue, there are two ways that you can do provisioning:

1. Dynamic Carrier Operation: used when creating circuits with the CEFD Bandwidth Manager (dSCPC).
2. Static Carrier Operation: used when creating circuits in a point-to-point configuration.

5.2 Dynamic Provisioning

When provisioning equipment and circuits for use with the CEFD Bandwidth Manager, you must complete all Inband configurations at a minimum for correct dSCPC operations.

dSCPC provisioning assumes that the VMS, hub and remote apparatus are operational.

5.2.1 Add Service Group

1. Click the Root view in the navigation pane.
2. At the top of the card are two tabs: *home* and *configuration*. Click *configuration*.

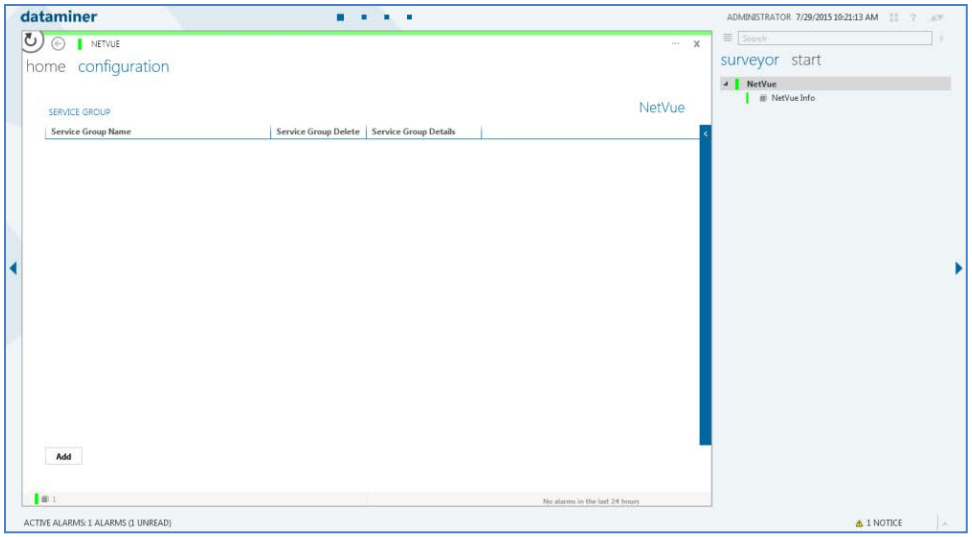


Figure 5-1. Service Group Configuration Page

3. Click the *Add* button at the bottom of the card.
4. Enter a *Name* for the Service Group.
5. Click *Add.*

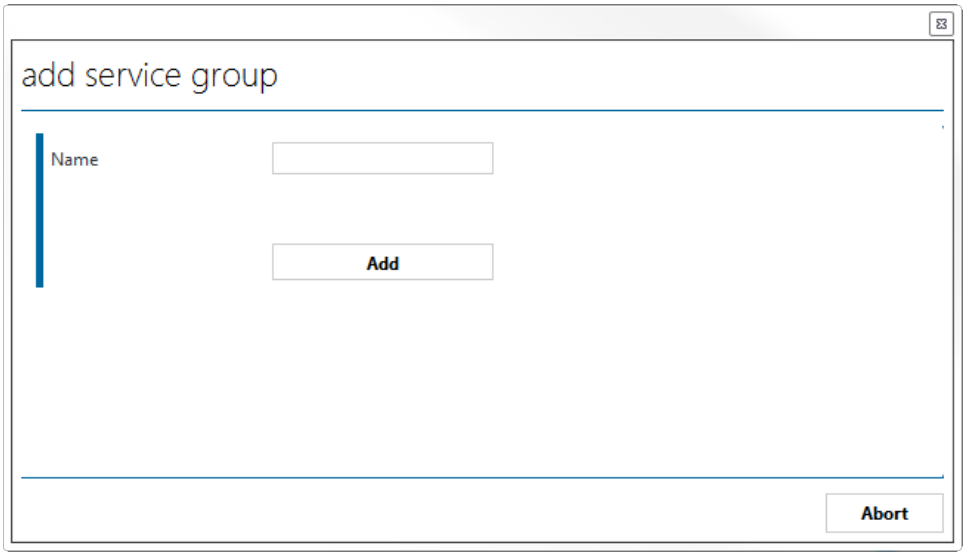


Figure 5-2. Add Service Group Page

The SERVICE GROUP view is added to the Navigation pane, along with the associated Service Group Equipment view.

6. Click the *Details* button for the newly added Service Group.

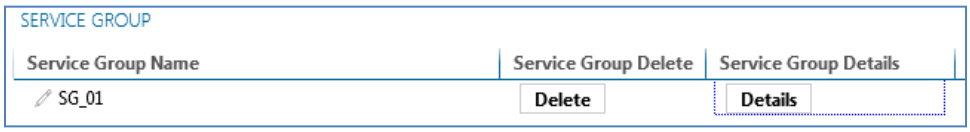


Figure 5-3. Service Group Details

This opens the SERVICE GROUP card, where you can make configurations for that Service Group.

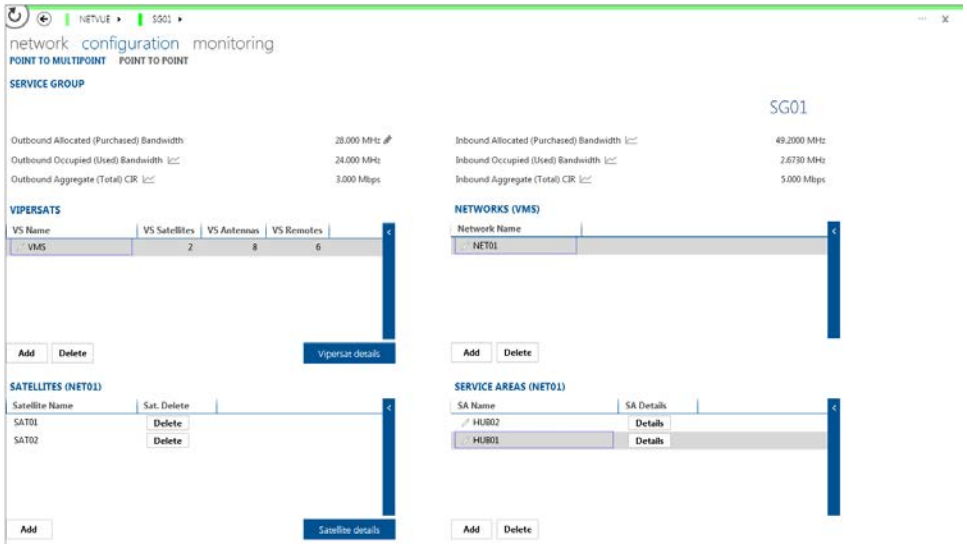


Figure 5-4. Service Group Card Page

5.2.2 Add Vipersat

From the SERVICE GROUP card:

1. Click the *Add* button under the *Vipersat* table.
2. Enter a *Name* for the CEFD Bandwidth Manager.
3. Enter the *IP Address* of the CEFD Bandwidth Manager.
4. Click *Add***.**

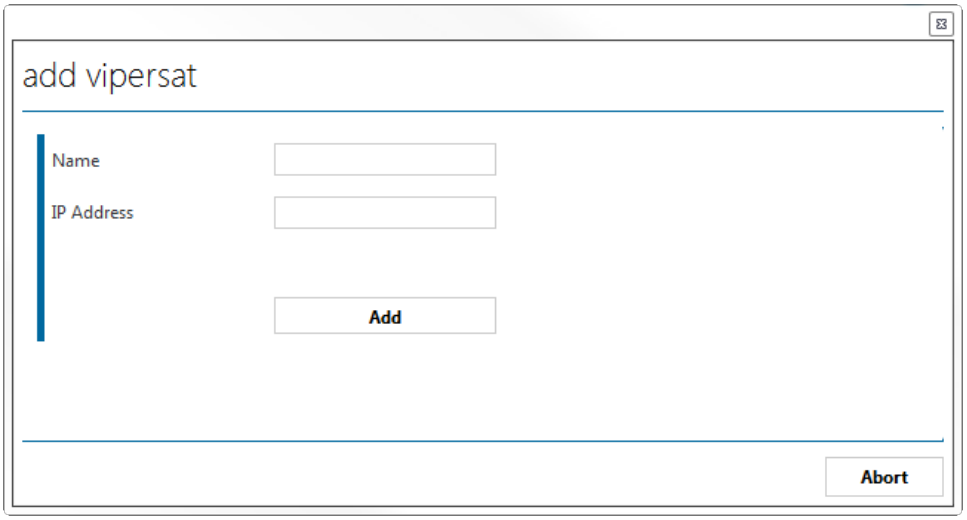


Figure 5-5. Add Vipersat Page

The Vipersat server is added to the Navigation pane. All equipment associated with the CEFD Bandwidth Manager will populate in NetVue automatically, under the Service Group Equipment view.

5.2.2.1 Vipersat Details

After the CEFD Bandwidth Manager has been created:

1. Left-click the desired server in the VIPERSAT table.
2. Click *Vipersat details* in the lower right corner of the VIPERSAT table.

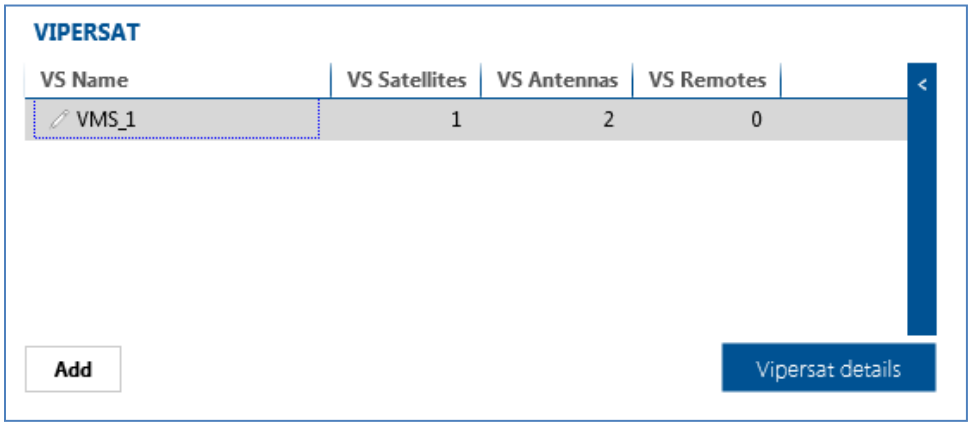


Figure 5-6. Vipersat Table Page

5.2.2.1.1 General Tab

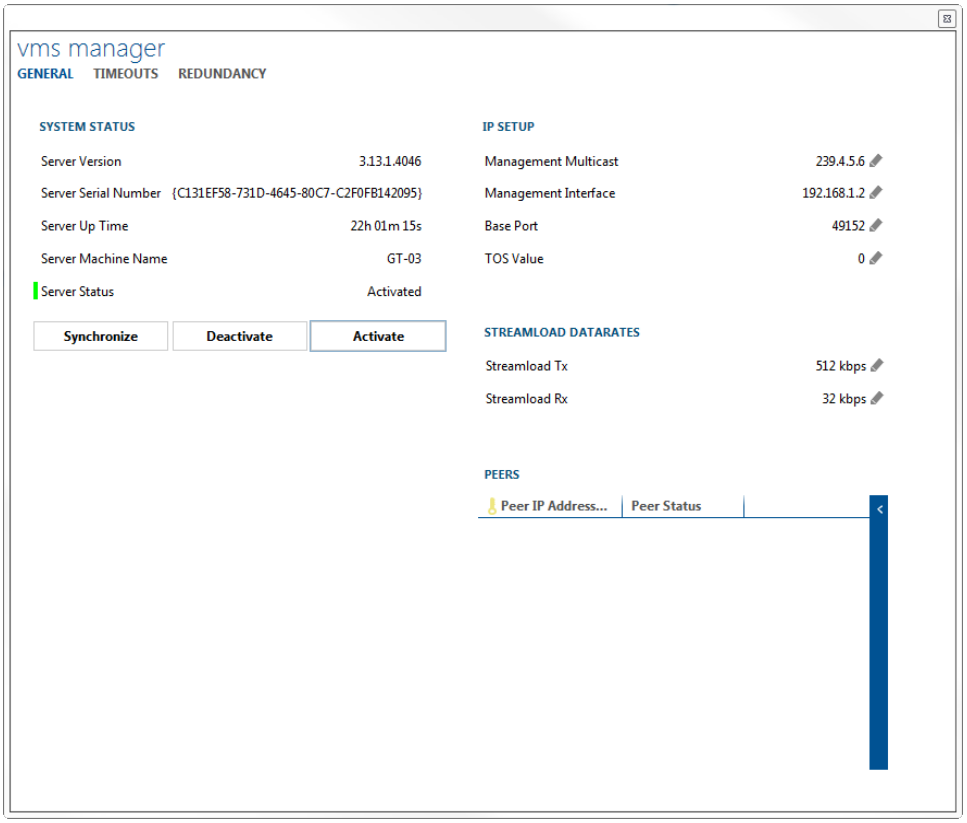


Figure 5-7. General Tab Page

The *GENERAL* tab shows the basic information and configuration for the CEFD Bandwidth Manager.

SYSTEM STATUS

- *Server Version*: The software version of the CEFD Bandwidth Manager
- *Server Serial Number*: The VKU serial number assigned to the server. To operate the CEFD Bandwidth Manager, this must be installed.
- *Server up Time*: How long the CEFD Bandwidth Manager has been running.
- *Server Machine Name*: The name assigned to the Windows server.
- *Server Status*: The status of the CEFD Bandwidth Manager (activated or deactivated).
    - *Synchronize*: Synchronizes the database when redundancy exists between two CEFD Bandwidth Managers.
    - *Deactivate*: Deactivates the CEFD Bandwidth Manager, resulting in no dynamic switching.
    - *Activate*: Activates the CEFD Bandwidth Manager, allowing the server to command and manage dynamic SCPC remotes.

IP SETUP

- *Management Multicast*: The multicast IP address that the CEFD Bandwidth Manager will use to communicate with all devices in the network. This multicast IP address must be identical to the Management Multicast entered in the CTOG-250/HTO-1.
- *Management Interface*: The management IP address for the CEFD Bandwidth Manager.
- *Base Port*: The starting base port for all UDP messages; by default, this is set to 49,152 and must NOT be changed unless directed by CEFD.
- *TOS Value*: Provides the ability to give the CEFD Bandwidth Manager a Type of Service value on the local LAN.

STREAMLOAD DATA RATES

- *Streamload Tx*: The transmission rate of configuration files sent by the CEFD Bandwidth Manager in kbps.
- *Streamload Rx*: The receive rate of configuration files received by the CEFD Bandwidth Manager in kbps.

PEERS

- This table shows adjacent CEFD Bandwidth Managers with their associated IP addresses and status.

5.2.2.1.2 Timeouts Tab

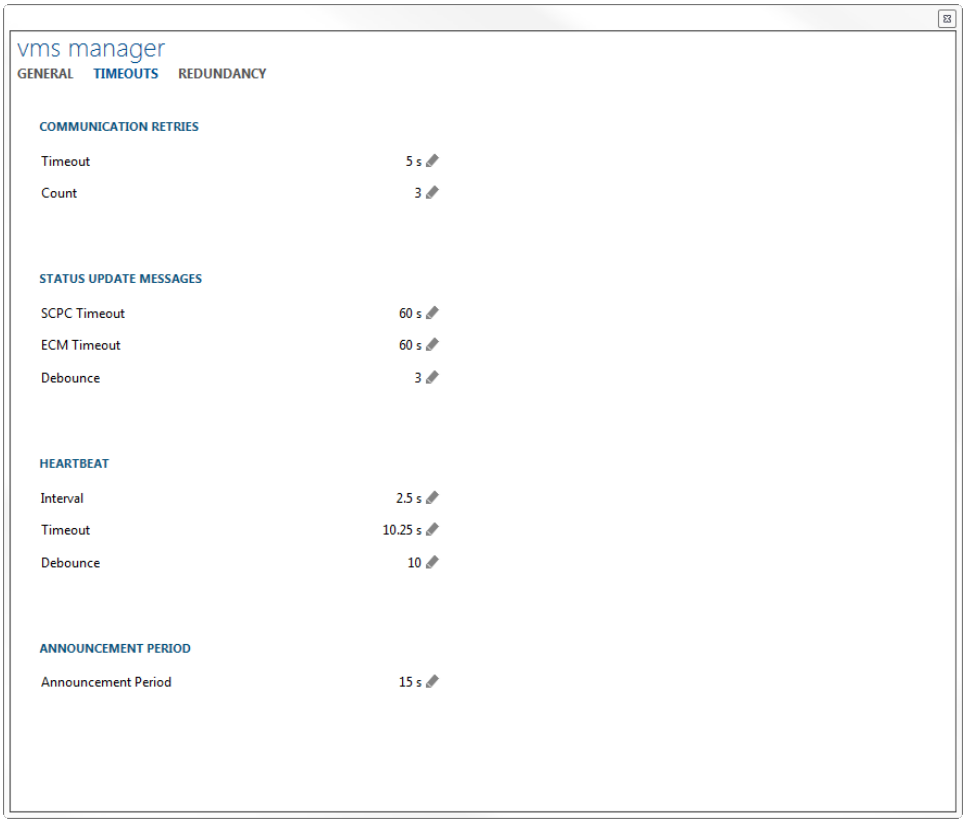


Figure 5-8. Timeouts Tab Page

The *TIMEOUTS* tab shows the parameters associated with how the CEFD Bandwidth Manager calculates loss of communication with a device in the network.

The recommendation is to keep all of these settings at their default values.

- *COMMUNICATION RETRIES*: The communications timer values set timeouts for command messages.
    - The *Timeout* is the wait between messages, which works with the *Count.* A retry count of 3 and a timeout of 5 seconds sets the message failure at a total timeout of 15 seconds, with 3 attempts to command the modem.
- *STATUS UPDATE MESSAGES*: These values set the dual timeouts and debounce for remotes that are in SCPC or ECM.
    - *SCPC Timeout*: The time interval between the sending of the Status update Messages to the CEFD Bandwidth Manager by remotes that are in SCPC mode.
    - *ECM Timeout*: The time interval between the sending of the Status update Messages to the CEFD Bandwidth Manager by remotes that are in Entry Channel Mode.
    - *Debounce*: A counter setting for the number of consecutive time intervals that can pass without the CEFD Bandwidth Manager receiving a Status update Message for a particular remote, before a switch failure occurs for that remote.

- *HEARTBEAT*: Provides timer settings for the hub device redundancy messaging.
    - *Interval*: updates the modem to send its heartbeat message to the CEFD Bandwidth Manager at the set rate.
    - *Timeout*: How long the CEFD Bandwidth Manager will wait before calculating communications failure and executing a device redundancy switchover.
    - *Debounce*: A counter setting for the number of consecutive alarm messages the CEFD Bandwidth Manager will receive from a particular hub device before a redundancy switch is activated.
- *ANNOUNCEMENT PERIOD*: The interval at which the CEFD Bandwidth Manager will multicast its management IP address to all listening devices within the network. For example, this makes sure that any remotes that are not online during a redundancy switch will pick up the new managing address when they come back online.

5.2.2.1.3 Redundancy Tab

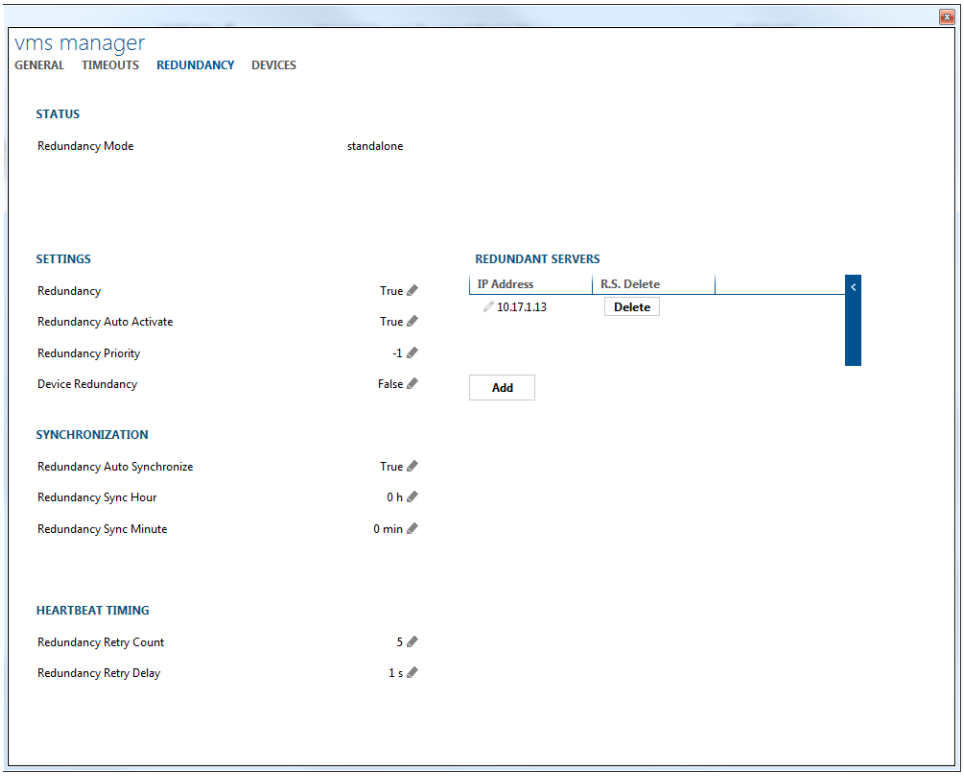


Figure 5-9. Redundancy Tab Page

The *REDUNDANCY* tab contains all of the parameters and information required to allow redundancy between CEFD Bandwidth Managers.

STATUS

- *Redundancy Mode*
- *Redundancy Local*

SETTINGS

- *Redundancy*: Select whether this CEFD Bandwidth Manager will be part of a redundant configuration (true or false).
- *Redundancy Auto Activate*
    - *True*: The server that was last active will reactivate automatically and resume the active role.
    - *False*: A server will be activated only by an operator issuing an activate command manually on one of the servers.

When enabling Auto Activate, make sure that this setting is exactly the same for each Comtech EF Data Bandwidth Manager in the redundancy group.

- *Redundancy Priority*: Set the priority level for the CEFD Bandwidth Manager for becoming active during a switch-over. The lower number is the higher priority.

SYNCHRONIZATION

- *Redundancy Auto Synchronize*: Select to enable or disable the periodic database synchronization operation for this server. It is recommended that this setting is enabled for each server that belongs to a redundancy group.
- *Redundancy Sync Hour*: The daily time, in hours, when the database synchronization must occur.
- *Redundancy Sync Minute*: The daily time, in minutes, when the database synchronization must occur.

HEARTBEAT TIMING

- *Redundancy Retry Count*: Represents how many heartbeats are missed before the device is considered to be offline.
- *Redundancy Retry Delay*: Represents how long the system waits before sending another heartbeat request.

REDUNDANT SERVERS

- Lists (by IP address) the other CEFD Bandwidth Managers that are in the redundancy group with the local server.

5.2.2.2 Devices Tab

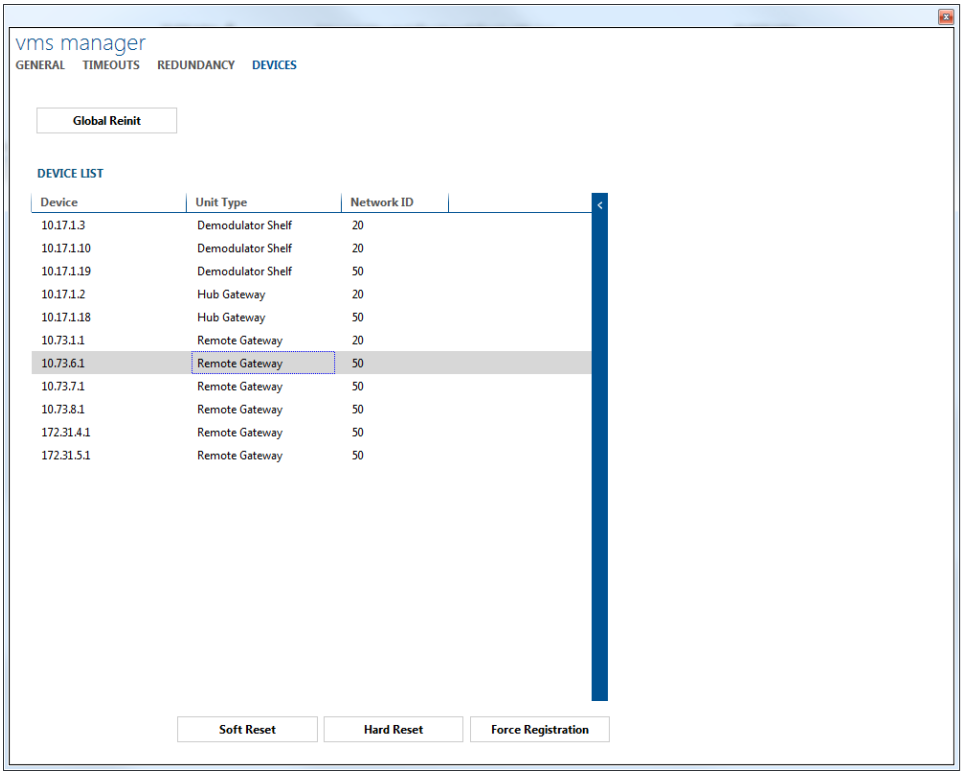


Figure 5-10. Devices Tab Page

NetVue provides the capability to perform global commands that are specific to the bandwidth manager and its interaction with the devices. The global commands are located in the **Bandwidth Manager->Details View** under the **Devices View**.

- Global Re-init – Forces the Bandwidth Manager to poll the network for device updates.
- Soft Reset – Causes the selected device to refresh all latched alarms.
- Hard Reset – Causes the device to reboot.
- Force Registration – Attempts to force the device to register with the Bandwidth Manager.

5.2.3 Add Network

On the SERVICE GROUP card:

1. Click the *Add* button below the *Networks* table.
2. Enter a name for the new *Network*.

5.2.4 Add Satellite

On the SERVICE GROUP card:

1. Under the *VIPERSAT* table, click the CEFD Bandwidth Manager.
2. In the *NETWORKS* table, click on the Network for which you are adding a satellite to.

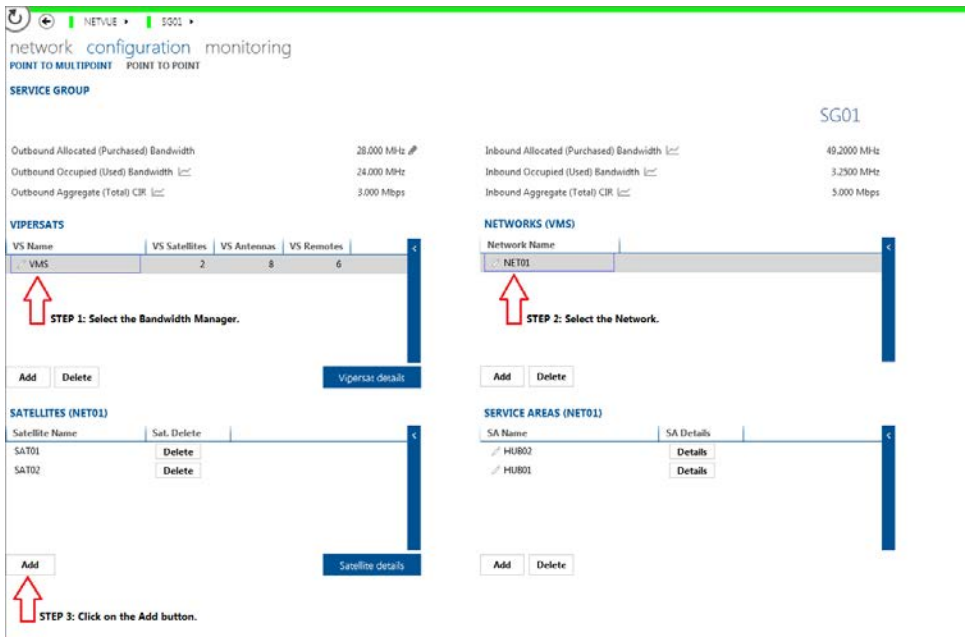


Figure 5-11. Adding a Satellite Page

3. Click the *Add* button under the *Satellite* table and fill in the following:

   Name: Enter the name of the satellite.
   Contact: Enter the contact information (phone number, email, …) for the satellite provider.
   Operator: Enter the name of the satellite provider.
   Center Frequency (GHz): Enter the center frequency of the satellite in GHz.
   Translation Frequency (GHz): Enter the translation frequency of the satellite in GHz.
   Orbital Position (deg): Enter the orbital position of the satellite in degrees.
   Orbital Direction: Select either *East* or *West*.
   Guard Band: Enter the guard band information.
   Switch All on Roam Away: Select *True* or *False.*

4. Click *Create.*

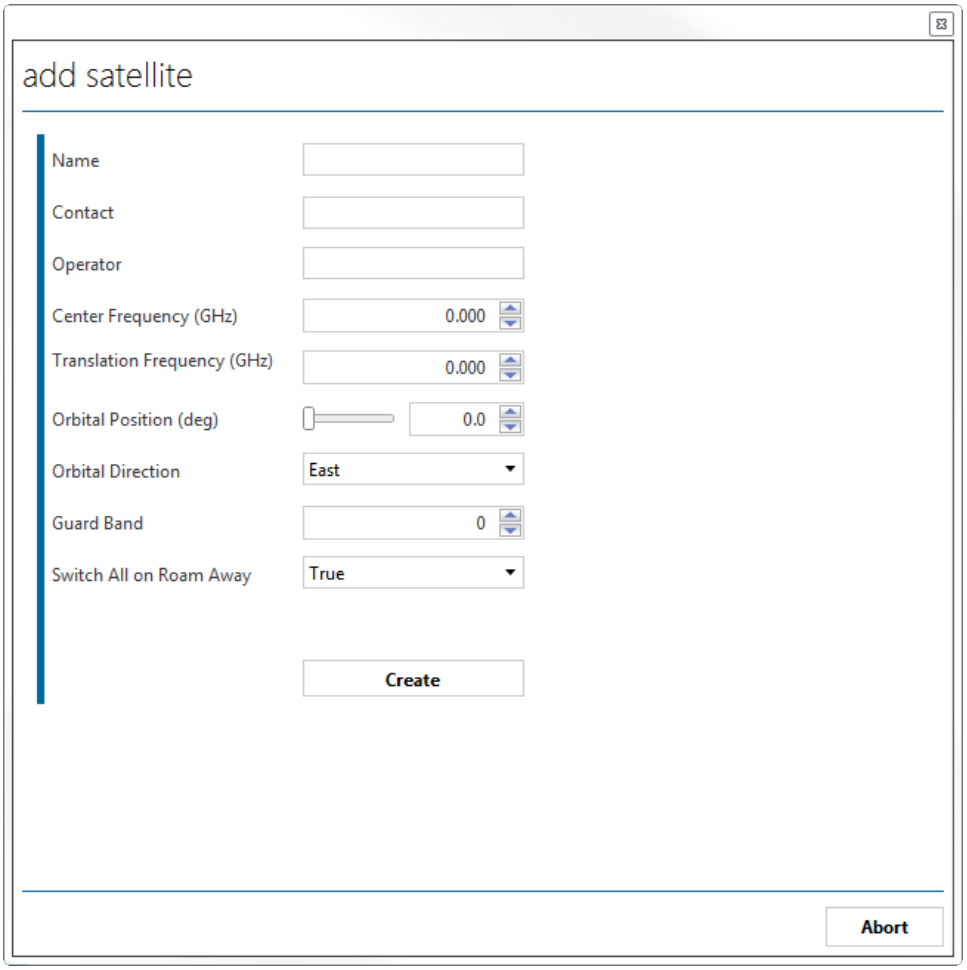


Figure 5-12 Add Satellite Page

The* Contact, Operator, Orbital Position *and* Orbital Direction *are all optional fields. You do not need set them to add the Satellite.

5.2.4.1 Configure Satellite Details

In the *SATELLITES* table:

1. Left-click the name of the satellite to be configured.
2. In the lower right corner of the table, select *Satellite details*.

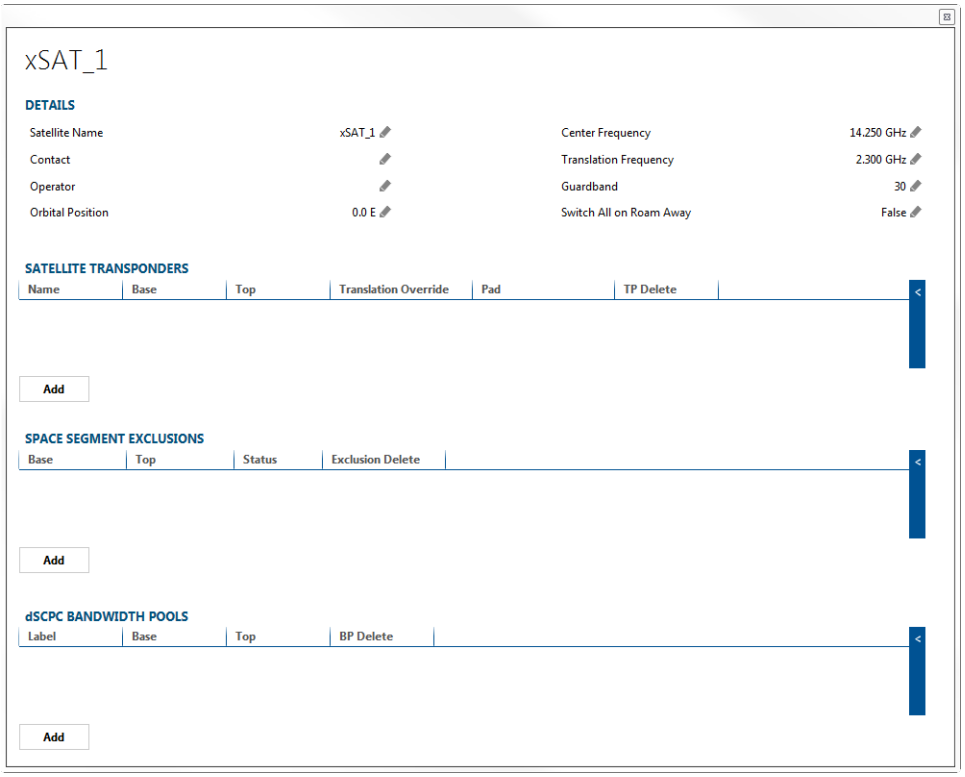


Figure 5-13. Satellite Details Page

DETAILS

Under the *Details* section, you can change any of the information for the selected satellite.

SATELLITE TRANSPONDERS

To add a transponder, click the *Add* button under the *SATELLITE TRANSPONDERS* table.

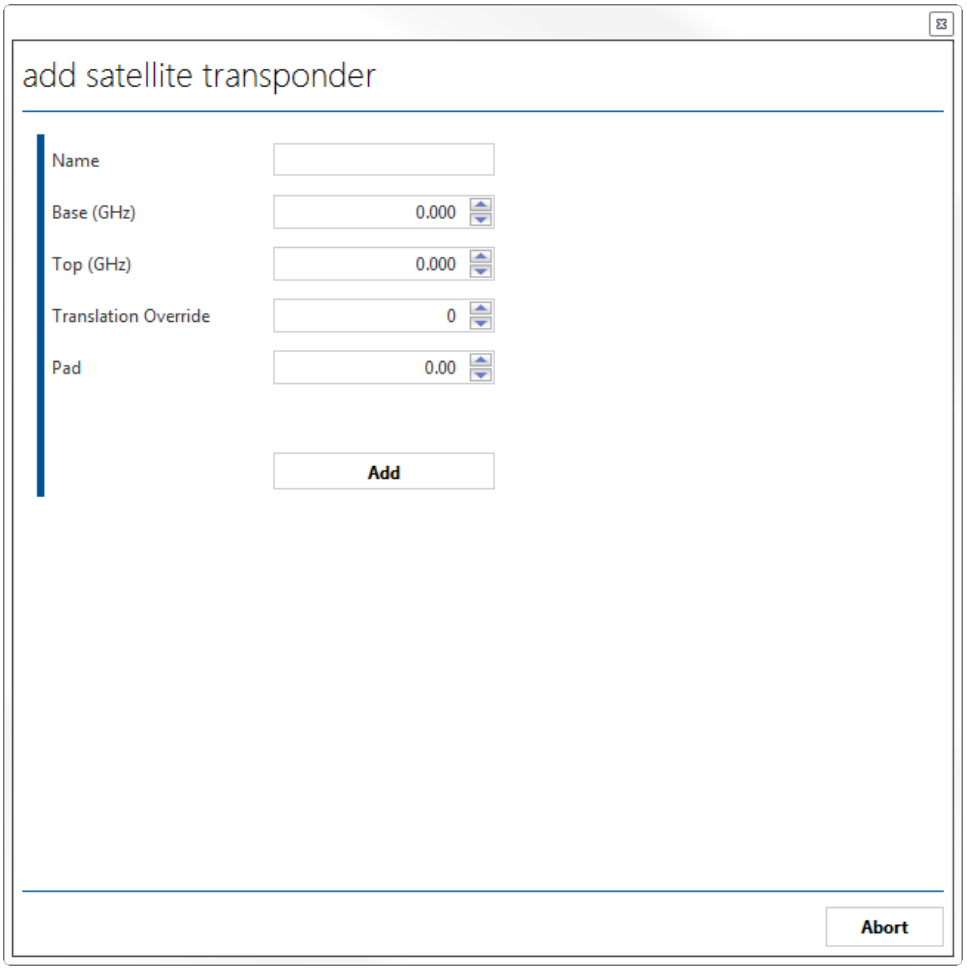


Figure 5-14. Add Satellite Transponder Page

3. Enter the *Name* of the transponder.
4. Enter the *Base* frequency in GHz.
5. Enter the *Top* frequency in GHz.
6. Enter the *Translation Override* of the transponder.
7. Enter the *Pad* for the transponder.
8. Click *Add.*

To delete a transponder from the table, click the* Delete *button adjacent to the transponder that must be deleted.

SPACE SEGMENT EXCLUSIONS

Exclusions are used to block out a section of bandwidth in the dSCPC bandwidth pool.

1. To add an exclusion, click the *Add* button under the *SPACE SEGMENT EXCLUSIONS* table.

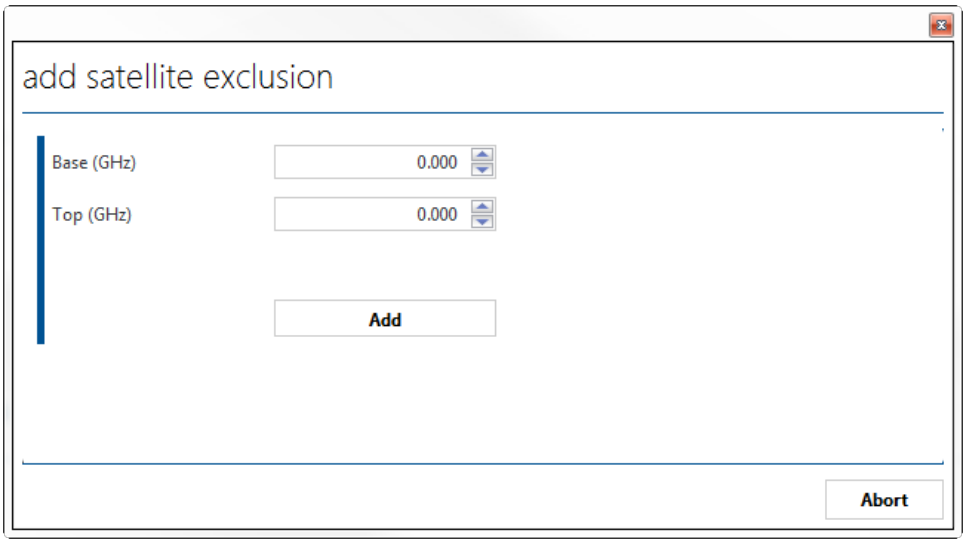


Figure 5-15. Add Satellite Exclusion Page

2. Enter the *Base* frequency in GHz
3. Enter the *Top* frequency in GHz
4. Click *Add*

To delete an exclusion from the table, click the* Delete *button adjacent to the exclusion that must be deleted.

dSCPC Bandwidth Pool

To create a bandwidth pool:

1. Click the *Add* button under the *dSCPC BANDWIDTH POOL* table.

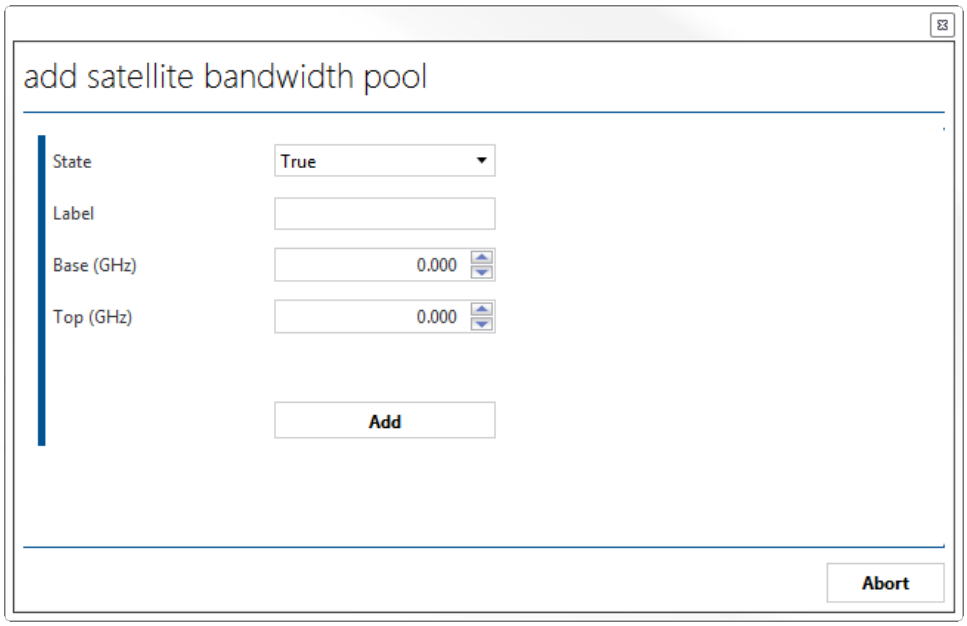


Figure 5-16. Add Satellite Bandwidth Pool Page

2. Enter / Edit the following information:

   State: Enable or disable the CEFD Bandwidth Manager from using this bandwidth pool by selecting *True* or *False*
   Label: Enter a name for the dSCPC bandwidth pool
   Base (GHz): Enter the base frequency in GHz
   Top (GHz): Enter the top frequency in GHz

3. Click *Add.*

To delete a bandwidth pool, click the* Delete *button adjacent to the pool that must be deleted.

5.2.5 Add Service Area

Once the CEFD Bandwidth Manager, Network, and Satellite have been created in NetVue, you can add a Service Area.

1. Click the *Add* button under the *SERVICE AREA* table.
2. Enter / Edit the following information:
   Enter the *name* of the Service Area.
   Select the *IP address* of the CTOG-250 or HTO-1 associated with the Service Area.
   Select the *Satellite* associated with the Service Area.
3. Click *Add*.

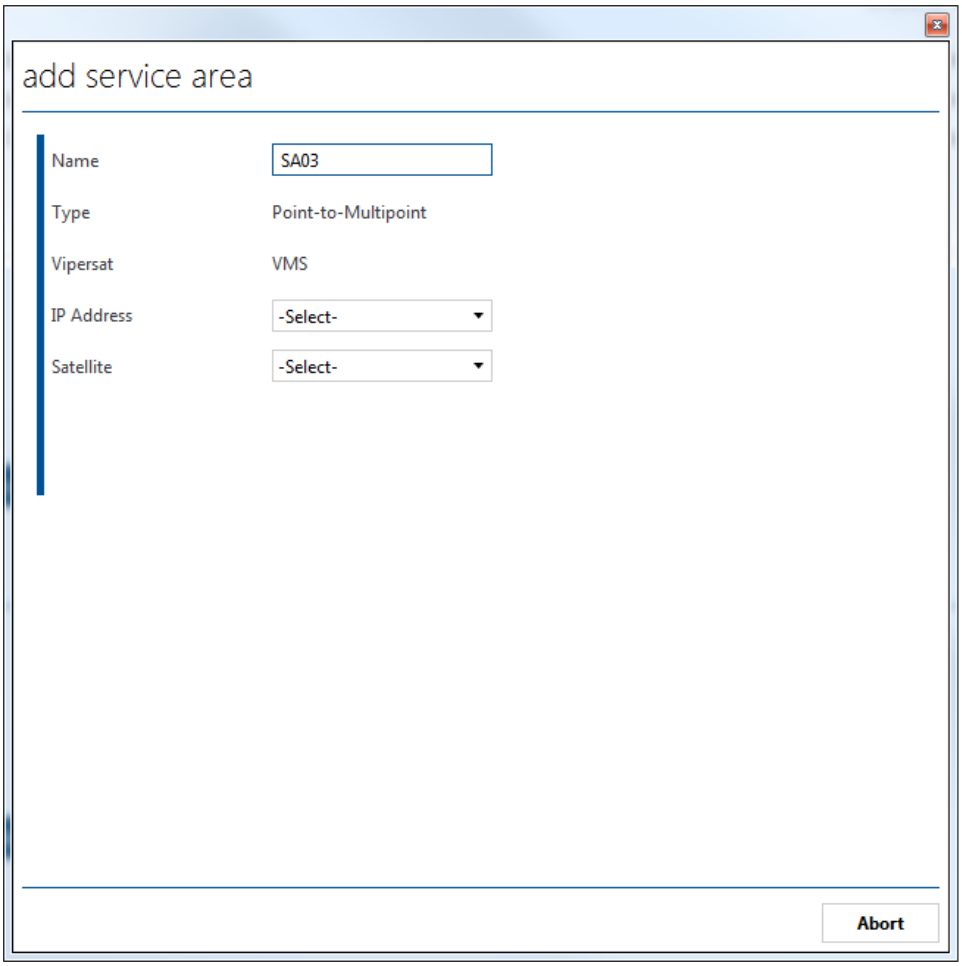


Figure 5-17. Add Service Area Page

5.2.6 Configure Service Area

1. To configure the Service Area, select the Service Area from the list on the SERVICE GROUP card.
2. Click *Details* on the Service Area that will be configured.

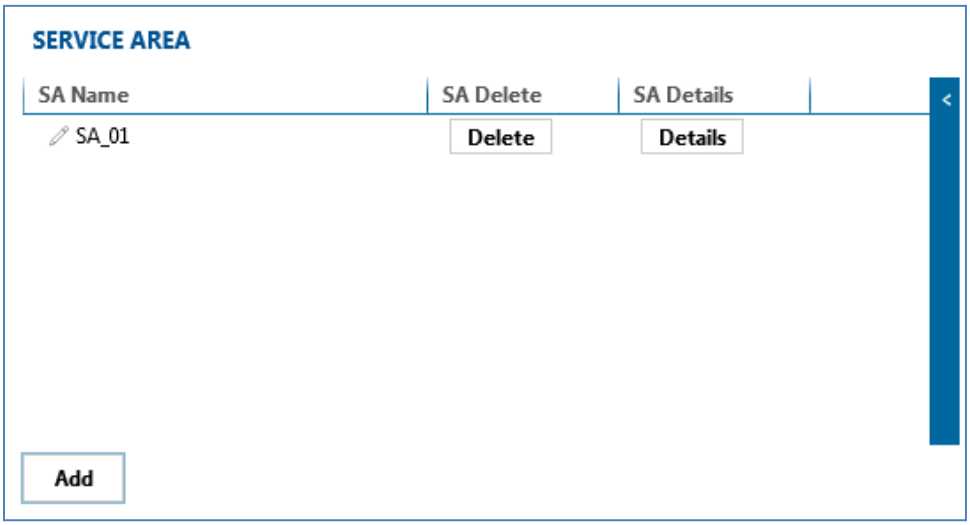


Figure 5-18. Service Area Page

5.2.6.1 Point-to-point Networks (Beta – not fully supported in this release)

Clicking on the details button for a **Point-to-point** network opens the *SERVICE AREA* card, where you can make additional configuration changes.

Figure 5-19. Point-to-Point Configuration Views

On this card, the Point-to-Point View settings will display the following submenus:

- *General – The General Page displays read only information associated to the Service Area.*
- *Hub Settings* – The Hub Settings page allows the operator to configure the components that will be used in the Hub Environment.
- *Remote Settings* – The Remote Settings page allows the operator to configure the components that will be used at the remote.
- *Circuit Settings* – Allows the linkage between hub equipment and remote equipment to create a circuit.

5.2.6.1.1 General

1. On the Point-to-Point View Page, select configuration.
2. Select *General* at the top of the page.

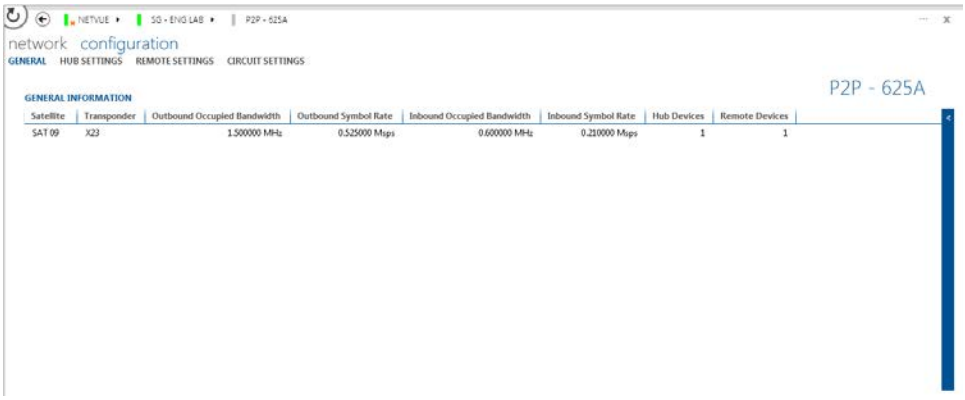


Figure 5-20. General Configuration View

General: The General Page displays read only information associated to the Service Area.

- *Satellite: Displays the satellite(s) associated to the Service Area.*
- *Transponder: Displays the transponder(s) associated to the Service Area.*
- *Outbound Occupied Bandwidth: Displays the Outbound Occupied Bandwidth consumed for the particular Satellite/Transponder.*
- *Outbound Symbol Rate: Displays the Outbound Symbol Rate for the particular Satellite/Transponder.*
- *Inbound Occupied Bandwidth: Displays the Inbound Occupied Bandwidth for the particular Satellite/Transponder.*
- *Inbound Symbol Rate: Displays the Inbound Symbol Rate for the particular Satellite/Transponder.*
- *Hub Devices: Displays the number of associated Hub Equipment for the Satellite/Transponder.*
- *Remote Devices: Displays the number of associated Remote Equipment for the Satellite/Transponder.*

5.2.6.1.2 Hub Configuration

To start the Hub configuration:

1. On the Point-to-Point View Page, select *configuration*.
2. Select *Hub Settings* at the top of the page.

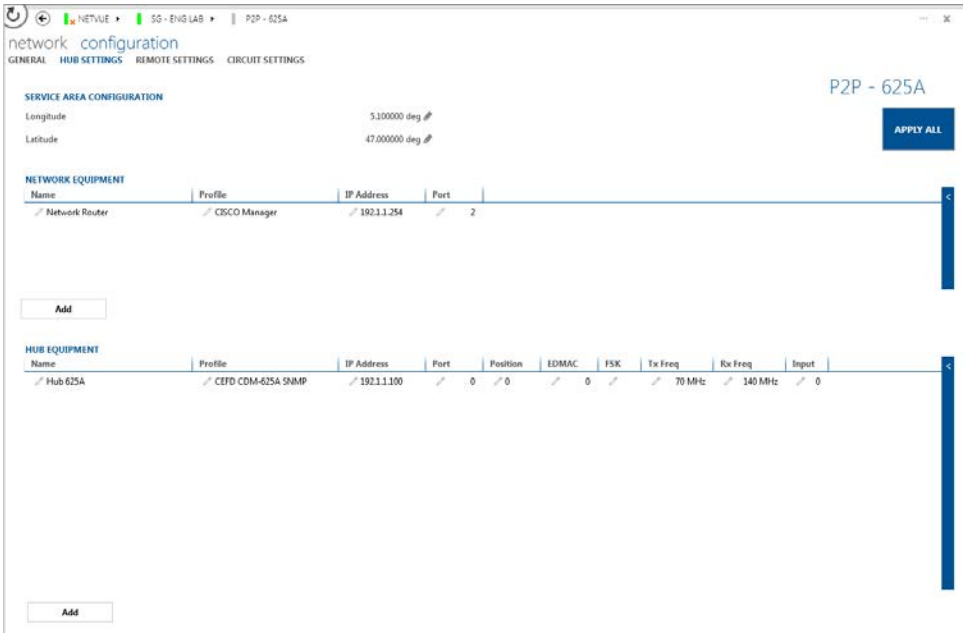


Figure 5-21. Hub Settings Page

Hub Settings – The Hub Settings page allows the operator to configure the components that belong in the Hub Environment – it is broken down to two subsections:

Network Equipment: A list of equipment that is not in the RF path to be monitored by NetVue.

Hub Equipment: A list of equipment that is in the RF path to be monitored by NetVue.

Under Service Area Configuration, the longitude and latitude can be defined.

1. *To add Network Equipment,* Click *Add.*
2. Enter / Edit the following information:

   Name: Enter the name of the Network Equipment.

   IP Address: Define the IP Address of the Device.

   Port: Define the port of the IP to Serial Gateway.

   Profile: Define the Equipment Type.

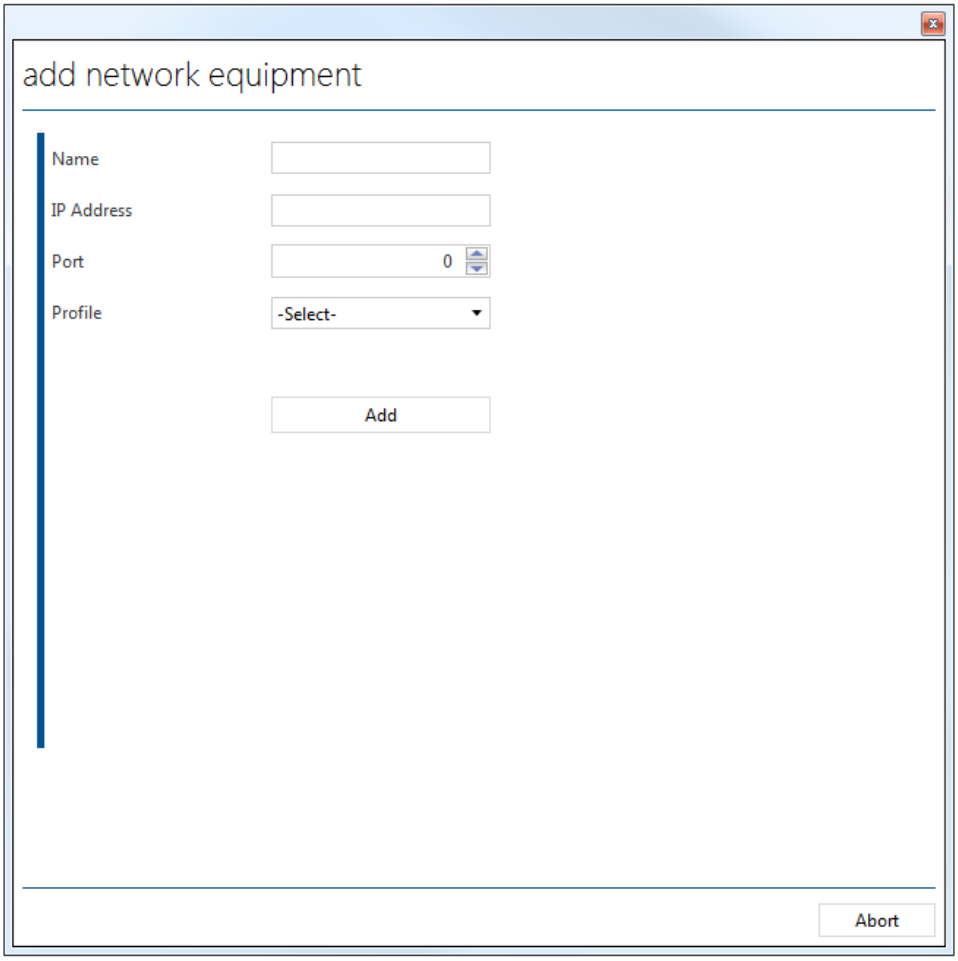


Figure 5-22. Add Network Equipment Page

To add Hub Equipment:

1. Click *Add.*
2. Enter / Edit the following information:

   Name: Enter the name of the Network Equipment.

   IP Address: Define the IP Address of the Device.

   Port: Define the port of the IP to Serial Gateway.

   Profile: Define the Equipment Type.

   Position: Defines the position of the equipment in the Circuit, where the number is the position (from right to left) on the circuit view and the number with a letter is the position A = Top and B = Bottom.

   EDMAC: If the device is a serial device, enter the EDMAC address.

   FSK: If FSK is in use, define as True.

   *Tx Frequency (MHz)***:** The center frequency (IF, L-band) to be programmed into the Spectrum Analyzer in order to appear in the thumbnail Spectral view of the TX signal in the Circuit View.

   Rx Frequency (MHz): The center frequency (IF, L-band) to be programmed into the Spectrum Analyzer in order to appear in the thumbnail Spectral view of the RX signal in the Circuit View

   Input: The input port on the spectrum analyzer. If the spectrum analyzer is single port device (Agilent or Anritsu) no entry is required. If multiport SED Decimator with eight (8) ports then ports 1 to 8.

3. Click *Add*.

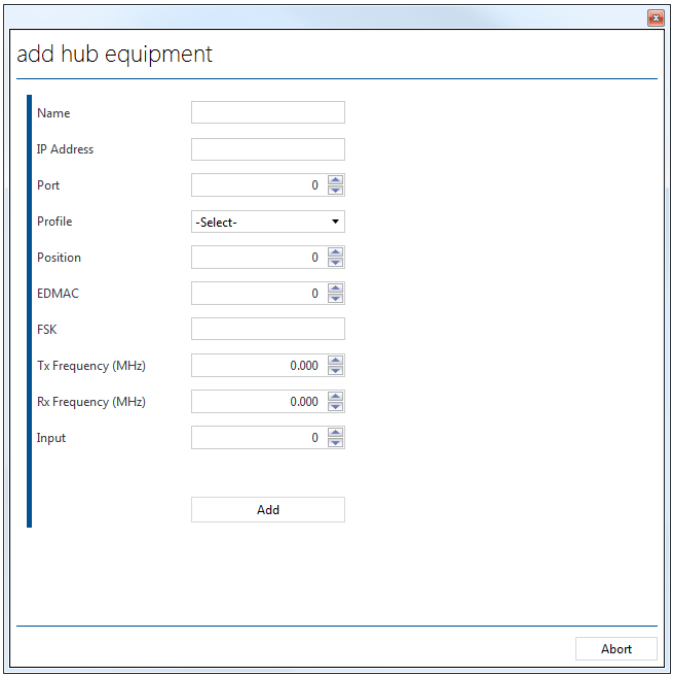


Figure 5-23. Add Hub Equipment Page

5.2.6.1.3 Remote Configuration

1. From the *Configuration* page on the Point-to-Point View card, select *Remote Settings*.

   Remote Settings – The Remote Settings page allows the operator to configure the components that are associated with the remote.

2. On the lower, left-hand side of the card, click *Create Remote.*
3. Enter / Edit the following information:

   Remote Name: Enter the name of the remote.
4. Click *Ok.*

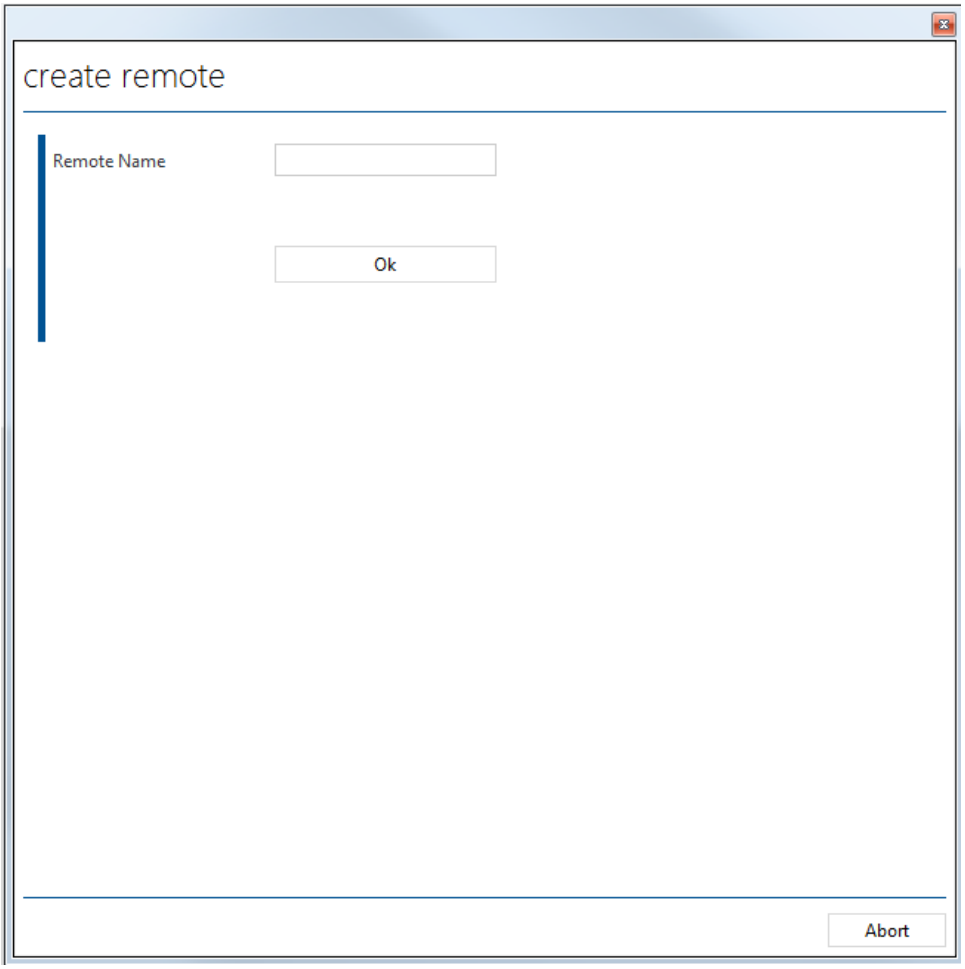


Figure 5-24. Add Remote Page

5. Once the Remote Site has been created it will display in the Remote table, select the remote within the table to display the Remote Configuration Pane:

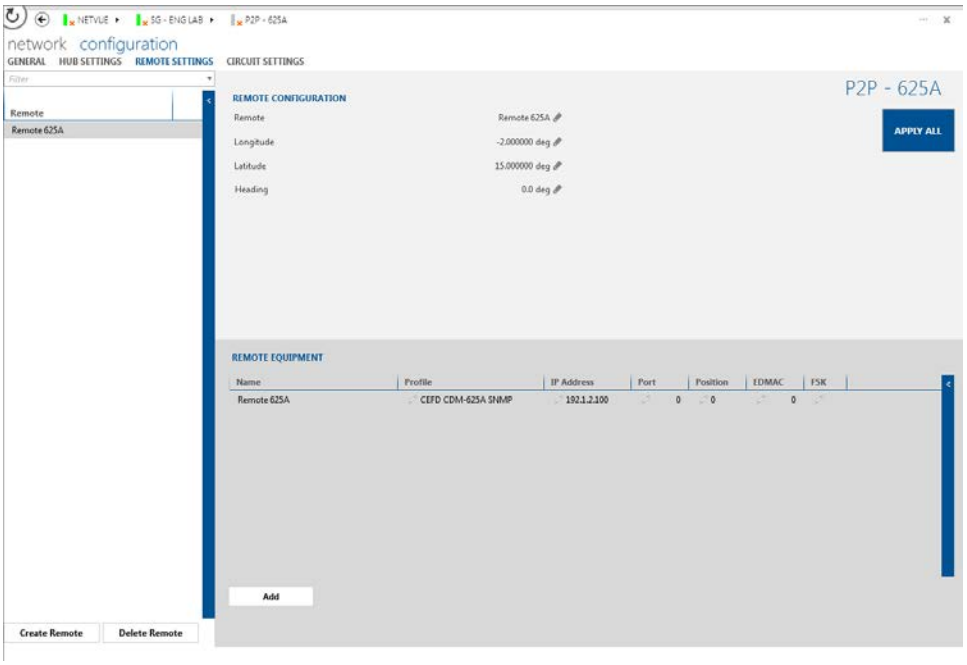


Figure 5-25 Remote Configuration Pane

Remote Configuration Pane – Allows an operator to make configurations to an individual remote site:

- *Remote*: Displays the current remote name and also allows you to modify the name of the remote.
- *Longitude: W*here the equipment is assigned – this results in the placement on the map view
- *Latitude:* Where the equipment is assigned – this results in the placement on the map view
- *Heading: W*here the equipment is assigned – this results in the placement on the map view

To add a Remote Equipment*:*

1. Click *Add*.
2. Enter / Edit the following information:

   Name: Enter the name of the equipment.
   IP Address: Enter the IP address of the device or of the IP to Serial Gateway.
   Port: Enter the IP Port of the IP to Serial Gateway.
   Profile: Defines the type of equipment to be associated to the remote site.
   Position: Defines the position of the equipment in the Circuit, where the number is the position (from right to left) on the circuit view and the number with a letter is the position A = Top and B = Bottom.
   EDMAC: If the device is a serial device, enter the EDMAC address.
   FSK: If FSK is in use, define as True.
3. Click *Add.*

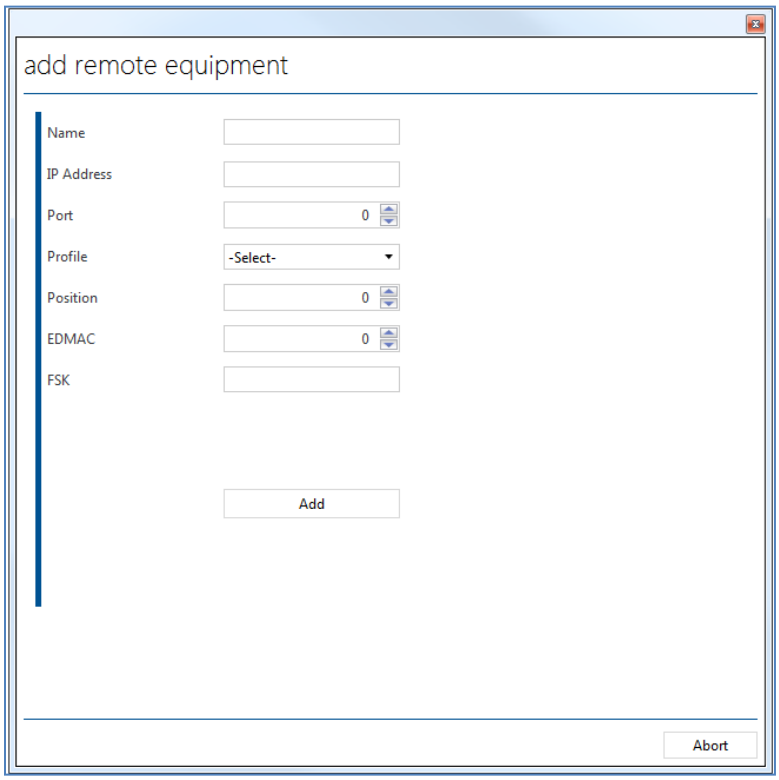


Figure 5-26. Add Remote Equipment

4. Repeat the steps above for any additional equipment that is to be monitored at the remote site by NetVue.

5.2.6.1.4 Circuit Settings

1. From the *Configuration* page on the Point-to-Point View card, select *Circuit Settings*.

   Circuit Settings – Allows the linkage between hub equipment and remote equipment to create a circuit.

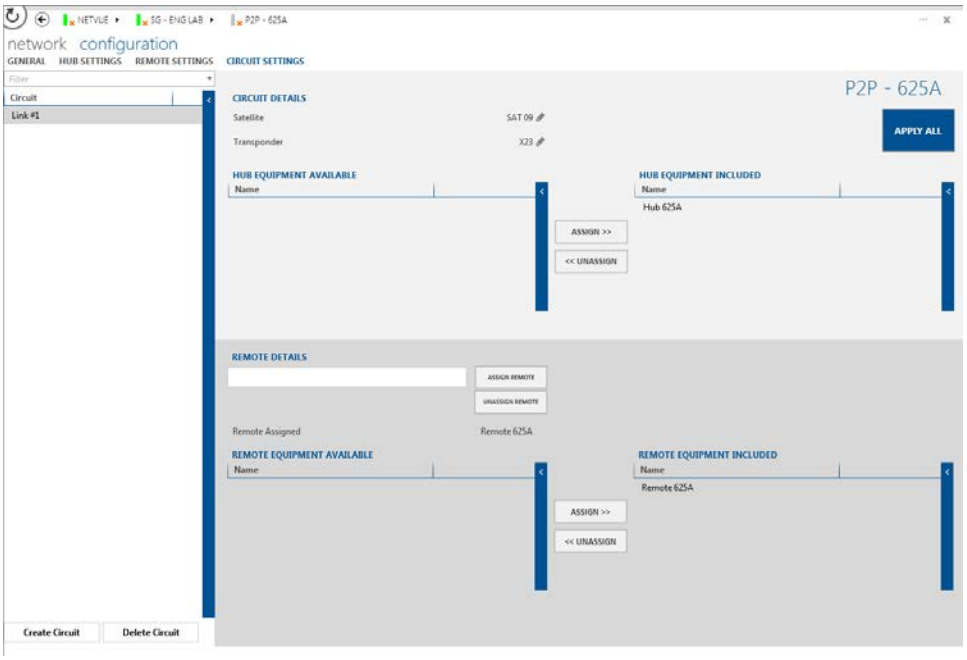


Figure 5-27. Circuit Settings Page

2. On the lower, left-hand side of the card, click *Create Circuit.*
3. Enter / Edit the following information:

   Circuit Name: Enter the name of the Circuit; this should be unique and easily identifiable to the network environment.

4. Click *Ok.*

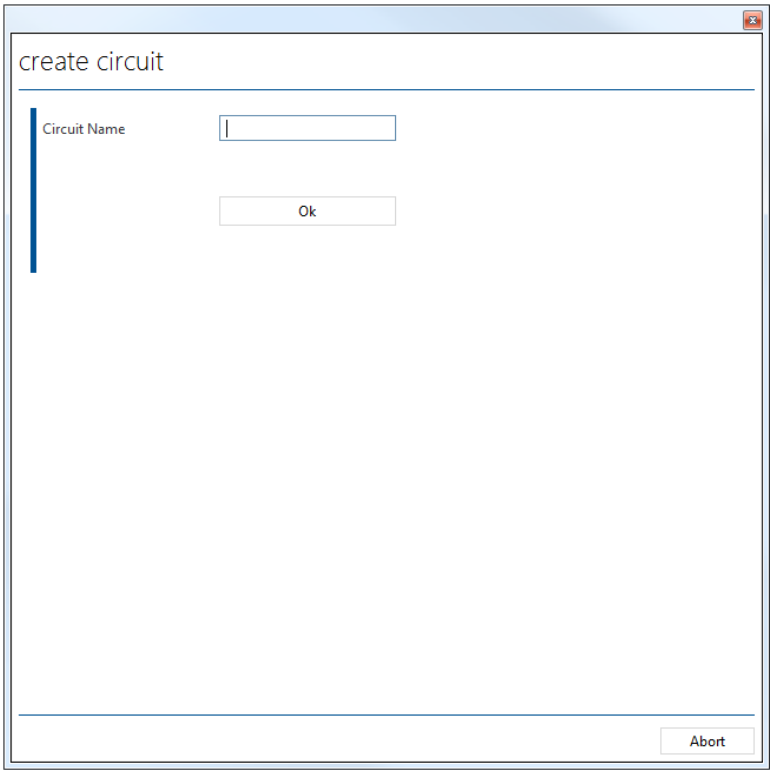


Figure 5-28. Create Circuit Page

5. Once the Circuit has been created it will display in the Circuit table, select the Circuit within the table to display the Circuit Configuration Pane:

   Circuit Details – Allows creation of Satellite and Transponder:

   To change a parameter, click the pencil icon next to it.

   Hub Equipment – Displays the Available, and assigned Hub Equipment.

   - To assign equipment select it in the available table and select the >>
   - *To un-assign equipment select it in the assigned table and select the* <<

   Remote Equipment – Displays the Available, and assigned Remote Equipment.

   - To assign equipment select it in the available table and select the >>
   - *To un-assign equipment select it in the assigned table and select the* <<

Once all of the equipment has been assigned, click *Apply All*.

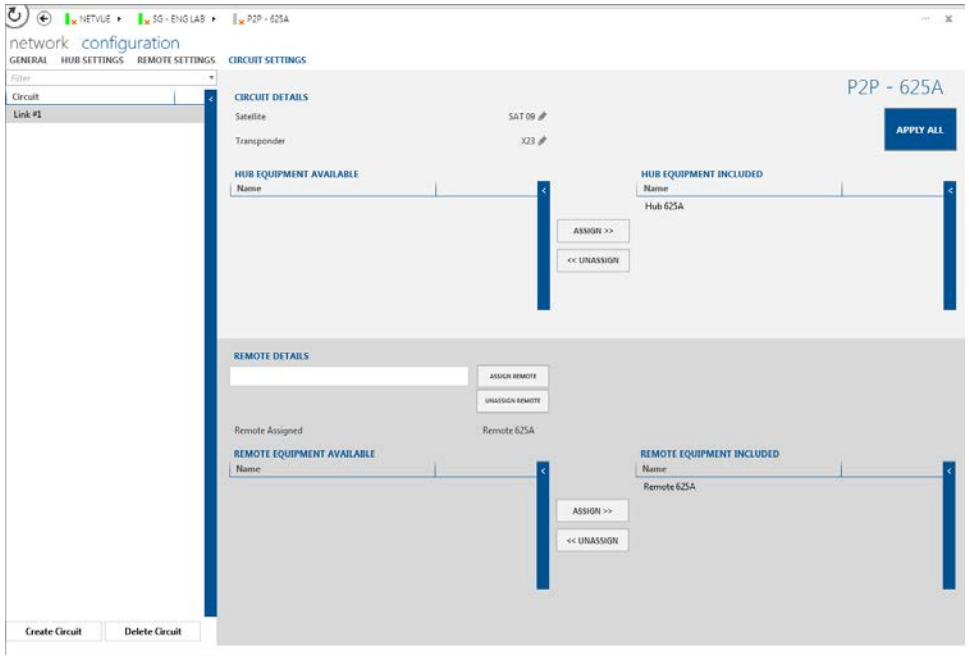


Figure 5-29. Circuit Configuration Page

5.2.6.2 Point-to-Multipoint Networks

1. Click on the details button for a **Point-to-Multipoint** network to open the *SERVICE AREA* card, where you can make additional configuration changes.

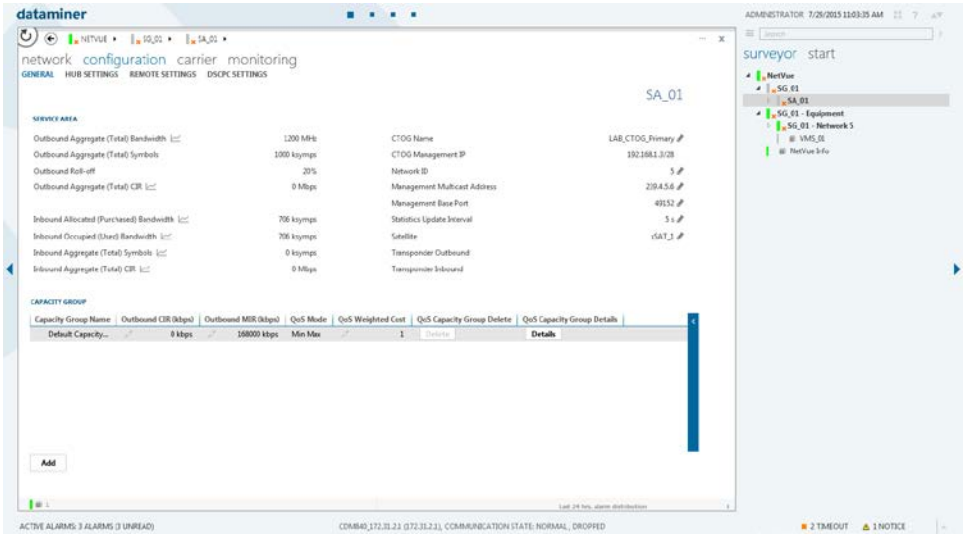


Figure 5-30. Service Area Card Page

2. On this card, change these Service Area settings:

   CTOG/HTO Name: The name of the CTOG-250 or HTO-1

   Network ID: Defines to which network the device belongs (valid range is 1-254)

   Management Multicast Address: The multicast IP assigned to all modems in the network that are managed by the CEFD Bandwidth Manager

CAUTION

Changing the *Management Base Port* address affects the entire network.

Configuration changes will be required for all modems.

It is necessary to change this setting ONLY if network port addressing is in contention.

- ***Management Base Port*: The management port used by the CEFD Bandwidth Manager to send and receive the management UDP packets**
- ***Statistics update Interval*: The time in seconds between each scheduled update from the remote sites**
- ***Satellite*: The satellite associated with this Service Area**

5.2.6.2.1 Hub Configuration

To start the Hub configuration:

1. On the Service Area page, select *Hub Settings* at the top of the page.
2. On the lower, left-hand side of the card, click *Create Hub.*
3. Enter / Edit the following information:

   Name: Enter the name of the hub.

   Comments: Enter any comments about the hub.

   Longitude: Enter the longitude of the hub.

   Latitude: Enter the latitude of the hub.

   Heading: Enter the heading, if necessary.

   Subnet: Select the subnet associated with the hub.
4. Click *Next.*

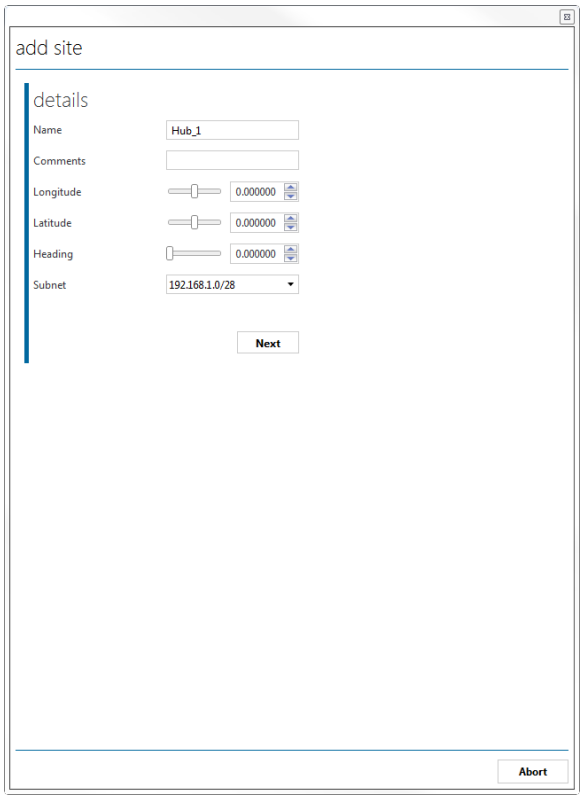


Figure 5-31. Add Site Page

5. On the next screen, enter the RF Profile information for the hub site.

   Converter Type: Select what frequency band to use (*L-Band*, *70 MHz*, *140 MHz* or *Custom*).

   Name: Enter the name of the up and down converters.

   Local Oscillator (GHz): Enter the LO frequency of the up and down converters.

   Bandwidth (MHz): Enter the bandwidth information for the up and down converters.

   Inversion: Select whether or not the up and down converters are inverted (*True* or *False*).

   Power Limit (dBm): Enter the power limit in dBm for the up converter, to prevent saturation.

6. Click *Next*.

Figure 5-32. Hub RF Profile Page

The hub is now created in NetVue. Use the *GENERAL* tab on the *hub settings* page to change the newly-created configuration.

7. To add the hub equipment, click the *EQUIPMENT* tab at the top of the *hub settings* page.

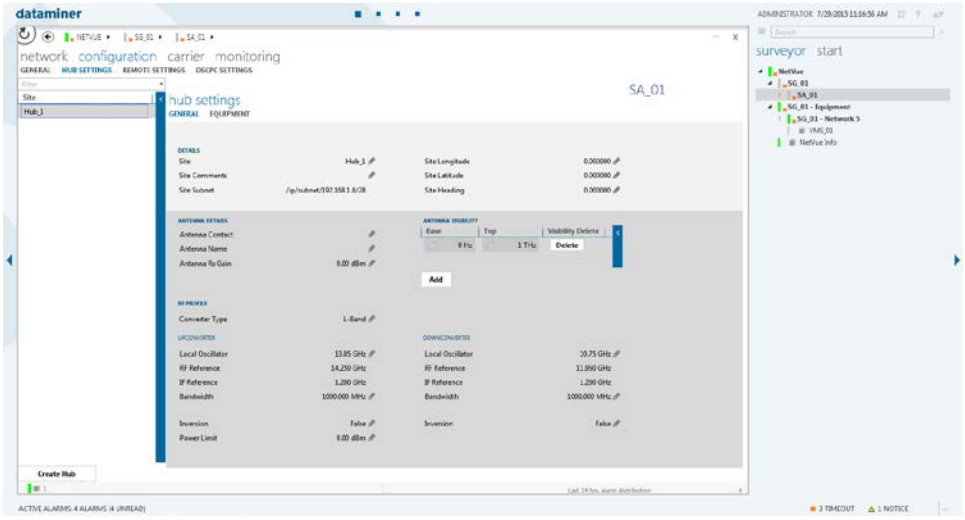


Figure 5-33. General Hub Settings Page

8. In the *Available modulators* section, select the modulator(s) that will be associated with the hub site.
9. Click the *ADD>>* button to assign them to the hub.
10. In the *Available demodulators* section, select the demodulator(s) that will be associated with the hub site.
11. Click the *ADD>>* button to assign them to the hub.
12. Select the toggle button under *ECM* to assign the demodulator as the ECM controller.
13. Select the toggle button under *Allocatable* to allocate the demodulator for use with the CEFD Bandwidth Manager.

To change the name of the modulators/demodulators, click the pencil icon next to the default name.

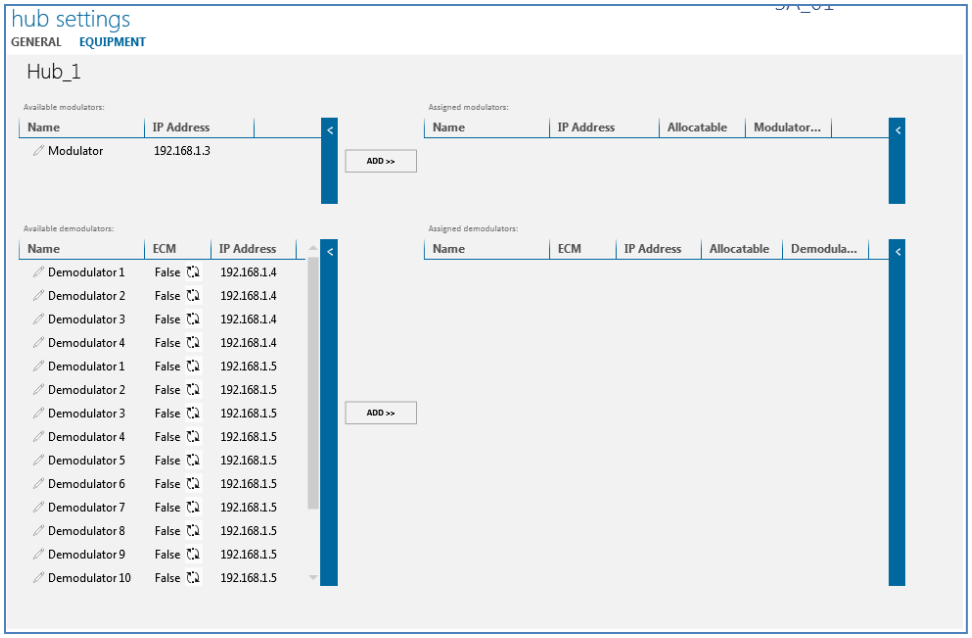


Figure 5-34. Hub Equipment Settings Page

5.2.6.2.2 Remote Configuration

5.2.6.2.2.1 Remote Configuration - General

1. From the *Configuration* page on the Service Area card, select *Remote Settings*.
2. On the lower, left-hand side of the card, click *Create Remote.*
3. Enter / Edit the following information:

   Name: Enter the name of the remote.
   Comments: Enter any comments about the remote**.**
   Longitude: Enter the longitude of the remote*.*
   Latitude: Enter the latitude of the remote**.**
   Heading: Enter the heading, if necessary**.**
   Subnet: Select the subnet associated with the remote*.*
4. Click *Next.*

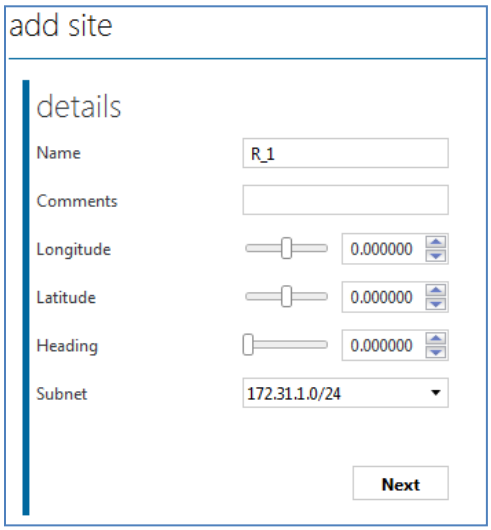


Figure 5-35. Add Site Page

5. On the next screen, enter the RF Profile information for the remote site:

   Converter Type: Select the frequency band (*L-Band*, *70 MHz*, *140 MHz* or *Custom*).
   Name: Enter the name of the up and down converters.
   Local Oscillator (GHz): Enter the LO frequency of the up and down converters.
   Bandwidth (MHz): Enter the bandwidth information for the up and down converters.
   Inversion: Select whether or not the up and down converters are inverted (*True* or *False*).
   Power Limit (dBm): Enter the power limit in dBm for the up converter, to prevent saturation.

6. Click *Next.*

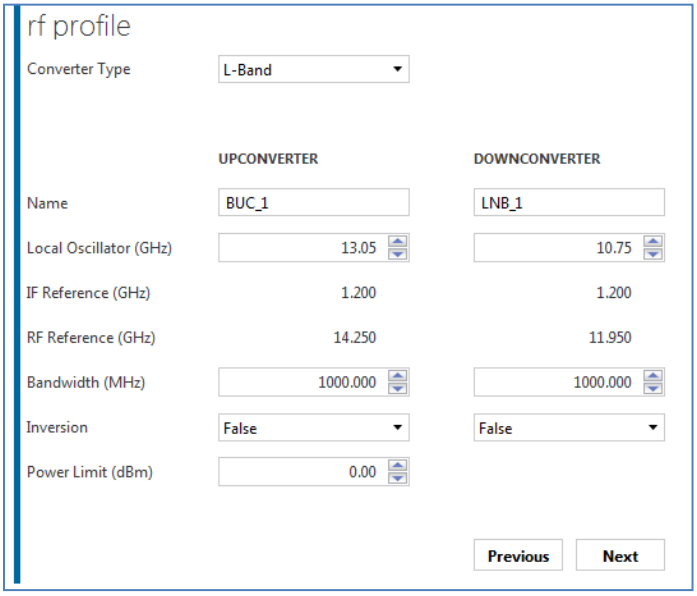


Figure 5-36. Remote RF Profile Page

The remote is created in NetVue. Use the *GENERAL* tab on the *remote settings* page to edit the newly-created configuration.

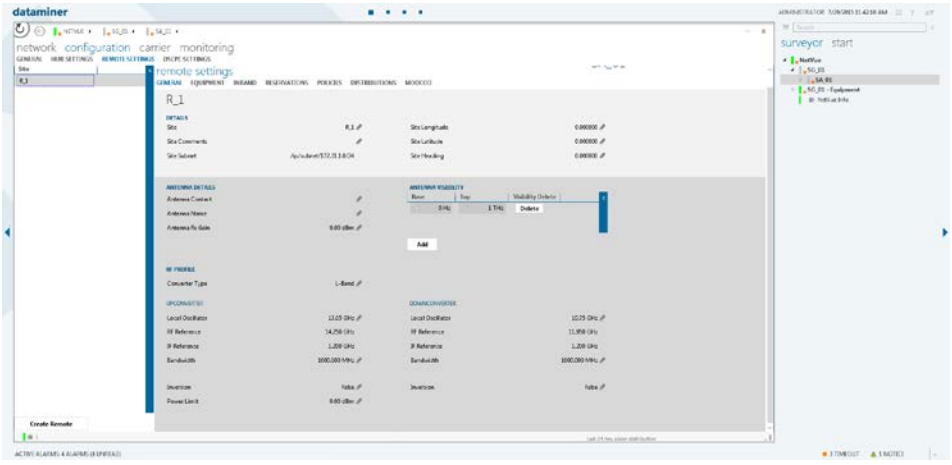


Figure 5-37. Remote Configuration - General Settings Page

5.2.6.2.2.2 Remote Configuration - Equipment

1. To add the remote equipment, click the *Equipment* tab at the top of the *Remote Settings* page.

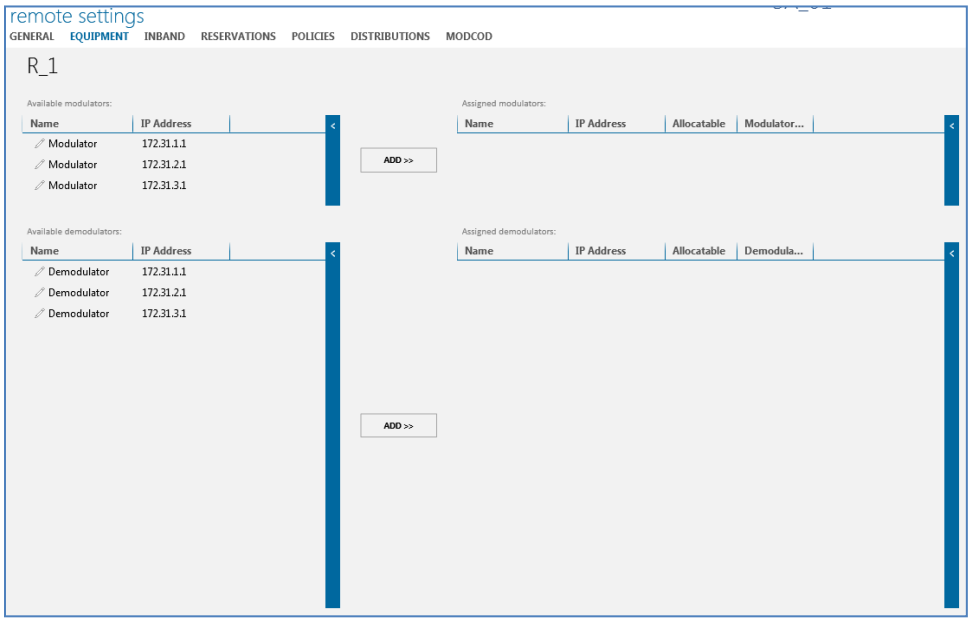


Figure 5-38. Remote Configuration - Equipment Page

2. In the *Available modulators* section, select the modulator(s) that will be associated with the remote site.

   Click the *ADD>>* button to assign them to the remote.

3. In the *Available demodulators* section, select the demodulator(s) that will be associated with the remote site.

   Click the *ADD>>* button to assign them to the remote.

4. Select the toggle button under *Allocatable* to allocate the demodulator for use with the CEFD Bandwidth Manager in meshing mode.

To change the name of the modulators/demodulators, click the pencil icon next to the default name.

5.2.6.2.2.3 Remote Configuration - Inband

1. To enable Inband for the remote site, click the *Inband* tab at the top of the *remote settings* page.

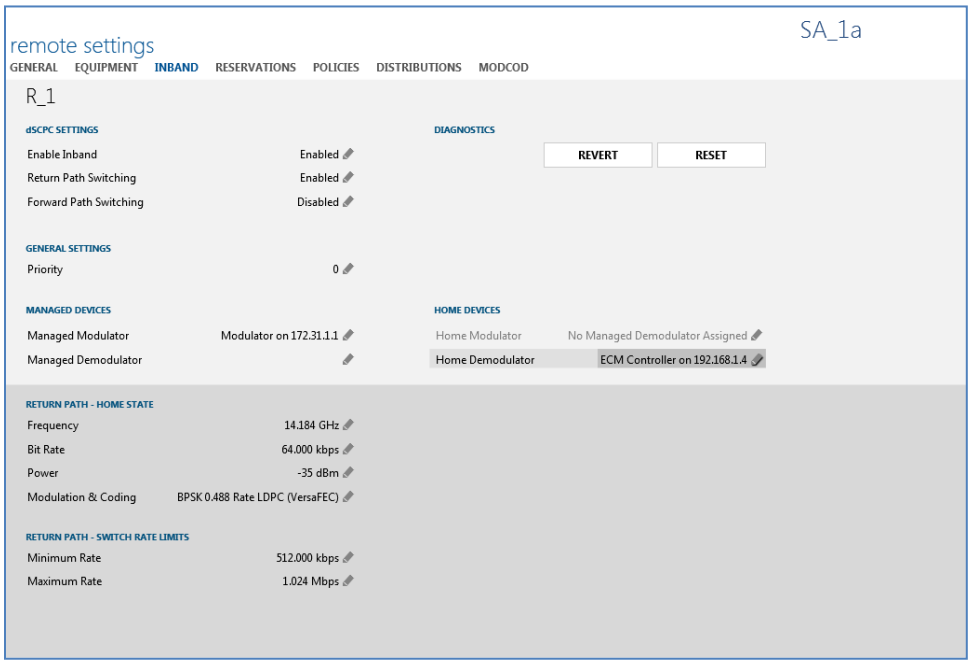


Figure 5-39. Remote Configuration – Inband Page

2. Enter / Edit the following information:

   Enable Inband: Select *Enabled* to enable the Inband, or *Disabled* to disable the Inband settings.

   Return Path Switching: *Enable* or *Disable* Return Path Switching.

   Forward Path Switching: *Enable* or *Disable* Forward Path Switching.

   Priority: If required, specify a priority for the site.

   Managed Modulator: Select the remote modulator (used with Return Path Switching).

   Managed Demodulator: Select the remote demodulator (used with Forward Path Switching).

   Home Modulator: Select the hub modulator used for the TDM (used with Forward Path Switching).

   Home Demodulator: Select the home-state ECM controller for this remote (used with Return Path Switching).

   Frequency: Set the home-state frequency, in GHz, for the remote modem (should correspond to the frequency of the ECM channel).

   Bit Rate: Set the home-state bit rate, in kbps, for the remote modem (should correspond to the bit rate of the ECM channel).

   Power: Set the home-state power level, in dBm, for the remote modem.

   Modulation & Coding: Set the home-state MODCOD for the remote modem (should correspond to the MODCOD of the ECM channel).

   Minimum Rate: Set the minimum switch rate limit, in kbps, for the remote site.

   Maximum Rate: Set the maximum switch rate limit, in kbps, for the remote site.

If all parameters are configured correctly, the remote site will switch out into the bandwidth pool.

5.2.6.2.2.4 Remote Configuration - Reservations

1. To configure the Remote Reservations, click the *Reservations* tab at the top of the *remote settings* page.

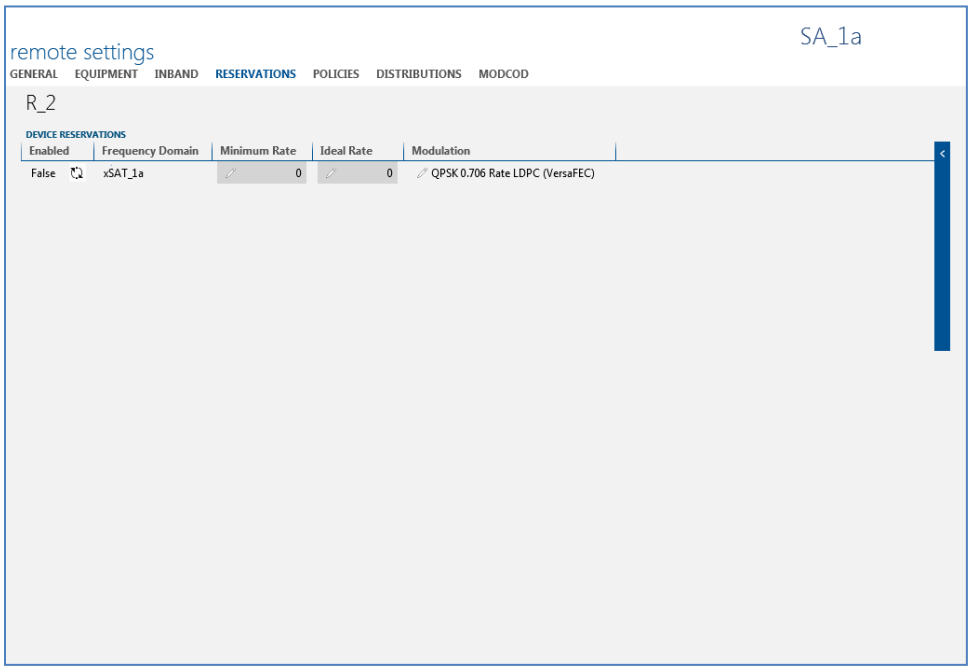


Figure 5-40. Remote Configuration - Reservations Page

2. Enter / Edit the following information:

   Enabled: Select *True* or *False* to enable or disable the site reservation.
   Minimum Rate: Set the desired minimum rate for the site.
   Ideal Rate: Set the ideal rate for the site.
   Modulation: Select the MODCOD used for the reservation.

5.2.6.2.2.5 Remote Configuration - Policies

To configure the Remote Policies, click the *Policies* tab at the top of the *Remote Settings* page.

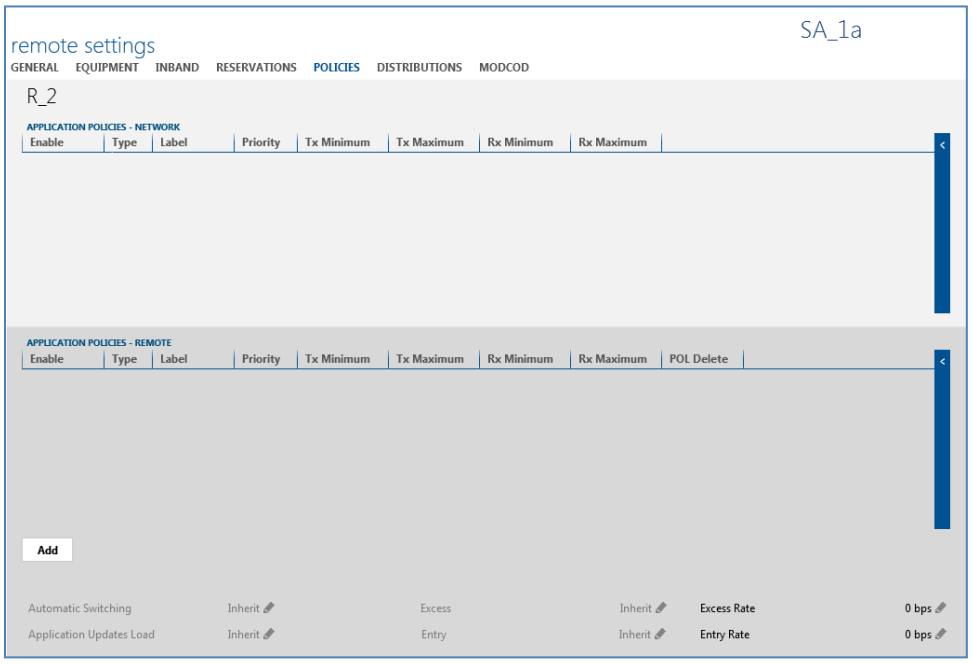


Figure 5-41. Remote Configuration - Policies Page

If configured, a list of the network policies appears under the *APPLICATION POLICIES – NETWORK* table.

1. To add a new, individual remote policy, click the *Add* button under the APPLICATION POLICIES – REMOTE table.

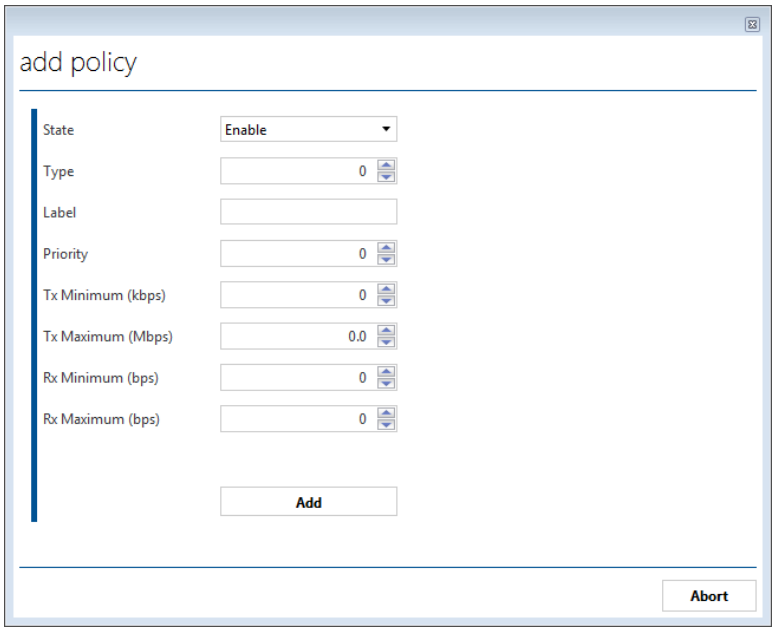


Figure 5-42. Remote Configuration – Policy Page

2. Enter / Edit the following information:

   State: Enabled or Disabled.
   Type: Application Policy Type numbers have these meanings:
   - 0 – ECM Load Switching
   - 1 – Scheduled Switching and VFS
   - 2 – Voice
   - 3 – Video
   - 4-63 – Reserved for the System
   - 64-253 – User Defined
   - 254 – Uninterruptable Switch / Immobile Carrier

   Label: Enter a label for the policy.
   Priority: Enter a priority level to be assigned to the policy.

A lower number means a higher priority. Priority 1 is the highest priority. Exception: Priority 0 (default) means No priority.

   Tx Minimum (kbps): Enter the minimum transmit rate in kbps.
   Tx Maximum (kbps): Enter the maximum transmit rate in kbps.
   Rx Minimum (kbps): Enter the minimum receive rate in kbps.
   Rx Maximum (kbps): Enter the maximum receive rate in kbps.

3. Click *Add*.

4. At the bottom of the *POLICIES* page, configure these parameters as well:

   Automatic Switching: Select *Enabled*, *Disabled* or *Inherit*. By default, this is enabled for the entire network. Thus, this is set to **Inherit** for each remote by default.

   Application updates Load: Select *Enabled*, *Disabled* or *Inherit*. By default, this is set to *Inherit*.

   Excess: Select *Enabled*, *Disabled* or *Inherit*. By default, this is set to *Inherit*.

   Entry: Select *Enabled*, *Disabled* or *Inherit*. By default, this is set to *Inherit*.

   Excess Rate: Set the desired excess bit rate for all application switching. This adds an extra margin of bandwidth to the carrier.

   Entry Rate: Set the desired entry rate for the site. By default, the initial data rate is the minimum switch rate setting.

5.2.6.2.2.6 Remote Configuration - Distributions

1. To configure the Remote Distribution lists, click the *DISTRIBUTIONS* tab at the top of the *remote settings* page.

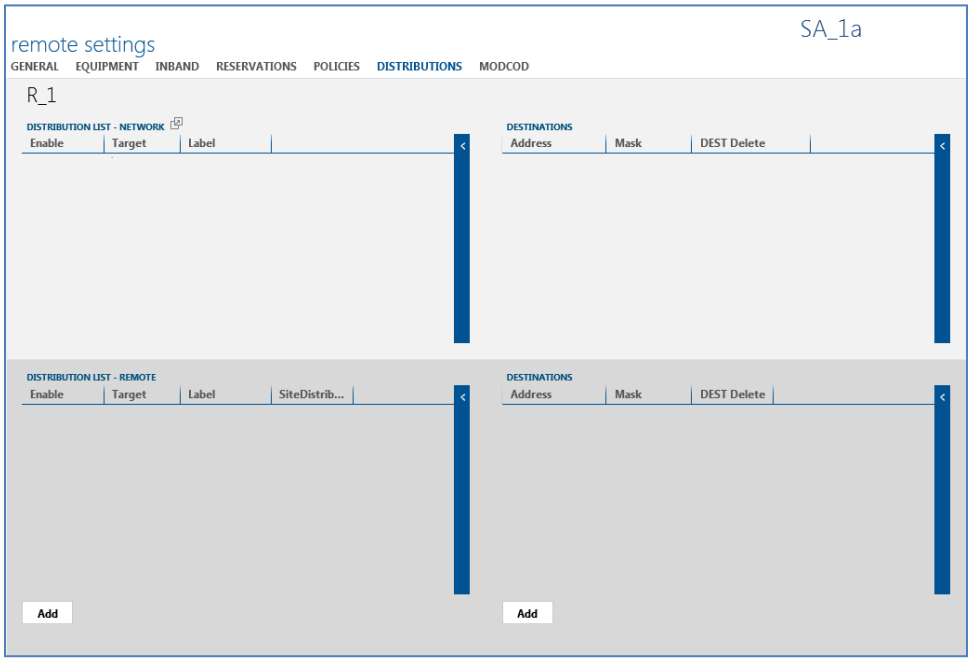


Figure 5-43. Remote Configuration - Distribution Page

If configured, a list of network distributions shows up under the DISTRIBUTION LIST – NETWORK table.

2. To add a new, individual remote distribution list, click the *Add* button under the DISTRIBUTION LIST – REMOTE table.

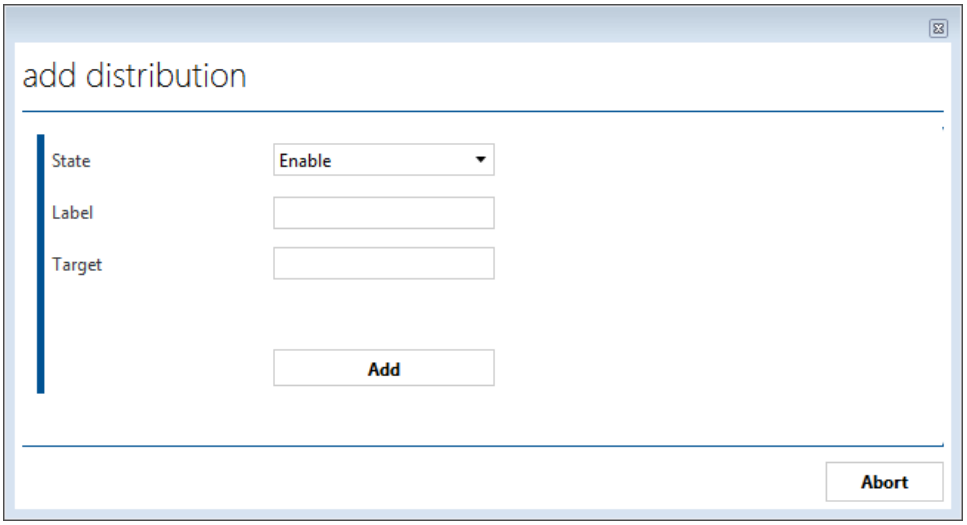


Figure 5-44. Add Distribution Page

3. Enter / Edit the following information:

   State: *Enable* or *Disable* this rule.
   Label: Enter a label for this rule.
   Target: Set the target multicast or unicast address.

4. Click *Add.*

If the Target address is set to 0.0.0.0, ANY application switch for this site activates the list.

5. Click the *Add* button under the DESTINATIONS table.

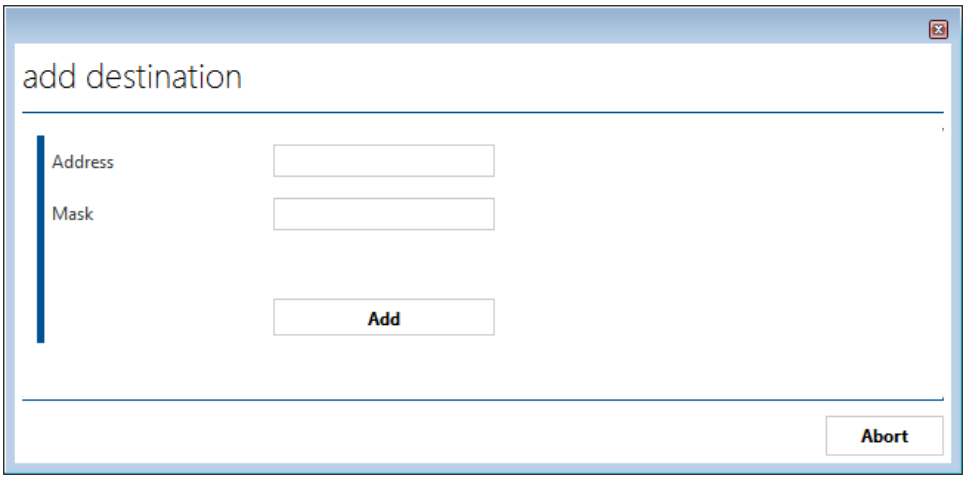


Figure 5-45. Add Destination Page

6. Enter / Edit the following information:

   Address: Enter the IP address to be added to the list.
   Mask: Enter the subnet mask to be added to the list.

7. Click *Add.*

5.2.6.2.2.7 Remote Configuration – MODCOD

1. To configure the remote MODCOD information, click the *MODCOD* tab at the top of the *remote settings* page.

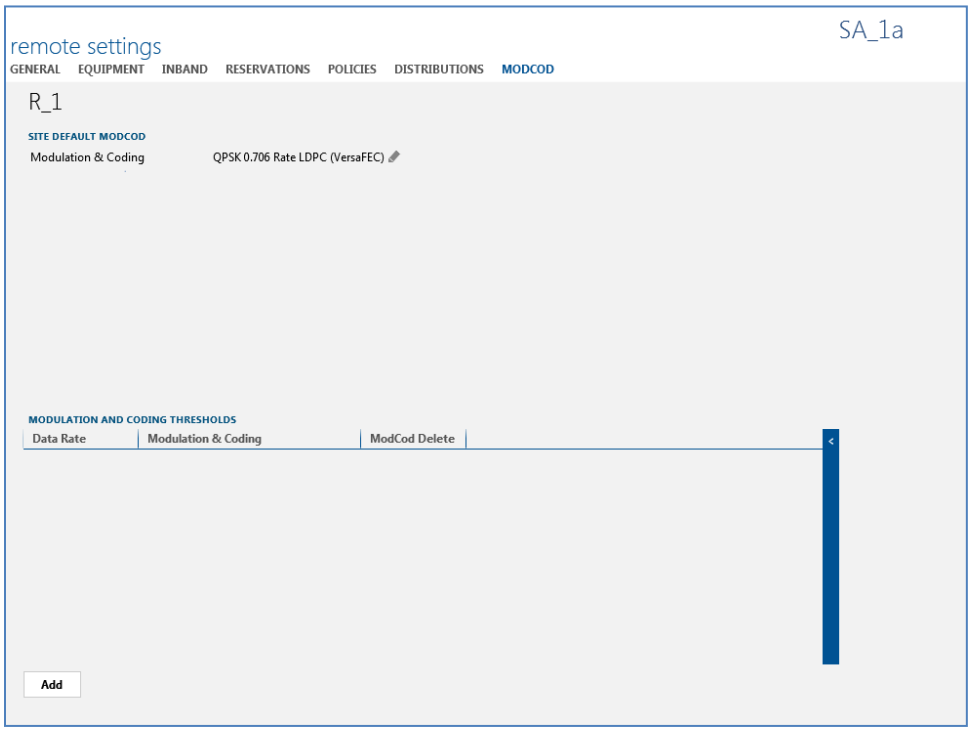


Figure 5-46. Remote Configuration - MODCOD Page

2. Click the pencil icon next to the *SITE DEFAULT MODCOD* to change the default MODCOD setting for the remote site.
3. To add MODCOD thresholds, click the *Add* button under the *MODULATION AND CODING THRESHOLDS* table.

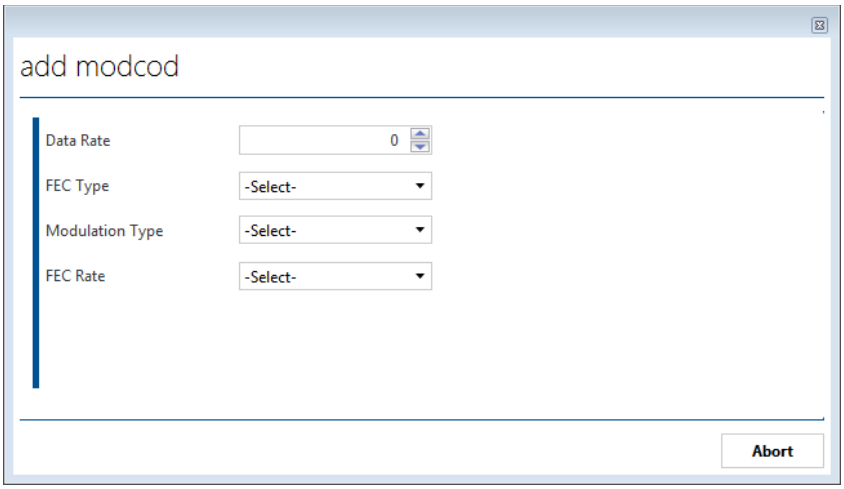


Figure 5-47. Add MODCOD Page

4. Enter / Edit the following information:

   Data Rate: Set the data rate in kbps.
   FEC Type: Select the desired FEC.
   Modulation Type: Select the desired modulation.
   FEC Rate: Select the desired FEC rate.

5. Click *Add.*

5.2.6.2.3 DSCPC Configuration

1. On the Service Area page, select *DSCPC SETTINGS* at the top of the page to start the network DSCPC configuration.

   Use this page to set network-wide policies that affect all of the remotes in the network.

   To change a parameter, click the pencil icon next to it.

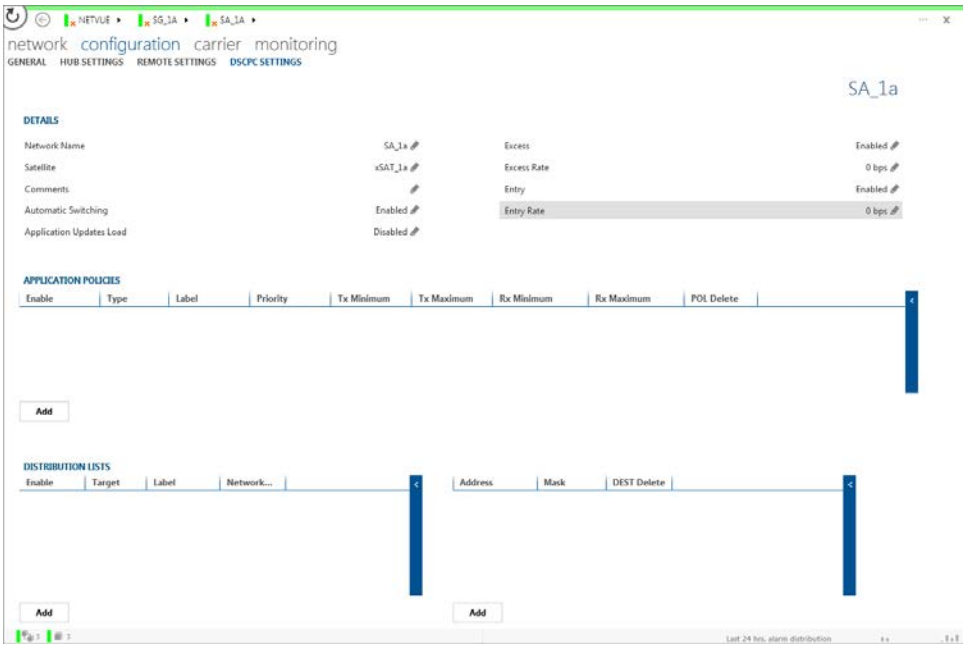


Figure 5-48. DSCPC Configuration Page

2. Enter / Edit the following information:

   Network Name: Edit the Service Area network name.
   Satellite: Edit the name of the Satellite associated with the Service Area.
   Comments: Add or delete comments.
   Automatic Switching: Enable or Disable automatic switching for the entire network.
   Application updates Load: *Enable* or *Disable* application updates load for the entire network.
   Excess: *Enable* or *Disable* excess for the entire network.
   Excess Rate: Set the excess rate to be used across the network.
   Entry: *Enable* or *Disable* entry for the entire network.
   Entry Rate: Set the entry rate to be used across the network.

5.2.6.2.3.1 Application Policies

1. To create an application policy that will affect the entire network, click the *Add* button under the APPLICATION POLICIES table.

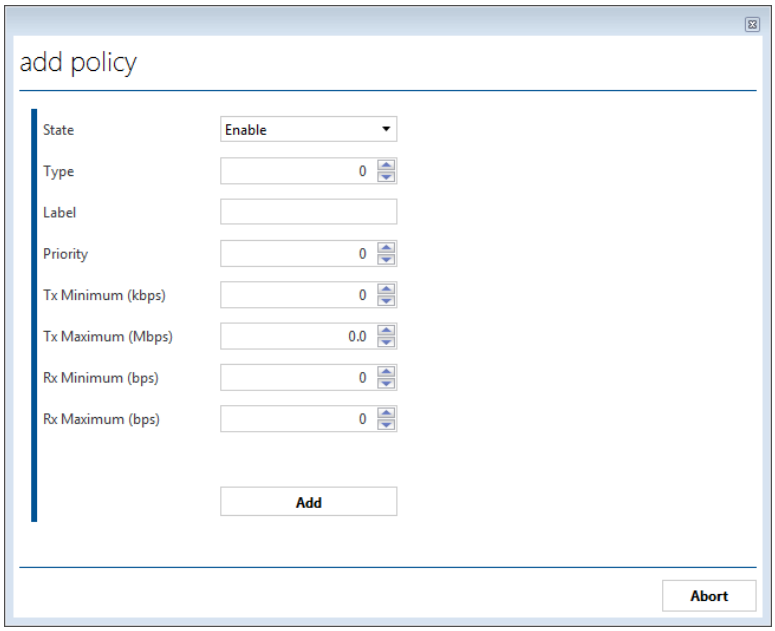


Figure 5-49. Network Application Policy

2. Enter / Edit the following information:

   State: Select *Enabled* or *Disabled*.
   Type: Application Policy Type numbers have these meanings:
   - 0 – ECM Load Switching
   - 1 – Scheduled Switching and VFS
   - 2 – Voice
   - 3 – Video
   - 4-63 – Reserved for the System
   - 64-253 – User Defined
   - 254 – Uninterruptable Switch / Immobile Carrier

   Label: Enter a label for the policy.
   Priority: Enter a priority level to be assigned to the policy.

   A lower number means a higher priority. Priority 1 is the highest priority. Exception: Priority 0 (default) means NO priority.

   Tx Minimum (kbps): Enter the minimum transmit rate in kbps.
   Tx Maximum (kbps): Enter the maximum transmit rate in kbps.
   Rx Minimum (kbps): Enter the minimum receive rate in kbps.
   Rx Maximum (kbps): Enter the maximum receive rate in kbps.

3. Click *Add*.

5.2.6.2.3.2 Distribution List

1. To create an application policy that affects the entire network, click the *Add* button under the DISTRIBUTION LIST – REMOTE table.

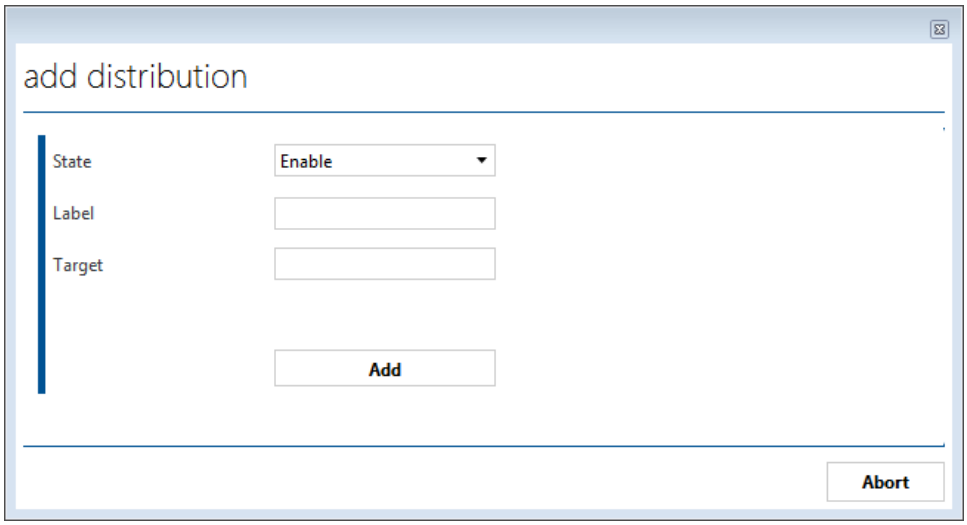


Figure 5-50. Network Distribution

2. Enter / Edit the following information:

   State: Select whether or not you want this rule to be *Enabled* or *Disabled.*
   Label: Enter a label for this rule.
   Target: Set the target multicast or unicast address.

3. Click *Add.*

If the Target address is set to 0.0.0.0, ANY application switch for this site activates the list.

4. Click the *Add* button under the DESTINATIONS table.

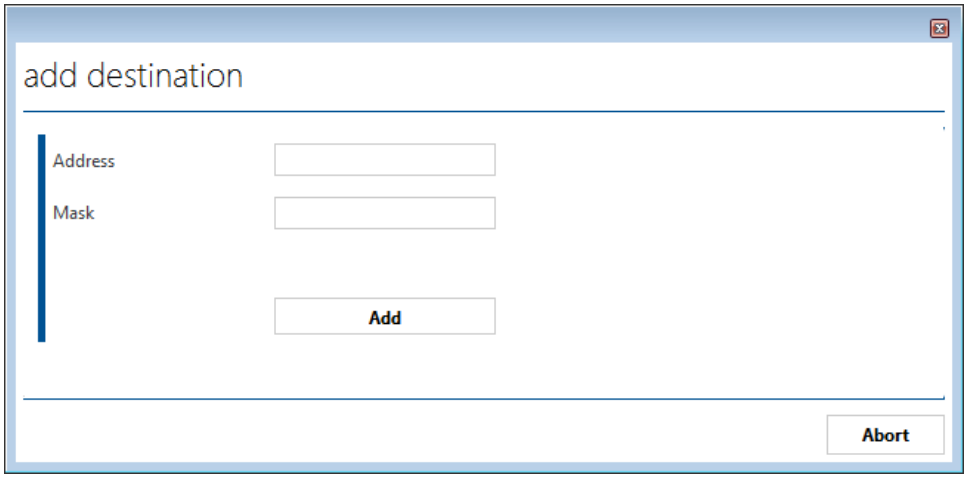


Figure 5-51. Network Destination

5. Enter / Edit the following information:

   Address: Enter the IP address to be added to the list.
   Mask: Enter the subnet mask to be added to the list.

6. *Click Add.*

5.2.6.2.4 Capacity Group Configuration

The Default Capacity Group is listed in the *CAPACITY GROUP* table.

1. To add a new Capacity Group, click the *Add* button under the table.

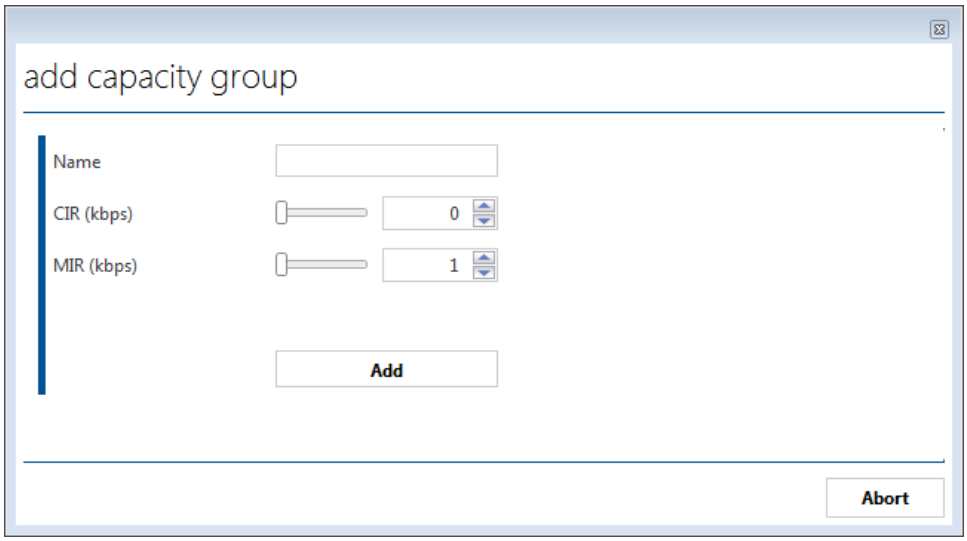


Figure 5-52. Add Capacity Group Page

2. Enter / Edit the following information:

   Name: Enter the name of the new Capacity Group
   CIR (*kbps*): Set the Committed Information Rate (CIR) for the Capacity Group in kbps

   MIR (*kbps*): Set the Maximum Information Rate (MIR) for the Capacity Group in kbps

3. Click *Add* to create the new Capacity Group

At this point, if you click the *Details* button for the desired Capacity Group in the CAPACITY GROUP table, the Capacity Group page opens, where you can edit that Capacity Group and add/delete QoS Groups within that Capacity Group.

To change a parameter, click the pencil icon next to it.

CAPACITY GROUP

Capacity Group Name	Outbound CIR (kbps)	Outbound MIR (kbps)	QoS Mode	QoS Weighted Cost	QoS Capacity Group Delete	QoS Capacity Group Details
Default Capacity...	0 kbps	168000 kbps	Min Max	1	Delete	Details
CG2	1024 kbps	2048 kbps	Min Max	1	Delete	Details

Figure 5-53. Capacity Group Table

5.2.6.2.4.1 QoS Group Configuration

From the Capacity Group page:

1. Click the *Add* button under the *QoS GROUP* TABLE to create a new QoS Group.
2. Enter / Edit the following information:

   Name: The name of the new QoS Group
   CIR (kbps): The Committed Information Rate (CIR) for the QoS Group in kbps
   MIR (kbps): The Maximum Information Rate (MIR) for the Capacity Group in kbps
   Mode: Select either *Off*, *Diff Serv*, *Max Priority*, *Min Max* or *Pri Weighted*
   MODCOD: Select the desired MODCOD
   Pairing ID: Enter a value between 1 and 1024 (0 means disabled).
3. Click *Add* to add the new QoS Group

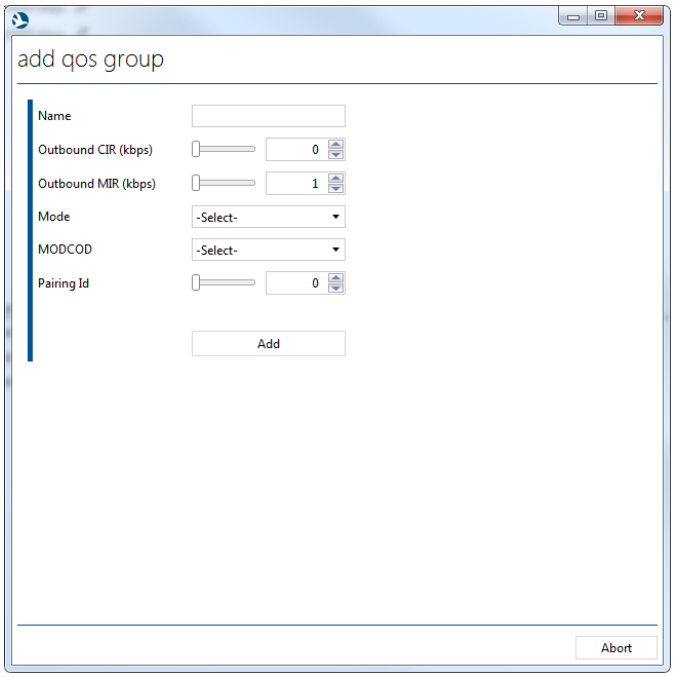


Figure 5-54. Add QoS Group Page

At this point, if you click the *Details* button for the desired QoS Group in the QoS GROUP TABLE, the QoS Group page opens, where you can edit the QoS Group and add or delete remotes, subnets, VLANs and rules.

To change a parameter, click the pencil icon next to it.

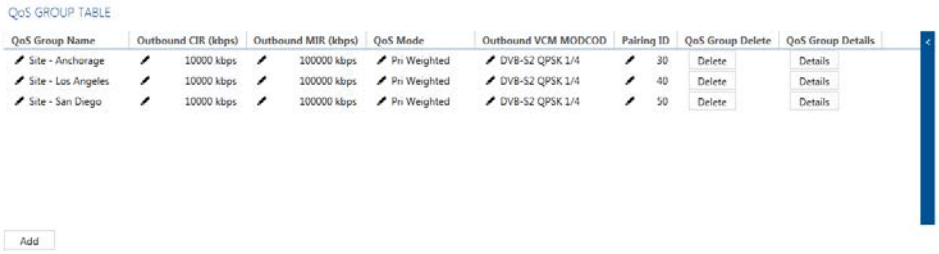


Figure 5-55. QoS Group Table

5.2.6.2.4.2 QoS Group Remote Configuration

From the Capacity Group page:

1. Click the *Details* button next to the QoS Group to be configured.
2. Select *OUTBOUND* at the top of the page to start the outbound QoS Group configuration.

Figure 5-56. QoS Group Configuration

INFO

Under the *INFO* section, you can change any of the previously configured information for the selected QoS Group.

REMOTES

1. To add a remote to the QoS Group, click the *Add* button under the *Remotes* table.

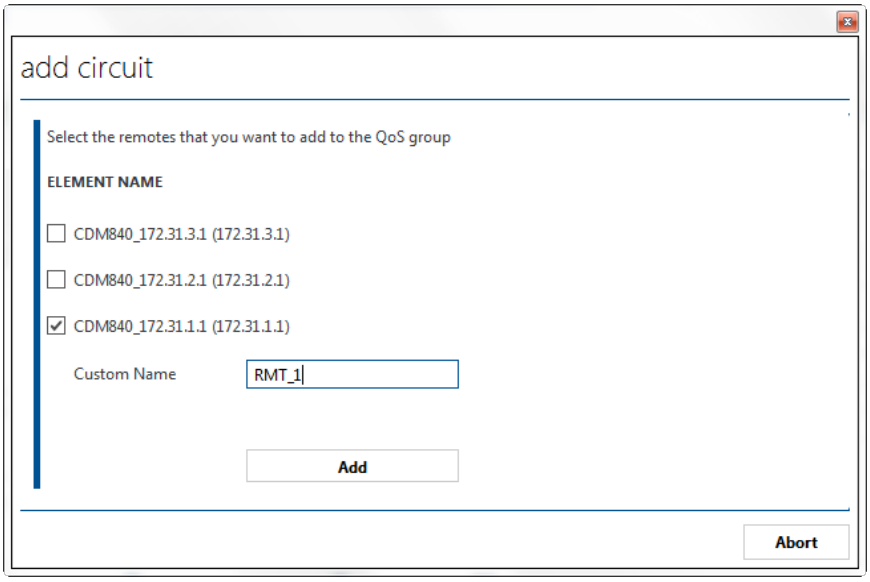


Figure 5-57. Add Circuit Page

2. Enter / Edit the following information:

   Select the remote(s) to be added to the QoS Group.
   Enter a *Custom Name* to label the remote.

3. Click *Add.*

SUBNET

1. To add a subnet to the QoS Group, click the *Add* button under the *SUBNET* table.

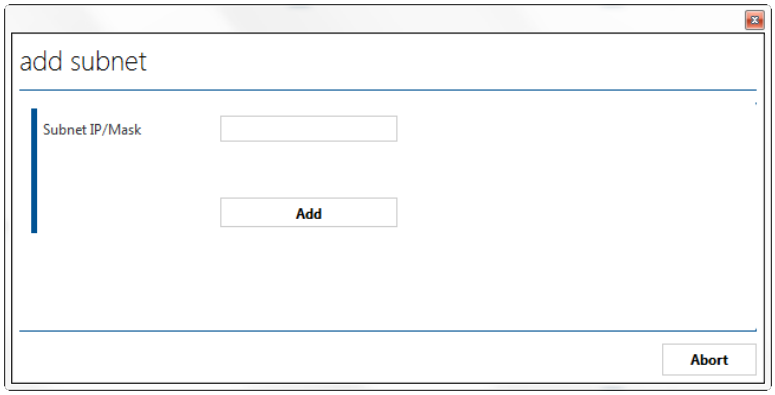


Figure 5-58. Add Subnet Page

2. Enter the *Subnet IP* and *Mask.*
3. Click *Add.*

VLAN

To add a VLAN to the QoS Group:

1. Click the *Add* button under the *VLAN* table.

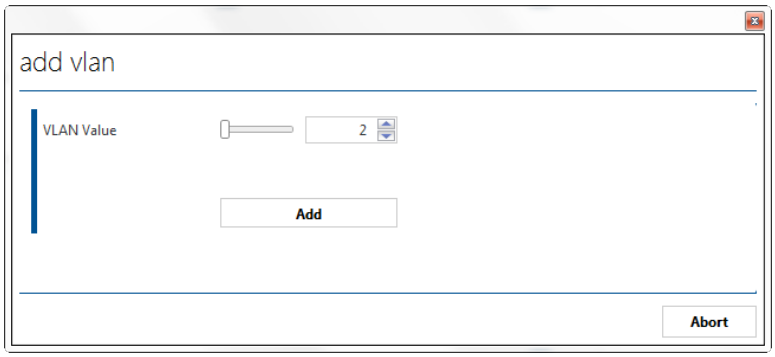


Figure 5-59. Add VLAN Page

2. Enter the *VLAN Value*.
3. Click *Add.*

OUTBOUND QoS RULES

To add a new outbound QoS rule:

1. Click the *Add* button under the *OUTBOUND QoS RULES* table.

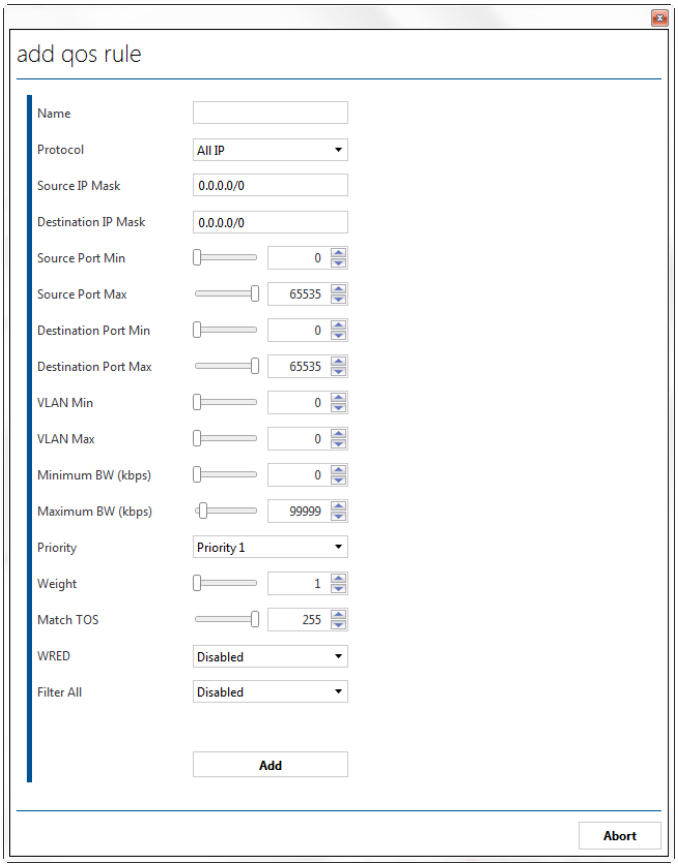


Figure 5-60. Add QoS Rule Page

2. Enter / Edit the following information:

   Name: Enter a name of the QoS rule.
   Protocol: Select the desired protocol.
   Source IP Mask: Enter the source IP address and subnet mask.
   Destination IP Mask: Enter the destination IP address and subnet mask.
   Source Port Min: Enter the minimum source port.
   Source Port Max: Enter the maximum source port.
   Destination Port Min: Enter the minimum destination port.
   Destination Port Max: Enter the maximum destination port.
   VLAN Min: Enter the minimum VLAN value.
   VLAN Max: Enter the maximum VLAN value.
   Minimum BW (kbps): Enter the minimum bandwidth in kbps.
   Maximum BW (kbps): Enter the maximum bandwidth in kbps.
   Priority: Select the priority level for this rule.
   Weight: Enter the weight.
   Match TOS: Select the TOS value to match.
   WRED: *Enable* or *Disable* Weighted Random Early Detection (WRED).

   When WRED is enabled, the QoS Queue attempts to drop packets smoothly as the queue becomes congested. This is recommended for queues that will carry TCP packets.

   Filter All: *Enable* or *Disable* the flow filter.

   Click *Add* to add the new rule.

INBOUND

Select *INBOUND* at the top of the page to start the inbound QoS Group configuration.

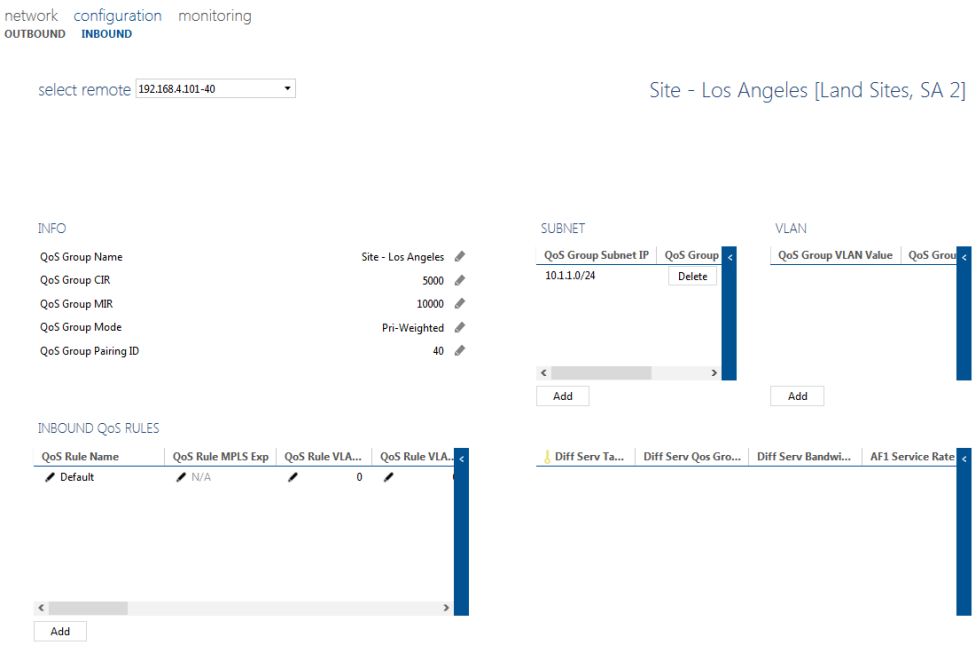


Figure 5-61. Inbound QoS Page

INFO

In the *INFO* section, you can change any of the previously configured information for the selected QoS Group.

INBOUND QoS RULES

In the *INBOUND QoS RULES* section, you can change any of the previously configured QoS rules.

To create a new QoS rule:

1. Click the *Add* button under the *INBOUND QoS RULES* table.

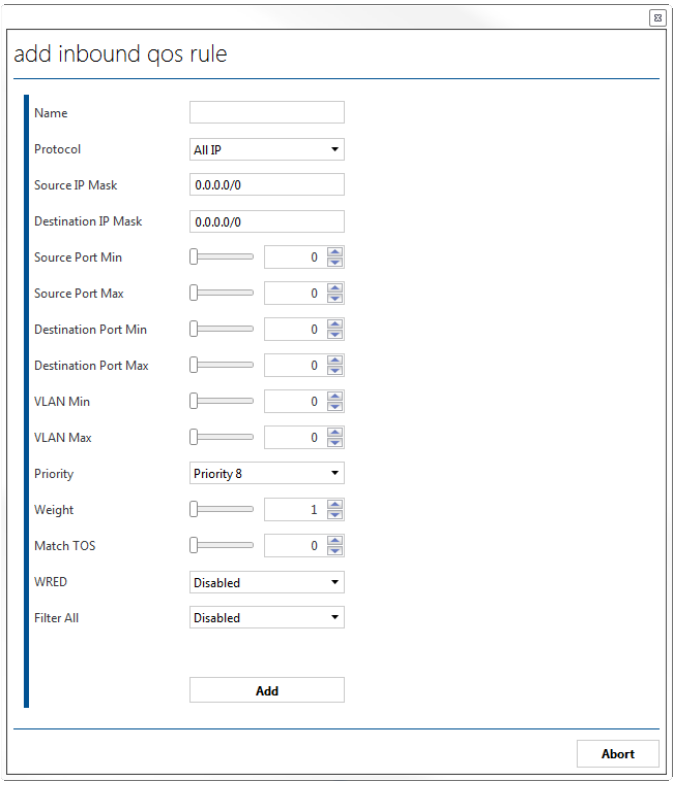


Figure 5-62. Add Inbound QoS Rule

2. Enter / Edit the following information:

   Name: Enter a name of the QoS rule.
   Protocol: Select the desired protocol.
   Source IP Mask: Enter the source IP address and subnet mask.
   Destination IP Mask: Enter the destination IP address and subnet mask.
   Source Port Min: Enter the minimum source port.
   Source Port Max: Enter the maximum source port.
   Destination Port Min: Enter the minimum destination port.
   Destination Port Max: Enter the maximum destination port.
   VLAN Min: Enter the minimum VLAN value.
   VLAN Max: Enter the maximum VLAN value.
   Minimum BW (kbps): Enter the minimum bandwidth in kbps.
   Maximum BW (kbps): Enter the maximum bandwidth in kbps.
   Priority: Select the priority level for this rule.
   Weight: Enter the weight.
   Match TOS: Select the TOS value to match.
   WRED: *Enable* or *Disable* Weighted Random Early Detection (WRED).

   When WRED is enabled, the QoS Queue attempts to drop packets smoothly as the queue becomes congested. This is recommended for queues that will carry TCP packets.

   Filter All: *Enable* or *Disable* the flow filter.

3. Click *Add* to add the new rule.

SUBNET

To add a subnet to the Inbound QoS Group:

1. Click the *Add* button under the *SUBNET* table.

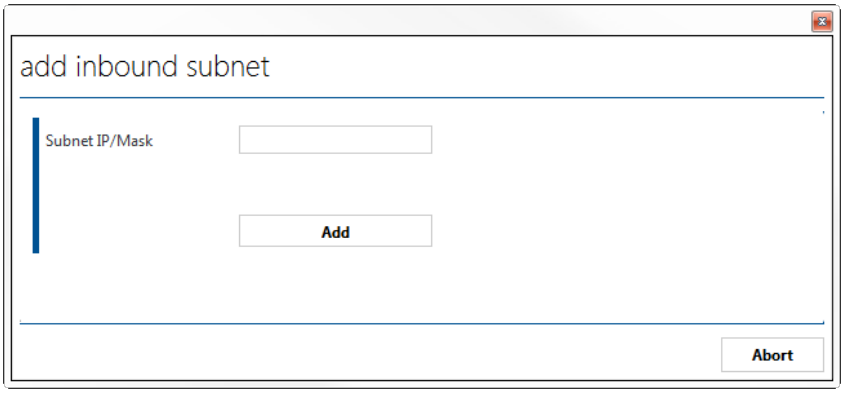


Figure 5-63. Add Inbound Subnet Page

2. Enter the **Subnet IP** and **Mask.**
3. Click *Add.*

VLAN

To add a VLAN to the Inbound QoS Group:

1. Click the *Add* button under the *VLAN* table.

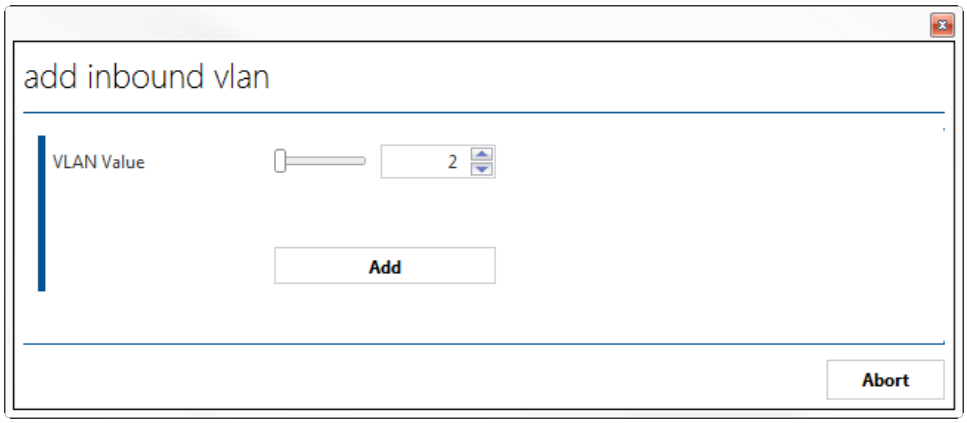


Figure 5-64. Add Inbound VLAN Page

2. Enter the **VLAN** *Value*.
3. Click *Add.*

5.3 Manual Provisioning

Manual provisioning is used when creating point-to-point circuits that will not be used by the CEFD Bandwidth Manager.

For more information, see the NetVue Provisioning Guide.

Chapter 6. NetVue Cube Security

6.1 Introduction

NetVue has a standard, fully integrated security module that lets you configure which users have access to what parts of the system. You can manage users with user profiles to define which actions they can perform, and keep a detailed log of all user activity.

Go to the system center to see the user interface:

Click Start **>** Apps **>** System Center

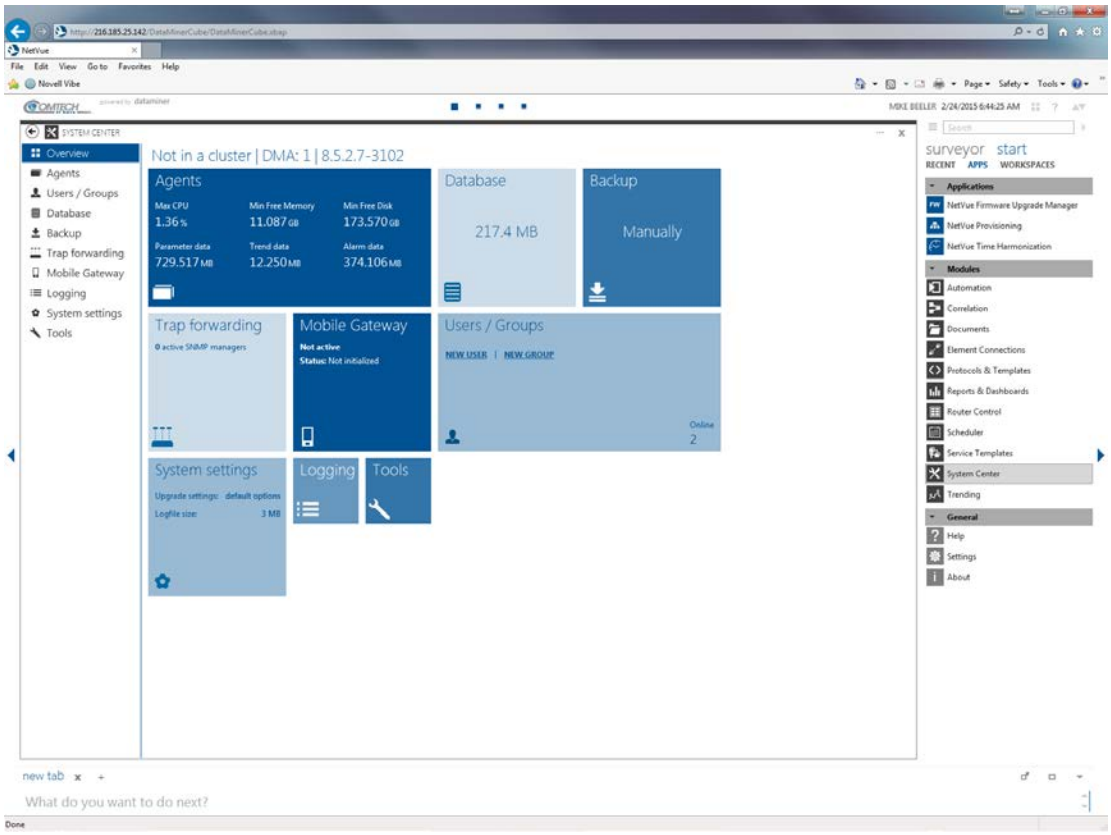


Figure 6-1. System Center

6.2 User Identification

Users must identify themselves with a unique user name and password.

NetVue supports two methods for user identification.

1. Autonomous User Identification:
   A NetVue Server Administrator defines Users within the NetVue System.
2. Domain:
   Users are defined in the corporate network domain, and are integrated transparently into the NetVue Server, after the server is added to the domain.

When the NetVue System is configured to integrate domain users, the NetVue client applications will log on to the NetVue Server automatically, with the user's Windows user account.

NetVue Server Security is tightly integrated with Microsoft Windows security. Even when the NetVue Server uses Autonomous User Identification, the users you create in NetVue are created automatically in the Windows operating system. This means that users who are authorized to access the NetVue Server will be automatically allowed to access the NetVue Server via the Windows operating system.

6.3 User Rights

After identification, users have access to the NetVue System according to the user rights they have been granted.

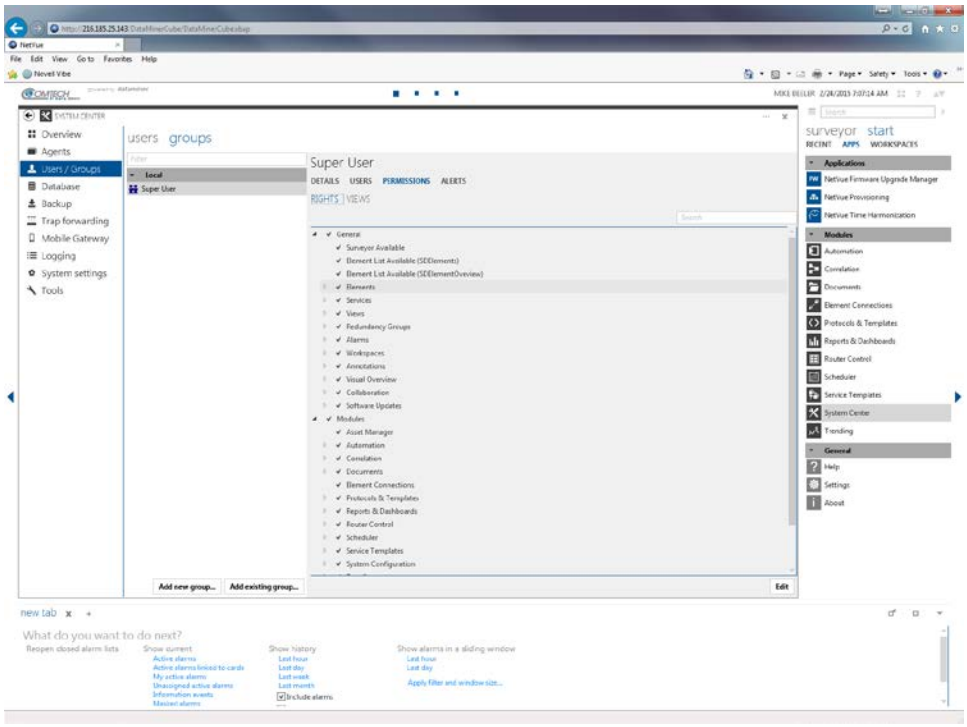


Figure 6-2. User Rights - Permissions

Three concepts control how rights are granted:

1. Permissions:

   Users' permissions to specific **actions** in the NetVue Server is based on the configuration of their user group. Examples of actions include: add elements, edit alarm templates, etc.

2. Views:

   Users' access to specific **items** in NetVue is based on their user group. In System Display, you can configure this only on the view level. In Cube, however, you can configure access rights for the items contained within views also.

3. Access levels:

   You can assign **access levels** to users and to individual parameters. Access levels range from 1 (highest level) to 5 (lowest level).

   A user can set a parameter only when its access level is equal to or lower than the user's access level. Example: A user with access level 3 can update parameters with access level 3, 4 and 5.

6.4 User Groups

NetVue users are part of one or more groups. Groups can have rights according to three concepts: permissions, views and access levels.

Users in those groups inherit the rights granted to their groups. You can also configure User settings at the group level.

Optionally, a user who is a member of a group can have a personal access level. A personal access level overrides the access level granted to the group.

There are two types of groups:

1. Local groups:
   Proprietary user groups, created and managed in NetVue
2. Domain groups:
   User groups available in the Windows domain, managed by the domain administrator

6.5 Types of Users

NetVue has three types of users:

1. Local users:
   - Proprietary users, known only to the local operating system of the NetVue Agents
   - Managed entirely by NetVue
   - Used mostly when the NetVue Servers have not been added to a domain
2. Manually added domain users:
   - For domain users, the user name and password are managed by the domain
   - All other properties are managed by NetVue
   - Used mostly when the NetVue Servers have been added to a domain on which the NetVue administrators do not have permission to change domain group memberships or update domain user properties
3. Automatically added domain users:
   - Domain users that are added automatically when a domain group is added to NetVue
   - Managed entirely by the domain
   - Used mostly when the NetVue Servers have been added to a domain on which the NetVue administrators do have permission to change domain group memberships and update domain user properties

6.5.1 Important Considerations for Domain Group Users

When a domain group is added to NetVue, the domain level email address, mobile number and pager number override those of the existing, manually added domain users.

When you delete a domain group from NetVue, all users in that domain group are deleted also, even if they are members of one or more proprietary NetVue groups. However, if they are members of at least one other domain group, they are not deleted.

6.6 Configure Security in System Center

Most security settings for users or user groups are configured in the System Center app.

To find these settings:

1. Go to **Start ‣ Apps ‣ System Center**
2. In the System Center overview, click the **Users/Groups** field
3. The **Users/Groups** section opens, with two tabs: **Users** and **Groups**

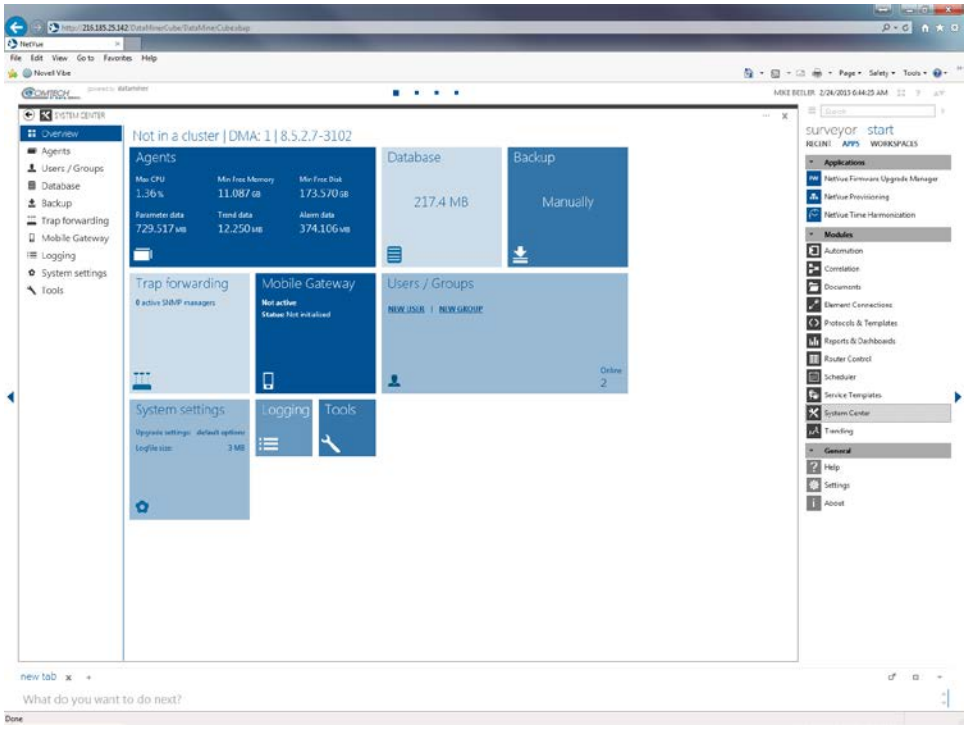


Figure 6-3. System Center

6.6.1 Opening a User Card

You can configure security settings for a single user on a user card.

To open a user card:

1. Search for a user by name in the navigation pane
2. Click the user record for that user

Next to the user name, the card shows whether the user is **online** or **offline**

To open your own user card, click your user name in the header bar and select My account.

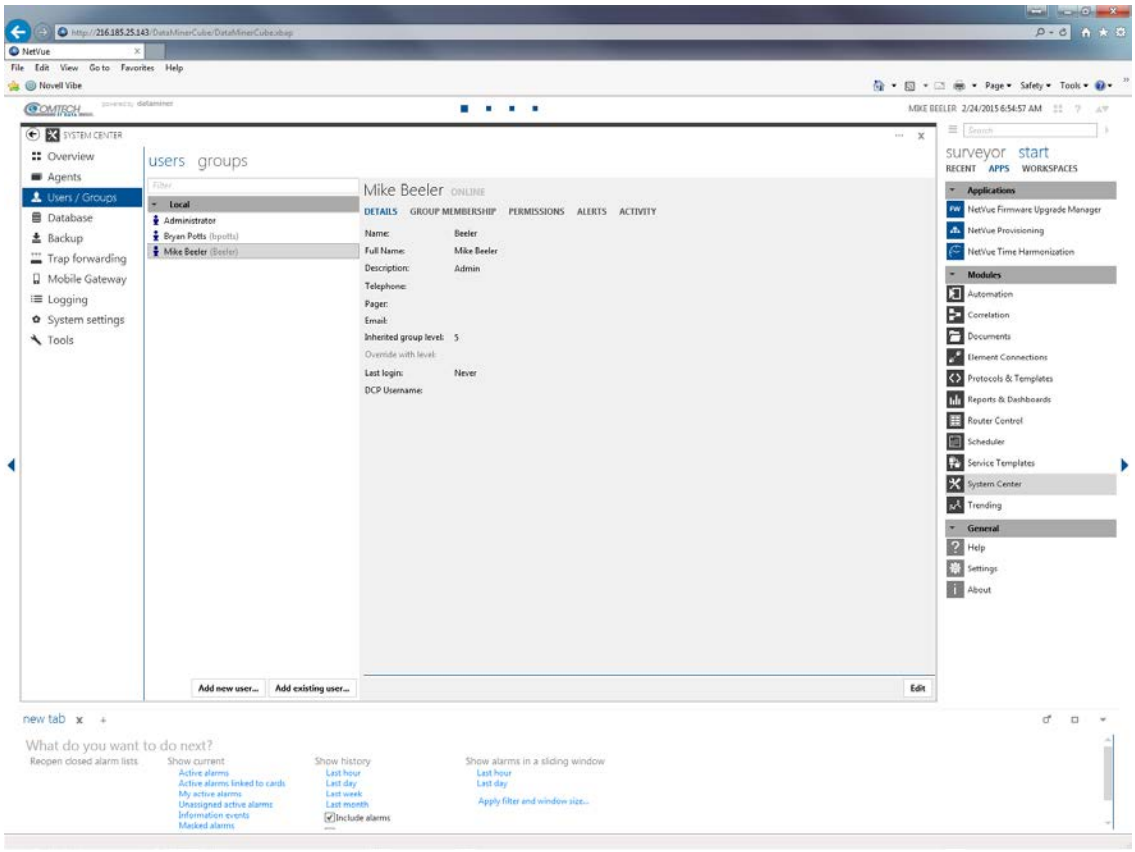


Figure 6-4. User Information/Configuration

6.6.2 Add a New User

There are two ways to add a new user to a NetVue Server in Cube. These differ, depending on whether the user is a local user or a domain user.

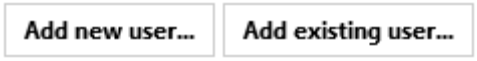


Figure 6-5. Add User or Add Existing User

6.6.2.1 Add a Local User

1. In the **Users / Groups** section of the System Center app, go to the **users** tab.
2. At the bottom of the list of users, click **Add new user**.
3. In the **Add new user** window, add the user's information:
   - Fill in the required fields **Name**, **Password** and **Confirm password**.
   - Fill in the **Telephone** field, so the user can receive text messages.

     Add telephone numbers in international format, starting with a "+" sign.
   - Fill in the **Email** field, so the user can receive email notifications or automated email messages.
   - Fill in the **Level** field, to set the user's security level if it is different from the user's group security level. Access levels range from 1 (highest level) to 5 (lowest level).
     - To require the user to change the password the next time they log on to the NetVue Server, select **User must change password at next login**.
     - To prevent the password from being changed, select **User cannot change password**.
     - To make sure that the password does not expire, select **Password never expires**.
4. To add another user, click **Add another**.
5. Otherwise, click **Add**.

The new user(s) are added to the list of **Local** users.

6.6.2.2 Add an Existing Domain User

1. In the **Users / Groups** section of the System Center app, go to the **users** tab.
2. At the bottom of the list of users, click **Add existing user**.
3. In the **Add existing user** window, select the user(s) you want to add and click **OK**.

   The new users are added to the list of **Domain** users.

   Some properties of domain users cannot be changed in NetVue. Examples include: name, password, etc.

   These users are marked by a gray user icon in the user list to show that domain users are read-only.

6.6.3 Delete a User

To delete a user from the NetVue Server:

1. In the **Users / Groups** section of the System Center app, go to the **users** tab.
2. Right-click the user in the **Local** or **Domain** list and select **Delete**.
3. In the confirmation window, click **OK**.

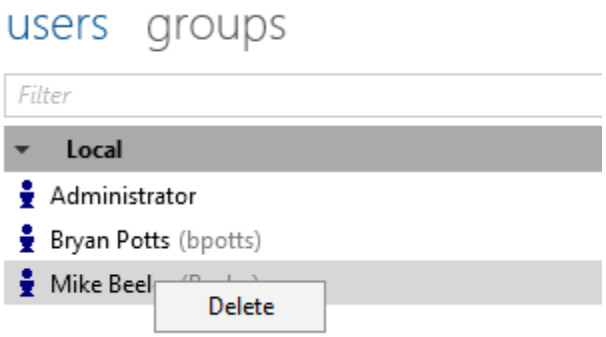


Figure 6-6. Delete User

6.6.3.1 Important Considerations when Deleting Users

When you delete a local user, the associated Windows user account is removed from the NetVue Agents.

When you delete a manually added domain user, only the reference to that user is removed from the NetVue System.

An automatically added domain user cannot be deleted. To remove such users, you must remove them from the domain group.

6.6.4 View User Information

To see detailed information on a user in NetVue Cube:

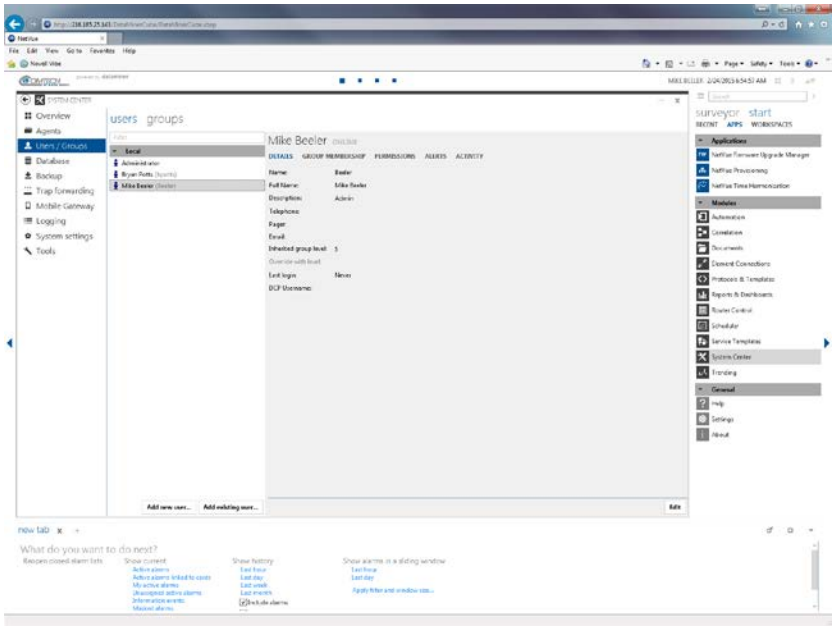


Figure 6-7. Detailed User Information

1. In the **Users / Groups** section of the System Center app, go to the **users** tab.
2. Select the user whose information you want to see.
3. In the details pane on the right:
   - Check the **Details** tab to see the user's contact details, security level, DCP username and last login.
   - Check the **Group membership** tab to see which group(s) have the user as a member.
   - Check the **Permissions** tab to see which permissions have been set for the user.

User permissions are inherited from the user group. They cannot be edited separately for a group member.

4. Check the **Alerts** tab to see which notifications have been set up for the user.

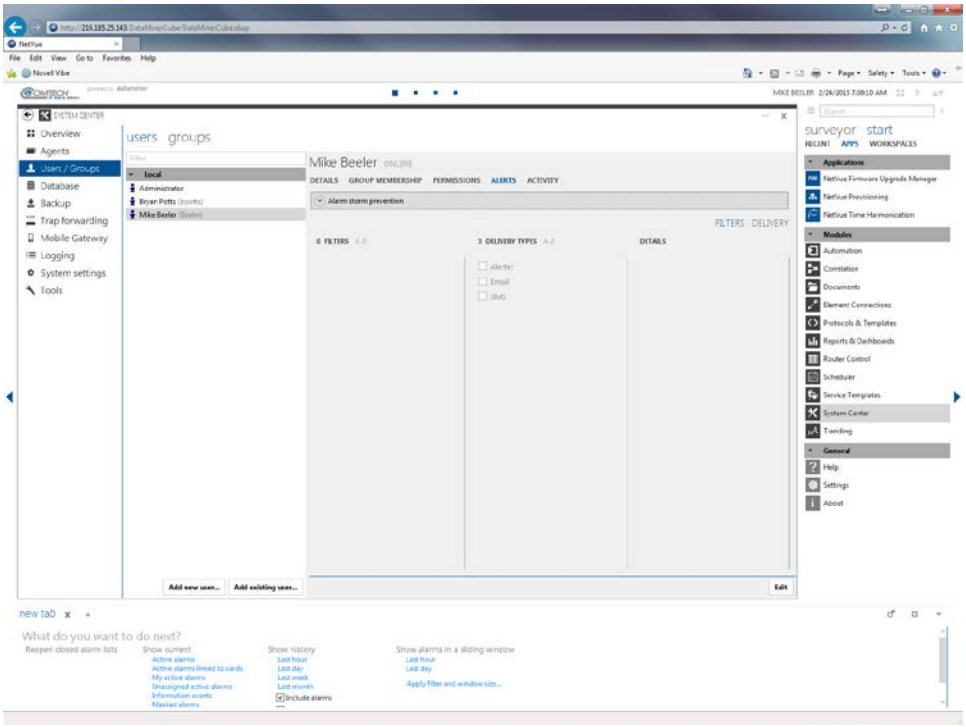


Figure 6-8. Alerts

5. Check the **Activity** tab to see a log of the user's recent activity. This tab consists of two pages:
    - The **Recent sessions** page shows when the user has recently logged on, and what client application was used.
    - The **Actions** page shows a detailed overview of all recent activity by the user on the NetVue Server.

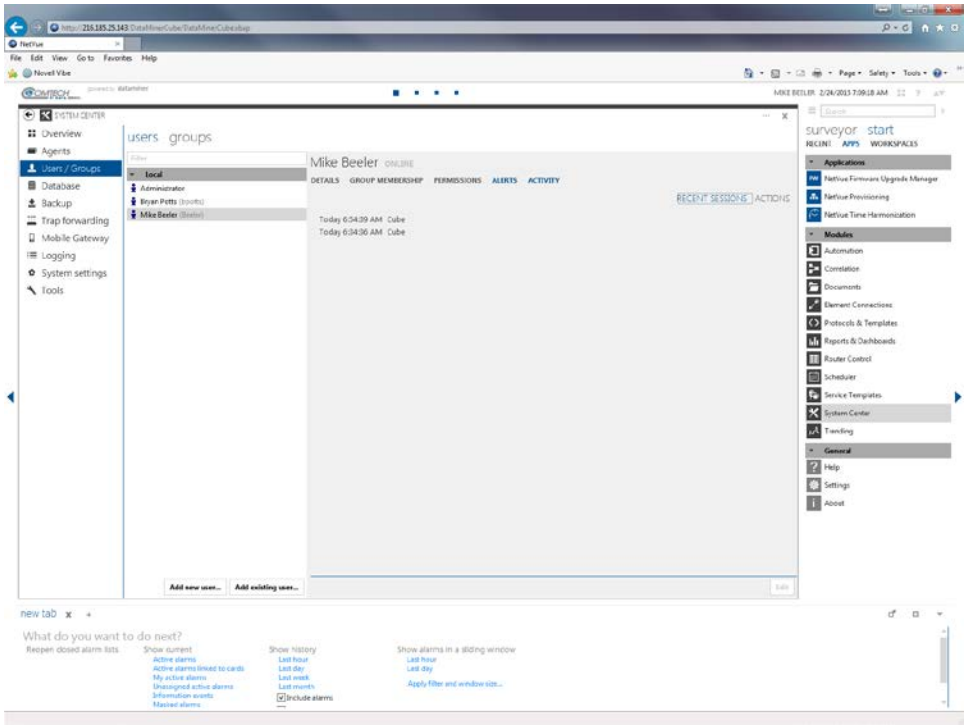


Figure 6-9. Activity

6.6.5 Edit User Details

To edit a user's details in NetVue Cube:

1. In the **Users / Groups** section of the System Center app, go to the **users** tab.
2. Select the user whose information you want to edit.
3. Alternatively, you can also open the user card for the user in question.
    - In the bottom right corner of the **details** tab, click the **Edit** button.
4. Fill in the new data in the applicable fields. For example, if you want to change a user's DCP login credentials, fill in **DCP Username** and **DCP Password**.
5. Click the **Apply** button in the bottom right corner.

6.6.6 Change a Users Group Membership

1. In the **Users / Groups** section of the System Center app, go to the **users** tab.
2. Select the applicable user.
3. Alternatively, you can also open the user card for the user in question.
    - Go to the **Group membership** tab.
    - Click the **Edit** button in the bottom right corner.

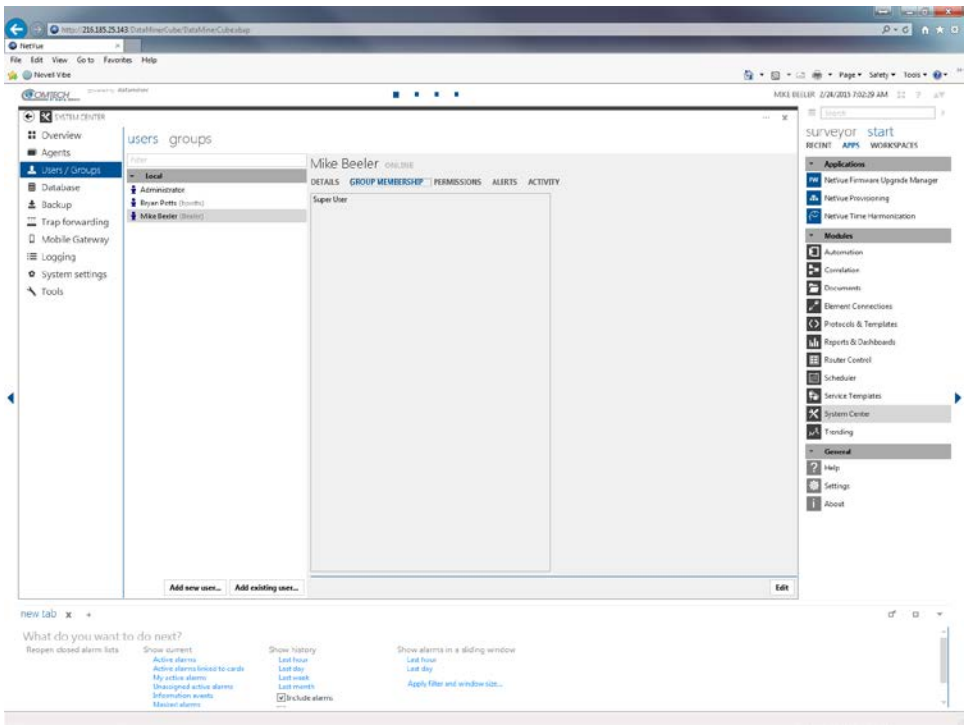


Figure 6-10. Group Membership

4. Use the **ADD >>** and **<< REMOVE** buttons to move different groups to or from the **Available groups** and **Included in groups** columns.
5. Click the **Apply** button.

In NetVue, you cannot add users to domain groups. Manage membership of domain groups on the domain.

6.6.7 Disconnect a User

In NetVue Cube, users who have the permission “Disconnect Other Users” can disconnect other users from a NetVue Agent.

1. Click the current user in the top-right corner of the screen to open the user console.
2. In the **Contacts** list, right-click the user you want to disconnect.
3. In the shortcut menu that lists all current client sessions of the selected user, choose to disconnect either one specific session or all sessions of the applicable user.
4. In the **Motivation** box, enter the reason why you want to disconnect the selected user session(s).
5. Click OK.

6.7 Notifications

You can configure notifications, so that when an alarm occurs for a specific alarm filter, a user receives a notification.

Configure notifications in the System Center. For personal notifications only, configure notifications directly from the Alarm Console or the Surveyor.

6.7.1 Configure Notifications in System Center

To configure notifications in System Center:

1. Go to **Start ‣ Apps ‣ System Center ‣ Users / Groups**
2. In the **users** tab, go to the **Alerts** subtab.
3. Click the **Edit** button in the bottom right corner.
4. Right-click in the **Filters** column to add a filter:
5. To add an existing alarm filter, in the right-click menu, select **Add filter**, and then select the applicable filter.
6. To add a new alarm filter, in the right-click menu, select **Create new filter**.
    - Add a name, type, and description for the filter.
    - Configure the filter.
    - Click **OK**.

    In the* Details *column of the Alerts tab, the description of the selected alarm filter is shown.

7. To combine several filters, repeat step 4 until all the necessary filters have been added.
8. In the **Delivery types** column, select one or more notification types: **Alerter**, **Email** or **SMS** (text message).
9. Click the **Apply** button.

6.7.2 Configure Notifications Directly from the Alarm Console or Surveyor

To configure an alarm filter for personal notifications directly from the Alarm Console or the Surveyor:

1. Right-click an alarm in the Alarm Console or right-click an element, service or view in the Surveyor.
2. Select **Actions ‣ Alert me**.
3. Your user card will open on the **Alerts** tab, where a filter is suggested:
   - Modify the suggested filter if necessary, and click **OK**.
4. In the **Delivery types** column, select one or more notification types: **Alerter**, **Email** or **SMS** (text message).
5. Click the **Apply** button.

6.7.2.1 Additional Information about Notifications

Notification filters are server-side filters. In Alerter, notification filters are added to the list of server-side filters.

You can configure User notifications on a user card, also. You can configure Notifications at the group level as well.

6.8 User Group Management

All functionalities for user group management in Cube are found in the **Users / Groups** section of the System Center app.

6.8.1 View Information about User Groups

To see information about an existing user group in NetVue Cube:

1. In the **Users / Groups** section of the System Center app, go to the **Groups** tab.
2. Select the applicable group from the **Local** or **Domain** list, depending on the type of group.
3. In the pane on the right:
   - Check the **Details** tab to see the group's name and security level.
   - Check the **Users** tab to see the list of users who are a member of the group.
   - Check the **Permissions** tab to see views the group has access to and the rights that have been configured for it.

6.8.2 Add a User Group

There are two ways to add a new user group to a NetVue Server in Cube, depending on whether it is a local group or a domain group.

6.8.2.1 Add a Local Group

1. In the **Users / Groups** section of the System Center app, go to the **groups** tab.
2. Click **Add new group**.

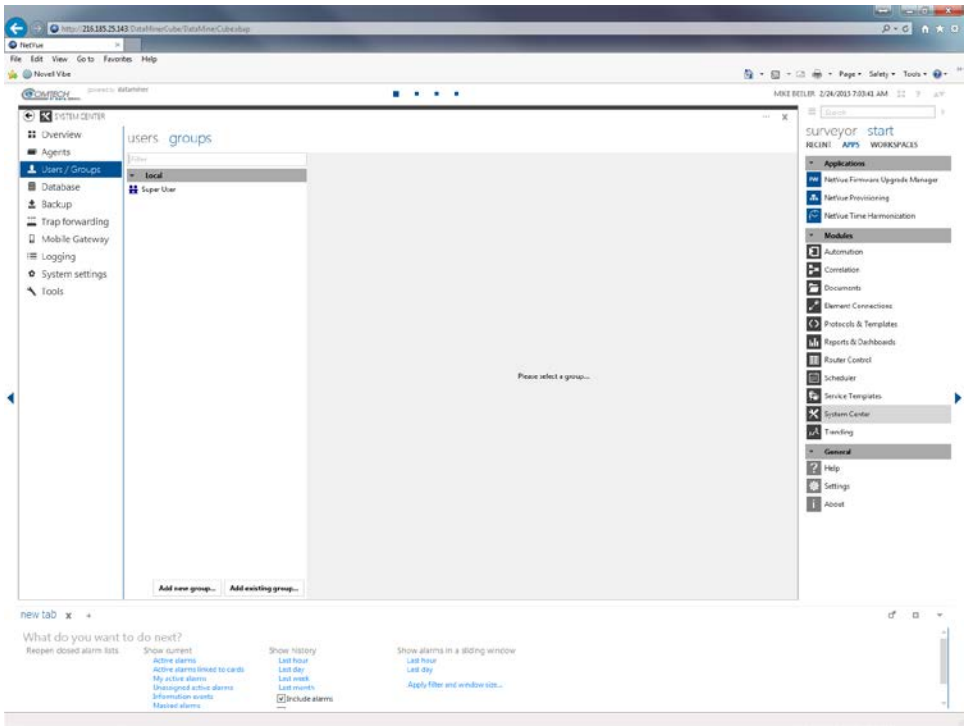


Figure 6-11. Groups

The new group is added to the list of **Local** groups.

6.8.2.2 Add an Existing Domain Group

1. In the **Users / Groups** section of the System Center app, go to the **groups** tab.
2. Click **Add existing group**.
3. In the **Add existing group** window, select the group(s) you want to add.
4. Click **OK**.

The new groups are added to the list of **Domain** groups.

6.8.2.3 Additional Information about Adding Domain Groups

- All members of the domain group are added to NetVue automatically.
- If changes are made to the domain group outside of NetVue (e.g. users are added or deleted), NetVue will update its security settings automatically.
- Some properties of domain users (e.g. name, password) cannot be changed in NetVue. To show that domain users are read-only, these users are marked by a gray user icon in the user list.

6.8.3 Configure a User Group

To configure a user group:

1. In the **Users / Groups** section of the System Center app:
   a. Go to the **Groups** tab.
   b. Select the applicable group.
2. Click the **Edit** button in the bottom right corner.
3. To change the group name, fill in the new name in the **Name** field of the **Details** tab.
4. To change the group's security level, enter a new level in the **Group level** field on the **Details** tab. Access levels range from 1 (highest level) to 5 (lowest level).
5. To change which users are members of the group, go to the **Users** tab:

   Move users to and from the **Available users** and **Included users** columns using the **ADD >>** and **<< REMOVE** buttons.
6. To set which views, elements and services a user has access to, go to the **Permissions** tab:
   a. Select the **Views** subtab.
   b. Select the applicable check boxes.

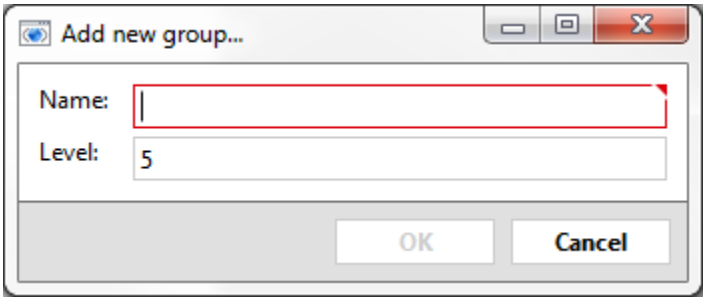


Figure 6-12. Add New Group

For each item, there are three check boxes for setting rights:

- Read access
- Write access
- Configuration rights

For CPE elements, you can configure access for objects on the lower topology levels as well.

7. To change the user permissions for a group:
    a. Go to the **Permissions** tab.
    b. Select the **Rights** subtab.
    c. Select the applicable check boxes.
8. To configure configurations for the group:
    a. Go to the **Alerts** tab.
    b. Do the same steps as for alerts for a single user.

    Unlike alerts for a single user, alerts for a group cannot be sent with Alerter.

9. Click **Apply**.

6.8.4 Delete a User Group

To delete a user group from the NetVue Server:

1. In the **Users / Groups** section of the System Center app, go to the **groups** tab.
2. Right-click the group in the **Local** or **Domain** list.
3. Select **Delete**.
4. In the confirmation window, click **OK**.

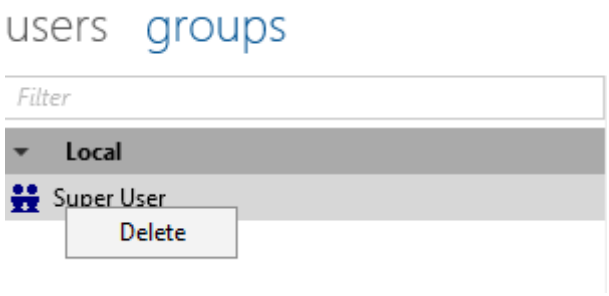


Figure 6-13. Delete User Group

6.9 About User Permissions

To find a specific user permission quickly, use the filter box in the top right corner of the list of permissions.

In the System Center app, the user permissions are divided into three main groups: General, Modules and Other. An overview of the different permissions follows.

6.9.1 General

6.9.1.1 Surveyor Available

Cube Permission	SD Permission	Description
Surveyor Available	Surveyor Access	Permission to access the Surveyor.

6.9.1.2 Element List Available

Cube Permission	SD Permission	Description
Element List Available (SDElements)	SD Administration: Elements	Permission to access the Admin ‣ Elements page of System Display.
Element List Available (SDElementsOverview)	SD System Overview: Elements Overview	Permission to access the View ‣ Element Overview page of System Display.

6.9.1.3 Elements

Cube Permission	SD Permission	Description
Access	Element Display/Card: Access	Permission to access Element Display or element cards.
Add	Element: Creating	Permission to create elements.
Edit	Element: Editing	Permission to update elements.
Delete	Element: Deleting	Permission to delete elements.
Import	Element: Import	Permission to import elements from CSV files.
Properties > Add	Element: Create Properties	Permission to create element properties.
Properties > Edit	Element: Change Property values	Permission to change the value of element properties.
Properties > Delete	Element: Delete Properties	Permission to delete element properties.
Lock/Unlock	Element: (Un)Lock	Permission to lock and unlock an element.
Force Unlock	Element: Force Unlock	Permission to unlock an element that has been locked by another user.

Cube Permission	SD Permission	Description
Start	Element: Starting	Permission to start elements.
Stop	Element: Stopping	Permission to stop elements.
Pause	Element: Pausing	Permission to pause elements.
Mask until clearance / for x time	Element: Masking until clearance/for x time	Permission to mask elements until they are cleared or for a specific time.
Mask until unmasking	Element: Masking until unmasking	Permission to mask elements until they are unmasked.

6.9.1.4 Elements > Element Display

Cube Permission	SD Permission	Description
DataDisplay: Access	Data Display: Access	Permission to access the Data Display side of an element card.
DataDisplay: View Write Parameters	Data Display: Viewing Write Parameters	Permission to view write parameters in Data Display.
Configure matrix options	Matrix options: Change	Permission to configure a matrix parameter.
Spectrum > Configure measurement points	Spectrum: Configure Measurement Points	Permission to configure measurements points for a Spectrum Analyzer Element.
Spectrum > Configure scripts & monitors	Spectrum: Configure Scripts & Monitors	Permission to manage spectrum scripts and spectrum monitors.
Spectrum > Edit / delete protected presets	Spectrum: Edit/Delete Protected Presets	Permission to update and delete protected spectrum analyzer presets.
Spectrum > Take device from other client	Spectrum: Take Device From Other Client	Permission to terminate a spectrum client sessions of another user in order to start a session yourself, in case the maximum number of concurrent client sessions is limited.
Spectrum > Take priority over monitors	Spectrum: Take Priority Over Monitors	Permission to temporarily take priority over spectrum monitors.

6.9.1.5 Services

Cube Permission	SD Permission	Description
Add	Service: Add	Permission to create services.
Edit	Service: Edit	Permission to edit services.
Delete	Service: Remove	Permission to delete services.
Properties > Add	Service: Create Properties	Permission to create service properties.
Properties > Edit	Service: Change Property values	Permission to change the value of service properties.
Properties > Delete	Service: Delete Properties	Permission to delete service properties.

6.9.1.6 Views

Cube Permission	SD Permission	Description
UI Available (SDViews)	SD Administration: Views	Permission to access the Admin ‣ **Views** page of System Display.
UI Available (SDVisualOverview)	SD System Overview: Visual Overview	Permission to access the View ‣ **Visual Overview** page of System Display.
Add / remove elements	Views: Adding/Deleting Elements	Permission to add and remove elements and services to and from views.
Add / remove views	Views: Adding/Deleting Views	Permission to add and remove views.
Assign Visio drawings	Views: Allocating Vdx-file	Permission to link Visio files to views.
Properties > Add	Views: Create Properties	Permission to create view properties.
Properties > Edit	Views: Change Property values	Permission to change the value of view properties.
Properties > Delete	Views: Delete Properties	Permission to delete view properties.

6.9.1.7 Redundancy Groups

Cube Permission	SD Permission	Description
Add	Redundancy groups: Add	Permission to create redundancy groups.
Edit	Redundancy groups: Edit	Permission to update redundancy groups.
Delete	Redundancy groups: Remove	Permission to delete redundancy groups.
Advanced > Change RG mode	Redundancy groups: Change redundancy mode	Permission to change the redundancy mode (automatic, manual, manual switchback) of a redundancy group (software redundancy only).
Advanced > Manual switch	Redundancy groups: manual Switch(Sw. now)	Permission to initiate a manual switch-over (software redundancy only).
Advanced > Set element in maintenance	Redundancy groups: Set element in maint.	Permission to set an element in maintenance.
Advanced > Configure elements in RG template	Redundancy Templates: Conf RG Elements	Permission to configure the elements in a redundancy group that was created as a redundancy group template.

6.9.1.8 Alarms

Cube Permission	SD Permission	Description
Alarm Console Available	AlarmConsole Access	Permission to access the Alarm Console.
Allow masking	Alarm: Masking	Permission to mask alarms.
Allow unmasking	Alarm: UnMasking	Permission to unmask alarms.
Allow unmasking element	Element: Unmasking	Permission to unmask elements.
Allow take & release ownership	Alarm: Take/Release Ownership	Permission to take ownership of alarms and to release that ownership.
Allow force release ownership (other user)	Alarm: Release Ownership of another user	Permission to release ownership of alarms owned by other users.
Allow viewing of system events	Alarm: View System Events	Permission to view system events in the Alarm Console
Extended context menu Alarm Console	AlarmConsole: Full Menu	Permission to access the Alarm Console shortcut menu.
Extended view menu Alarm Console	AlarmConsole: View SubMenu	Permission to access the View submenu of the Alarm Console shortcut menu.
Edit / delete protected files	Filters: Edit/Delete Protected Filters	Permission to update and/or delete protected filters.
Properties > Add	Alarm: Create Properties	Permission to add properties to alarms.
Properties > Edit	Alarm: Change Property values	Permission to change the value of alarm properties.

Cube Permission	SD Permission	Description
Properties > Delete	Alarm: Delete Properties	Permission to delete properties from alarms.

6.9.1.9 Workspaces

Cube Permission	SD Permission	Description
Add	Cube Workspace: Create	Permission to create workspaces in NetVue Cube.
Delete	Cube Workspace: Delete	Permission to delete workspaces in NetVue Cube.

6.9.1.10 Annotations

Cube Permission	SD Permission	Description
View	Annotations: View	Permission to view annotations.
Edit	Annotations: Edit	Permission to add and update annotations.

6.9.1.11 Visual Overview

Cube Permission	SD Permission	Description
Advanced navigation	Visual Overview: Advanced Navigation	Permission to navigate from one Visual Overview to another by clicking shapes that act as hyperlinks.
Download Visio drawings	Visual Overview: Download Drawings	Permission to download a Visio file from the NetVue System to the client computer.
Edit Visio drawings	Visual Overview: Edit Drawings	Permission to change Visio files using the embedded Visio file editor.

6.9.1.12 Collaboration

Cube Permission	SD Permission	Description
UI Available	Collaboration Access	Permission to start chat sessions.
Disconnect other users	Collaboration: Disconnect other users	Permission to end chat sessions of other users.

6.9.1.13 Software Updates

Cube Permission	SD Permission	Description
Download software updates from DCP	DCP: Download Software	Permission to download software from the NetVue Collaboration Platform.

If you upgrade NetVue from a version lower than 8.0.6, both this security permission and the permission Download protocols from DCP are enabled automatically for existing groups.

6.9.2 Modules

6.9.2.1 Asset Manager

Cube Permission	SD Permission	Description
Asset Manager	Asset Manager	Permission to use the Asset Manager app.

6.9.2.2 Automation

Cube Permission	SD Permission	Description
UI Available	SD Tools: Automation	Permission to access the NetVue Server Automation module.
Add	Automation: Create Scripts	Permission to create Automation scripts.
Edit	Automation: Edit Scripts	Permission to update Automation scripts.
Delete	Automation: Delete Scripts	Permission to delete Automation scripts.
Execute	Automation: Execute Scripts	Permission to execute Automation scripts.

6.9.2.3 Correlation

Cube Permission	SD Permission	Description
UI Available	SD Tools: Correlation	Permission to access the NetVue Server Correlation module.
Add	Correlation: Add Rules	Permission to create Correlation rules.
Edit	Correlation: Edit Rules	Permission to update Correlation rules.
Delete	Correlation: Delete Rules	Permission to delete Correlation rules.

6.9.2.4 Documents

Cube Permission	SD Permission	Description
UI Available	SD System Overview: Doc Overview	Permission to access the NetVue Documents user interface.
Add	Document: Adding	Permission to upload documents.
Edit	Document: Changing Type/Description	Permission to change the title of an uploaded document as well as the comments that are linked to it.
Delete	Document: Deleting	Permission to delete uploaded documents.

6.9.2.5 Element Connections

Cube Permission	SD Permission	Description
Element Connections	Element Connections	Permission to use view and configure element connections

6.9.2.6 Protocols & Templates > Protocols

Cube Permission	SD Permission	Description
UI Available	SD Administration: Protocols	Permission to access the NetVue protocols user interface.
Add	Protocol: Adding	Permission to add NetVue protocols.
Edit	Protocol: Editing	Permission to edit NetVue protocols.
Delete	Protocol: Deleting	Permission to delete NetVue protocols.
Download protocols from DCP	DCP: Download Protocols	Permission to download protocols from the NetVue Collaboration Platform.
Generate MIB	MIB: Getting	Permission to generate SNMP MIB files based on NetVue protocols.

6.9.2.7 Protocols & Templates > Alarm Templates

Cube Permission	SD Permission	Description
UI Available	SD Administration: Alarm Templates	Permission to access the alarm templates user interface.
Configure alarm templates (Add)	Alarm Templates: Creating	Permission to create alarm templates.
Configure alarm templates (Edit)	Alarm Templates: Changing	Permission to update alarm templates.
Configure alarm templates (Delete)	Alarm Templates: Deleting	Permission to delete alarm templates.

6.9.2.8 Protocols & Templates > Trend Templates

Cube Permission	SD Permission	Description
UI Available	SD Administration: Trend Templates	Permission to access the trend templates user interface.
Configure trend templates	Trend Templates: Changing	Permission to edit trend templates.

6.9.2.9 Reports & Dashboards > Reports

Cube Permission	SD Permission	Description
UI Available (SDReports)	SD Tools: Reports	Permission to access the NetVue Server Reports module.
UI Available (ReportsView)	Reports: Viewing	Permission to view reports.
Manage mail templates	Reports: Managing Mail Templates	Permission to manage reporter templates.

6.9.2.10 Reports & Dashboards > Dashboards

Cube Permission	SD Permission	Description
UI Available (SDDashboards)	SD Tools: Dashboards	Permission to access the NetVue Server Dashboards module.
UI Available (ViewDashboards)	Dashboards: View	Permission to view dashboards.
Add	Dashboards: Add	Permission to create dashboards.
Edit	Dashboards: Edit	Permission to update dashboards.
Delete	Dashboards: Delete	Permission to delete dashboards.

6.9.2.11 Router Control

Cube Permission	SD Permission	Description
RouterControlConfiguration	Router Control	Permission to configure matrices with the Router Control app.

6.9.2.12 Scheduler

Cube Permission	SD Permission	Description
UI Available	SD Tools: Scheduler	Permission to access the NetVue Server Scheduler module.
Add	Scheduler: Add TASKS	Permission to create tasks.
Edit	Scheduler: Edit TASKS	Permission to update tasks.
Delete	Scheduler: Delete TASKS	Permission to delete tasks.
Execute	Scheduler: Execute TASKS	Permission to execute tasks.

6.9.2.13 Service Templates

Cube Permission	SD Permission	Description
UI Available	Service Templates: View	Permission to view service templates.
Add	Service Templates: Create	Permission to create service templates.
Duplicate	Service Templates: Duplicate	Permission to duplicate service templates.
Edit	Service Templates: Edit	Permission to edit service templates.
Delete	Service Templates: Delete	Permission to delete service templates.
Apply	Service Templates: Apply	Permission to apply service templates.
Reapply	Service Templates: ReApply	Permission to reapply a service template to a service.
Detach	Service Templates: Detach	Permission to detach a service from its parent service template.
Export	Service Templates: Export	Permission to export service templates.

6.9.2.14 System Configuration > Agents

Cube Permission	SD Permission	Description
UI Available	SD Administration: Agents	Permission to access the Agents page in System Display and Cube.
Add	NetVue Agent: Adding	Permission to add NetVue Agents to the NetVue Server.
Delete	NetVue Agent: Deleting	Permission to remove NetVue Agents from the NetVue Server.
Redundancy: Switch	DMA Redundancy (failover): Switch	Permission to initiate a manual failover.
Redundancy: Configure	DMA Redundancy (failover): Configure	Permission to configure a pair of redundant NetVue Agents.

Cube Permission	SD Permission	Description
Change Operator Info	General Configuration: Changing Operator Info	Permission to change the operator information in System Display, or the System info in NetVue Cube.
Start	Agents: Starting	Permission to (re)start NetVue Agents.
Stop	Agents: Stopping	Permission to stop the NetVue Agent software on NetVue Agents.
Shutdown	Agents: Shutting down	Permission to shut down NetVue Agents.
Reboot	Agents: Rebooting	Permission to reboot NetVue Agents.
Change IP settings	Agents: Changing IP settings	Permission to update the virtual IP address settings of a NetVue Agent.
Change info	Agents: Changing Info	Permission to update the Name and Location fields of a NetVue Agent.
Clusters: Add	Agents: Adding Clusters	Permission to add NetVue Agents to NetVue Systems (also known as “clusters”).
Clusters: Delete	Agents: Deleting Clusters	Permission to remove NetVue Agents from NetVue Systems (also known as “clusters”).
AgentsInstallAppPackages	Agents: Install App Packages	Permission to install NetVue App packages (.dmapp).
AgentsUpgradeRestore	Agents: Upgrade/Restore	Permission to upgrade DMAs (.dmupgrade, .zip) and to restore backups (.dmbackup).

6.9.2.15 System Configuration > Security

Cube Permission	SD Permission	Description
UI Available	SD Administration: Security	Permission to access the Security page in System Display and the Users / Groups page in Cube.
Administrator	Security: Changing Settings	Permission to edit your own security settings.
Specific > Limited administrator	Security: Limited admin	Permission to create users and to add them to the groups of which you are a member yourself.
Specific > Edit other users	Security: Edit All Users	Permission to edit the security settings of all users.
View users from other groups	Security: View users from other groups	Permission to view users from other groups.
Group Settings > Edit own groups	Edit own groups	Limits the user groups listed in the Group Settings dialog box to those the current user is a member of. In the Create Settings dialog box, all users are shown who are members of the same group as the current user.

Cube Permission	SD Permission	Description
Group Settings > Edit all groups	Cube group settings: Edit all	Displays all available user groups in the Group Settings dialog box. In the Create Settings dialog box, all user groups with a settings file and all users are shown.

The permission** Edit other users **can be granted only to users who have also been granted the** Administrator **permission.

6.9.2.16 System Configuration > Security > Notifications / Alerts

Cube Permission	SD Permission	Description
UI Available	SD Tools: Notifications	Permission to access the Notifications user interface.
Configure Email	Notification: Edit Email notifications	Permission to manage your own email notifications.
Configure SMS	Notification: Edit Sms notifications	Permission to manage your own text message notifications.
Allow configuration of other users	Notification: Edit notifications of another user	Permission to manage email and text message notifications of other users.

6.9.2.17 System Configuration > Backup

Cube Permission	SD Permission	Description
UI Available	SD Administration: Backup	Permission to access the Backup page in System Display and Cube.
Configure	Backup: Changing Settings	Permission to configure the backup settings.

6.9.2.18 System Configuration > Database

Cube Permission	SD Permission	Description
UI Available	SD Administration: Database	Permission to access the Database page in System Display and Cube.
Configure Local DB	Database: Settings Local Db	Permission to change the settings of the local database.
Configure Central DB	Database: Settings Central Db	Permission to change the settings of the central database.

6.9.2.19 System Configuration > Logging

Cube Permission	SD Permission	Description
UI Available	SD Administration: Logging	Permission to access the Logging page in System Display and Cube.
Change settings	Logging: Changing Settings	Permission to change the log file settings.
Clear logfiles	Logging: Clearing Logfile	Permission to clear the log file.

6.9.2.20 System Configuration > Mobile Gateway

Cube Permission	SD Permission	Description
UI Available	SD Administration: Mobile Gateway	Permission to access the Admin ‣ Mobile Gateway page of System Display.
Configure general settings	Mobile Gateway: Changing Settings	Permission to change the settings of the Mobile Gateway.
Configure commands	Mobile Gateway: Changing Commands	Permission to manage the command list.
Configure destinations	Mobile Gateway: Changing Destinations	Permission to manage the destination list.
Configure remote users	Mobile Gateway: Changing Remote Users	Permission to manage the list of remote users.
Load logfile	Mobile Gateway: Loading Logfile	Only used in NetVue versions prior to 6.5.3.
Clear logfile	Mobile Gateway: Clearing Logfile	Only used in NetVue versions prior to 6.5.3.
Remove SMS from stack	Mobile Gateway: Remove SMS	Permission to remove text messages from the SMS stack.
Reset GSM	Mobile Gateway: Resetting GSM	Permission to reset the Mobile Gateway.
Send SMS	Mobile Gateway: Sending SMS	Permission to send ad hoc text messages.
Allow access to Mobile UI	Mobile UI: Access	Permission to access the NetVue mobile apps.

The permissions `Mobile Gateway: Clearing Logfile` and `Mobile Gateway: Loading Logfile` are no longer used. Since NetVue Server v6.5.3, the log file of Mobile Gateway is located in the general `C:\Skyline NetVue\Logging` directory and can be consulted in the Admin ‣ Logging page.

6.9.2.21 System Configuration > SNMP Managers

Cube Permission	SD Permission	Description
UI Available	SD Administration: SNMP Managers	Permission to access the SNMP Managers page in System Display and the Trap forwarding page in Cube.
Add	SNMP Managers: Creating	Permission to add SNMP Managers to the list.
Edit	SNMP Managers: Editing	Permission to make changes to the configuration of the listed SNMP Managers.
Delete	SNMP Managers: Deleting	Permission to delete SNMP Managers from the list.
Resend alarms	SNMP Managers: Resend	Permission to resend history alarms to a particular SNMP Manager.

6.9.2.22 System Configuration > Tools

Cube Permission	SD Permission	Description
Control background tasks of all users	Control Background Tasks of all users	Permission to see and control the background tasks of all users.
Allow access to query executor	Database: Executing Queries	Permission to execute SQL queries against the local or central database.

6.9.2.23 Trending

Cube Permission	SD Permission	Description
UI Available (SDTrendOverview)	SD System Overview: Trend Overview	Permission to access the View ‣ **Trend Overview** page of System Display.
UI Available (ViewTrending)	Trending: Accessing Graphs	Permission to view trend graphs of parameters that are being trended.

6.9.3 Other

Cube Permission	SD Permission	Description
AdminTools	Admin tools	Permission to access the Tools section of the System Center, and the Admin Tools menu in System Display.
ViewElementManager	CPE Manager: View	Permission to use the CPE Management module.

6.10 Configure User Settings for a Group

All users who have ever logged on to a NetVue Agent using NetVue Cube have their own personalized user settings on that NetVue Agent.

However, the system administrators can configure the settings for an entire user group, so that:

- All users in the group share the same default settings
- Specific default values are locked, so that users cannot change those settings.

To configure a user group, you can assign a new set of user settings containing only factory defaults, or an existing set of user settings from another user or user group.

1. In NetVue Cube, open the **Settings** card using either of these methods:
    a. Click **Start** ‣ **Apps** ‣ **Settings**.
    b. Or, click the current user in the top-right corner of the screen, and click **Settings**.
2. In the bottom-left corner of the **Settings** card, click **Configure group...**

    If you do not see the Configure group button, then you cannot configure user group settings. In that case, ask your system administrator to grant you the necessary permissions.

3. In the **Group settings** dialog box, select the user group to have user settings assigned.
4. Click **Assign.**
5. In the **Create settings for group [GroupName]** dialog box, you can either:
    a. Click **New settings**, if you want to assign a new set of user settings containing nothing but factory defaults.
    b. Click **Copy settings from** and select a user group from the list, if you want to copy the set of user settings from that user group to the user group you selected in step 3.
6. Click **OK** to close the **Create settings for group [GroupName]** dialog box.

6.11 NetVue User Guide

If a set of user settings is assigned to a user group, you can open that set and specify a default value for every setting in it.

1. In NetVue Cube, open the **Settings** card using one of these ways:
    a. Click **Start** ‣ **Apps** ‣ **Settings**.
    b. Or, click the current user in the top-right corner of the screen, and click **Settings**.
2. In the bottom-left corner of the **Settings** card, click **Configure group...**

    If you do not see the Configure group button, then you cannot configure user group settings. In that case, ask your system administrator to grant you the necessary permissions.

3. In the **Group settings** dialog box, select the user group to have the user settings configured, and click **Open**.

   If the Open button is unavailable, no user settings are assigned to the group. You must assign the settings to the group first, and then configure them.

4. Using the table of contents on the left, go through all pages of the **Settings** card and check each user setting. The settings in this window are the same as in the regular user settings window. However, there are two additional features:
   - Click the lock icon next to a setting to make sure users cannot change it themselves.
   - Click the eye icon next to a setting to hide the setting from users. When the icon shows a line across the eye, the setting is hidden.
5. Click **OK** to close the **Settings** card.

6.12 About the clientsettings.dat files

6.12.1 Locations of the clientsettings.dat files

Users and user groups can have a `clientsettings.dat` file. A `clientsettings.dat` file only contains user settings, no computer settings.

The `clientsettings.dat` file of a user is found at this path:

```
C:\Skyline DataMiner\Users\[UserName]
```

The `clientsettings.dat` file of a user group is found at this path:

```
C:\Skyline DataMiner\Users\SharedUserSettings\Groups\[GroupName]
```

6.12.2 User Permissions that are Required to Manage User Group Settings

For users to be able to assign and configure user group settings, you must grant them one of these user permissions:

In System Display:

- Cube group settings: Edit all
- Cube group settings: Edit own groups

In NetVue Cube:

- Group Settings > Edit all groups
- Group Settings > Edit own groups

6.12.3 If a User is a Member of More than One Group

If a user is a member of more than one user group, default user settings for this user are supplied from the first user group that has been assigned a set of user settings. In other words, the first user group that has a `clientsettings.dat` file supplies the settings for the user.

6.13 Set Up LDAP/Active Directory

NetVue supports any LDAP compatible directory (e.g., OpenLDAP) as an alternative to Active Directory for importing users and groups into a NetVue Server.

Setting up LDAP/Active Directory is straightforward. Set up the NetVue server to join an active domain. Contact your IT/Network representative for information about setting up or adding the NetVue server to the active domain.

Once the NetVue server has been added to the domain, the user must have NetVue Administrative rights as shown in Figure 6-14.

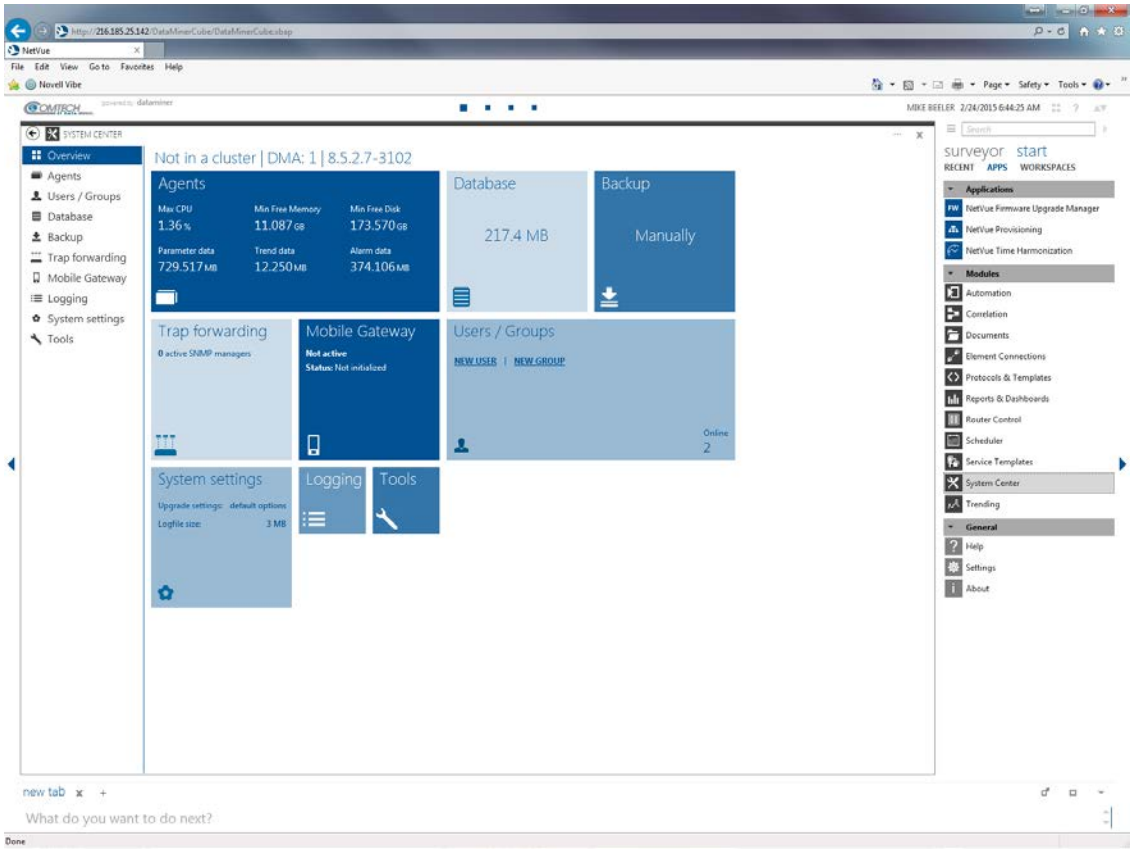


Figure 6-14. System Center with Security Enabled

Select the Users/Groups tab as if administering standard security. On the Security tab, there are two selections:

- **users**
- **groups**

For simplicity, using the **groups** tab allows entire lists (groups) of users to be added to the NetVue, instead of adding users individually.

1. To select a group:
    a. Select the "Add existing group" button.
    b. Check the group or groups that must be added.

Each user associated with the selected group is added to the NetVue as valid users. See Figure 6-15.

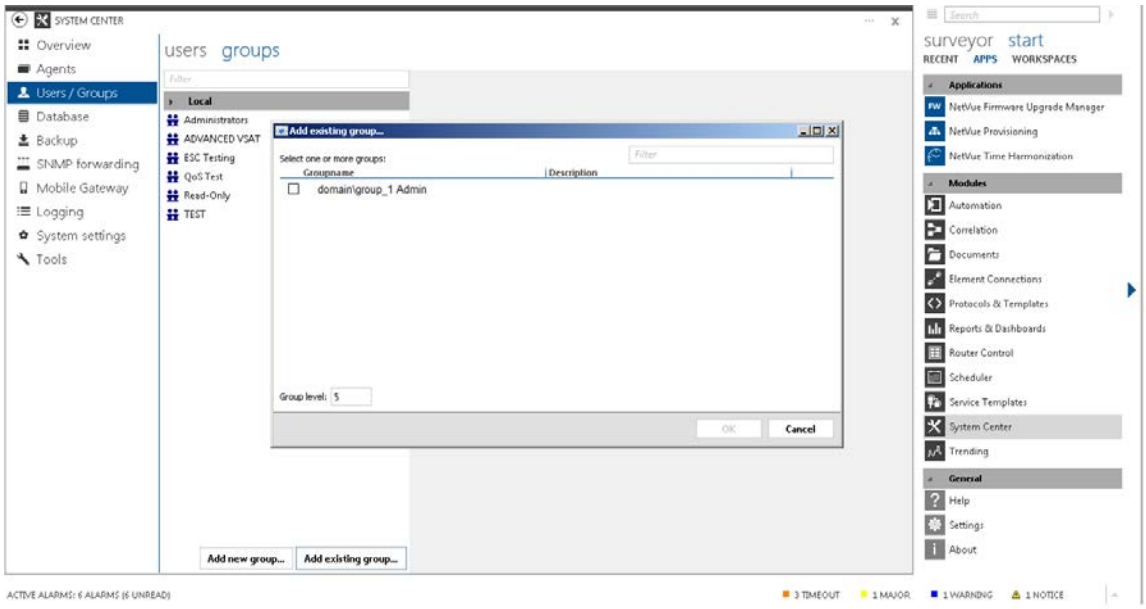


Figure 6-15. LDAP/Active Directory Groups

2. If a single user is to be added:
    a. Select **users**.
    b. Click the **Add existing user** button.
    c. Check the user or users that must be added.

Each user is associated with the native domain assigned to the NetVue server. See Figure 6-16.

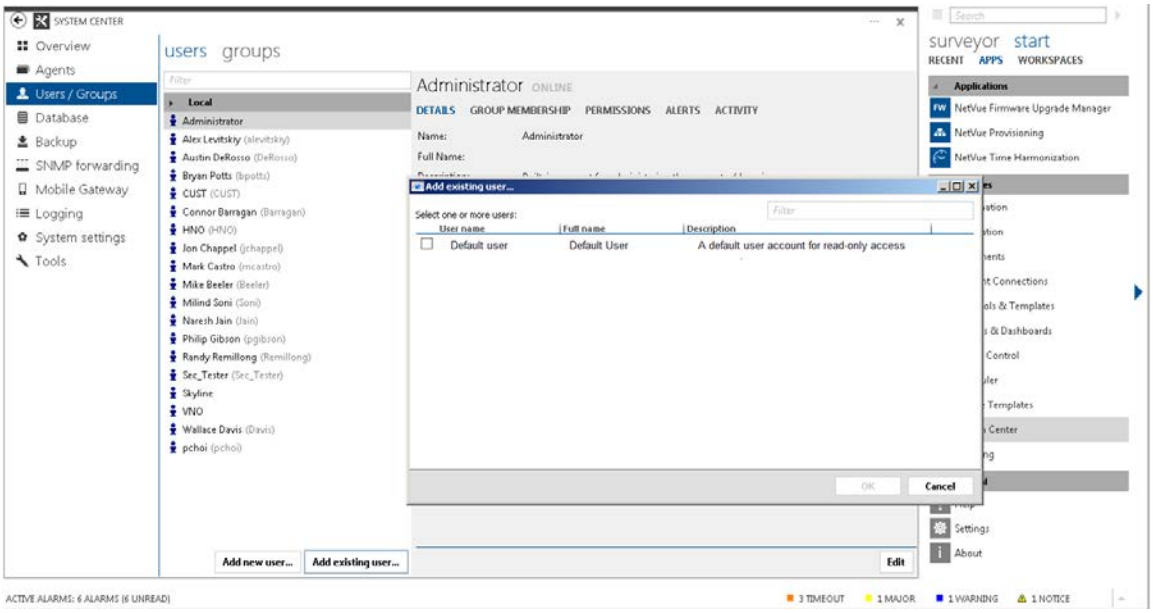


Figure 6-16. LDAP/Active Directory Users

Once the LDAP/Active Directory user has been added, the user is assigned a group membership and will appear as a manually configured user. See Figure 6-17.

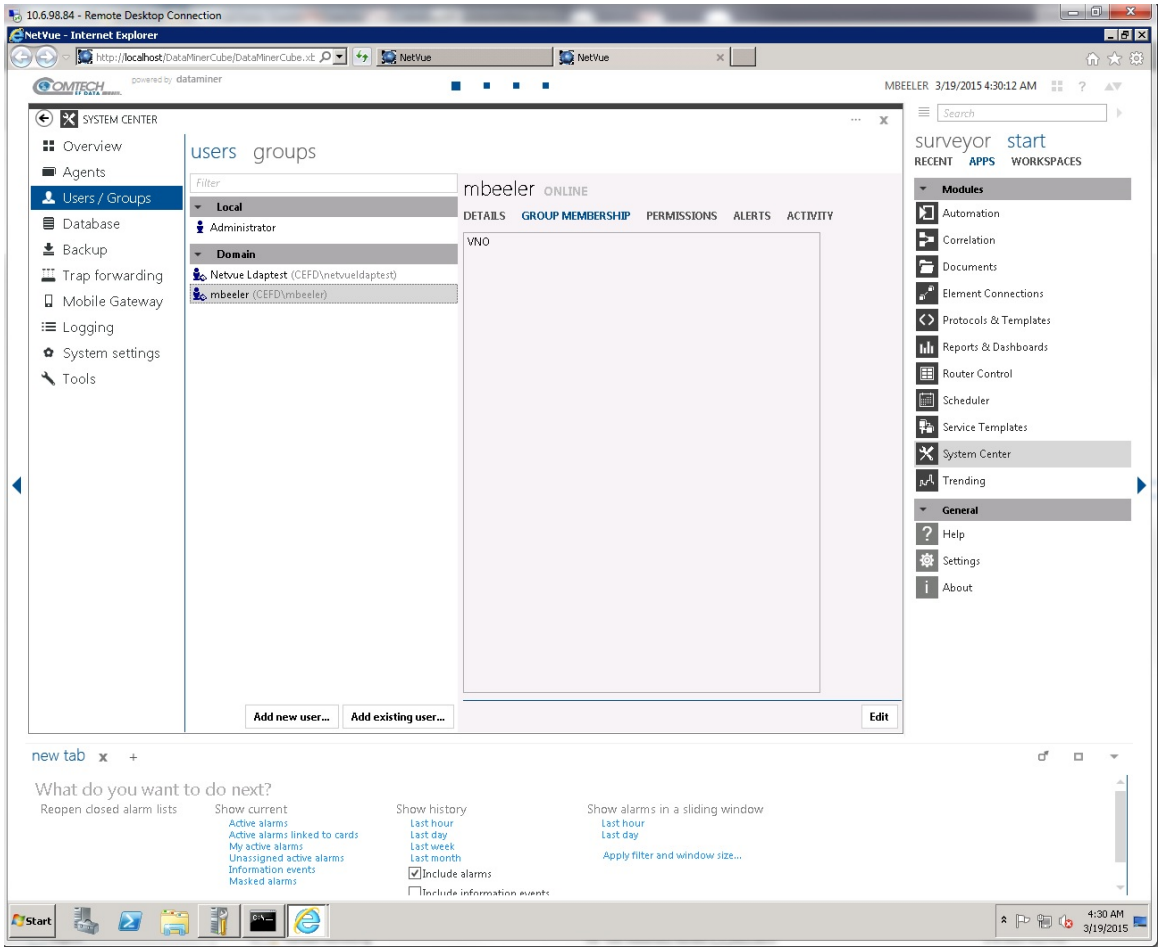


Figure 6-17. LDAP/Active Directory User Added and Assigned Group Membership

For both the **Add existing groups** or **Add existing users**, the user will be assigned a group access as described in the beginning of this chapter. See Figure 6-18.

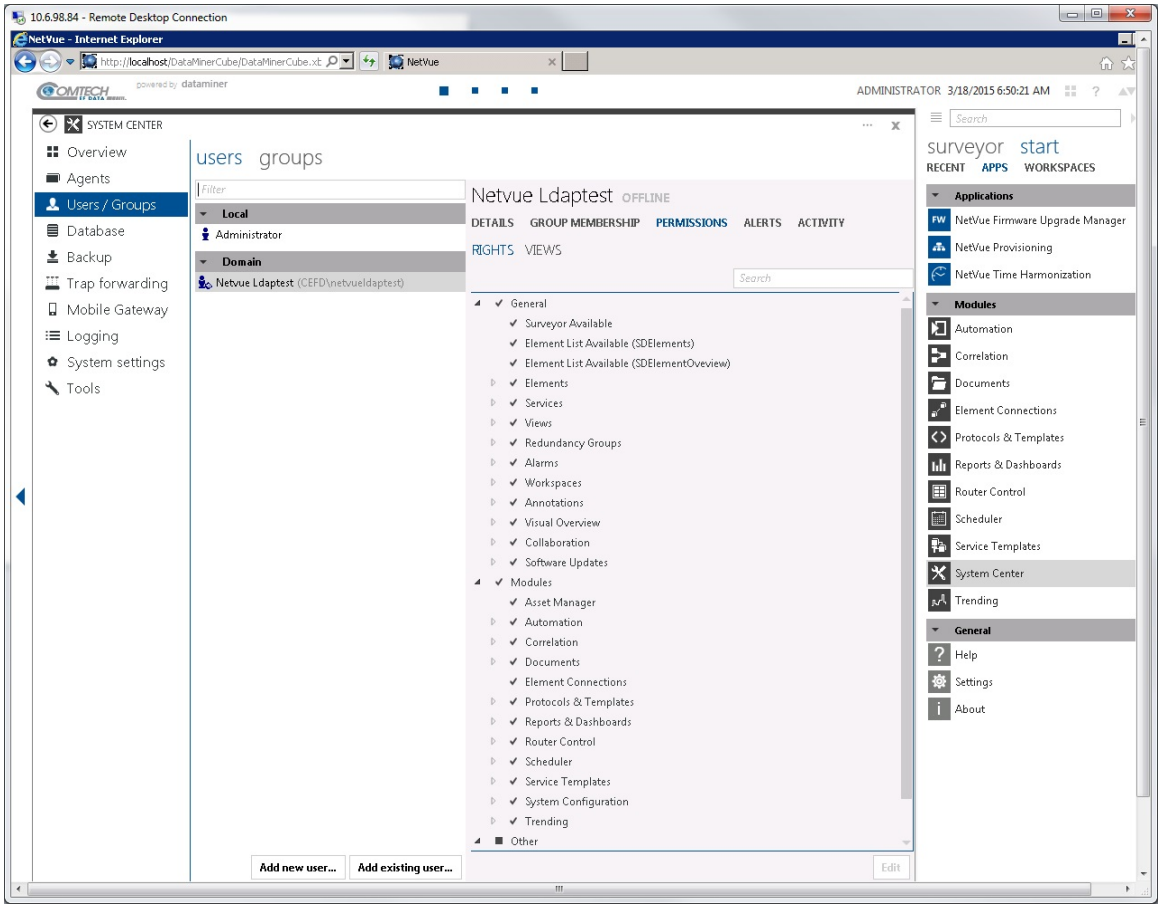


Figure 6-18. Permissions (Rights) for a LDAP/Active Directory User

If a user is removed from a domain, or their access level is changed, this is reflected in NetVue.

6.13.1 LDAP section in NetVue.xml

To establish a link between a NetVue Server and an LDAP (other than Active Directory), open the `DataMiner.xml` file and add or modify the `<LDAP>` tag. The `<LDAP>` tag should contain all necessary LDAP server settings.

6.13.1.1 OpenLDAP

This example shows how Global Telecom Company (GTC) has configured the LDAP tag for OpenLDAP:

```
<LDAP nonDomainLDAP="true" host="10.0.0.207"
      username="" password="" auth=""
      namingContext="DC=gtc,DC=local" useForFullName="true">
   <Group>
      <Filter>(objectClass=groupOfNames)</Filter>
      <Classname>groupOfNames|posixGroup</Classname>
      <NameField>cn</NameField>
      <DescriptionField>description</DescriptionField>
   </Group>
   <User>
      <Filter>(objectClass=inetOrgPerson)</Filter>
      <Classname>inetOrgPerson|person</Classname>
      <AccountNameField>uid</AccountNameField>
      <DisplayNameField>displayName</DisplayNameField>
      <DescriptionField>title</DescriptionField>
      <EmailField>mail</EmailField>
      <PhoneField>homePhone</PhoneField>
      <PagerField>pager</PagerField>
   </User>
</LDAP>
```

6.13.1.2 Active Directory

This example shows how Global Telecom Company (GTC) has configured the LDAP tag for Active Directory:

```
<LDAP nonDomainLDAP="true" host="dc.gtc.be"
      port="389" username="" password="" auth=""
      namingContext="DC=gtc,DC=local" useForFullName="true">
   <Group>
      <Filter>(&amp;(objectClass=group)
        (groupType:1.2.840.113556.1.4.803:=2147483648))</Filter>
      <Classname>group|foreignSecurityPrincipal</Classname>
      <NameField>name</NameField>
      <DescriptionField>description</DescriptionField>
   </Group>
   <User>

<Filter>(|(&amp;(objectCategory=person)(objectClass=user)(objectSid=*)
        (!samAccountType:1.2.840.113556.1.4.804:=3))

(&amp;(objectCategory=person)(objectClass=user)(!objectSid=*)))</Filter
>
      <Classname>person</Classname>
      <AccountNameField>sAMAccountName</AccountNameField>
      <DisplayNameField>name</DisplayNameField>
      <DescriptionField>description</DescriptionField>
      <EmailField>mail</EmailField>
      <PhoneField>telephoneNumber</PhoneField>
      <PagerField>pager</PagerField>
   </User>
</LDAP>
```

Typically, you do not have to add an <LDAP> tag when using Active Directory. However, if you must specify non-default settings (e.g., when you want to link to a secondary domain controller), add an <LDAP> tag and specify all necessary settings.

6.13.2 Remarks

If namingContext is empty, in case of Active Directory, it will be auto-discovered. When using OpenLDAP, namingContext must be specified.

The host name can be specified in either the host attribute of the <LDAP> tag, or the namingContext attribute of that same tag.

If you put it in the namingContext attribute, be sure to put it in front of the actual naming context data, separated by the forward slash /.

Examples:

- <LDAP host="dc.gtc.local" namingContext="dc=GTC,dc=local">
- <LDAP namingContext="dc.gtc.local/dc=GTC,dc=local">

If the LDAP server requires authentication, enter both the username and the password, and set auth to "**simple"**.

The <Filter> tags contain the LDAP search filters to find all groups and users. Note that in XML ampersands must be encoded as "&**amp**;".

The <Classname> tags indicate the object class(es) that identify groups and users. Multiple values can be separated with pipe characters ("|").

If you set the useForFullName attribute to "**true**" (i.e., the default setting), the full user names will be retrieved by means of LDAP. If you set this attribute to "**false**", full user names will be retrieved by means of NetAPI instead.

6.13.3 Automatic refresh of group membership and user information

When using Active Directory, group and user data are refreshed automatically. However, if you are using an LDAP compatible directory other than Active Directory, and you want to have group and user data refreshed automatically, then you should create a scheduled task that executes a javascript file containing this code:

```
var localDMS = new ActiveXObject("SLDMS.DMS");
var localReturn;
localDMS.Notify(92 /*DMS_REFRESH_LDAP*/, 0, "", "", localReturn);
```

The frequency with which a scheduled task should occur depends on the number of users and groups in your domain. For example, you could schedule the task to occur once a day.

BLANK PAGE

Chapter 7. NetVue Elements

7.1 Introduction to the NetVue™ Elements

An element in NetVue can be defined as any device that is being monitored by NetVue. These devices can be in one of three states:

- **Active:** This is the default state of the element when first added to NetVue. The element is being polled and the virtual IP address of the element is active.
- **Paused:** Communication between NetVue and the element has been paused, but the virtual IP address of the element is still active. This allows for the element and all associated resources to still be accessible.
- **Stopped:** Communication between NetVue and the element has been stopped and the virtual IP address of the element has been destroyed.

7.2 Change the State of an Element in NetVue

To change the state of an element in NetVue, do these steps:

1. In the **Surveyor** view, right-click the applicable element.
2. Choose **Status**.
3. Select the desired state for the selected element: **Activate, Pause, Stop** or **Restart.**

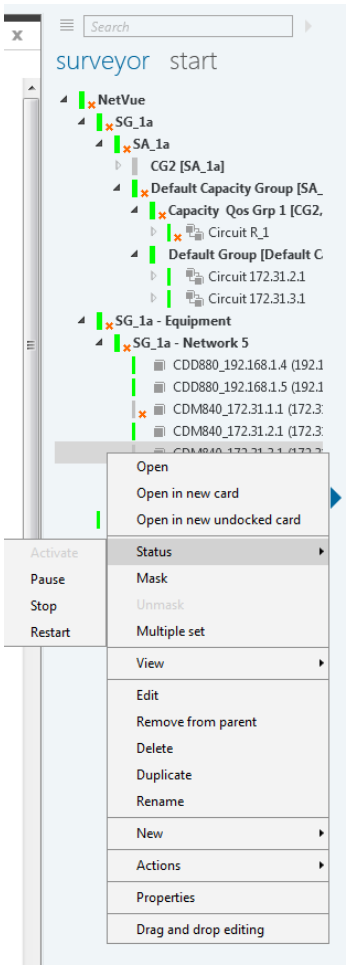


Figure 7-1. Element States

7.3 Add, Duplicate, and Delete Elements in NetVue

This section describes the necessary actions to add, duplicate, and delete an element from NetVue.

7.3.1 Add an Element

Do these steps to add an element to NetVue:

1. Right-click in the Surveyor menu (located on the right side of the NetVue Cube display) and select **New > Element**.

   This opens a card in the main display of the NetVue Cube.

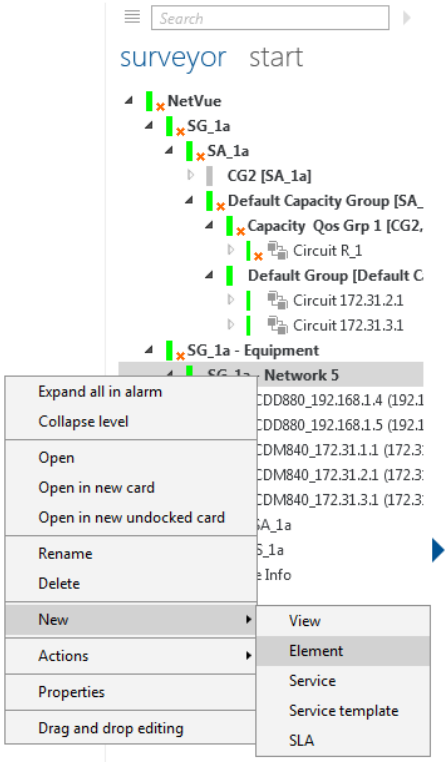


Figure 7-2. Add a New Element

2. In the **Edit** tab of the card, specify the information for the element to be added:

   - **Name:** The name of the element.

     The name of the element can be changed at any time. In the NetVue Cube, the element is identified by its unique ID, which is a combination of the DMA ID, where the element was created originally, and the ID of the element itself. If you must change the element name, make sure that the new name makes sense to the NetVue operators and users.

   - **Description**: A brief description of the element.
   - **DMA**: The DMA (NetVue server) responsible for the polling.

- **Protocol**: The name of the protocol that NetVue uses to communicate with the element. This selection box has all protocols available in NetVue. If you do not find the protocol you need, it must be added.
- **Version**: The version of the protocol that NetVue uses to communicate with the element. This selection box lists all versions of the protocol selected previously in the **Protocol** selection box.
- **Alarm Template:** The name of the alarm template that contains the alarm thresholds to be used while monitoring the element. This selection box lists:
    - The default alarm template: **<No Monitoring>**
    - All alarm templates associated with the protocol and the protocol version selected previously
- **Trend Template:** The name of the trend template that controls what trend data is stored in the database for the element. This selection box lists:
    - The default trend template: **<No Trending>**
    - All trend templates associated with the protocol and the protocol version selected previously

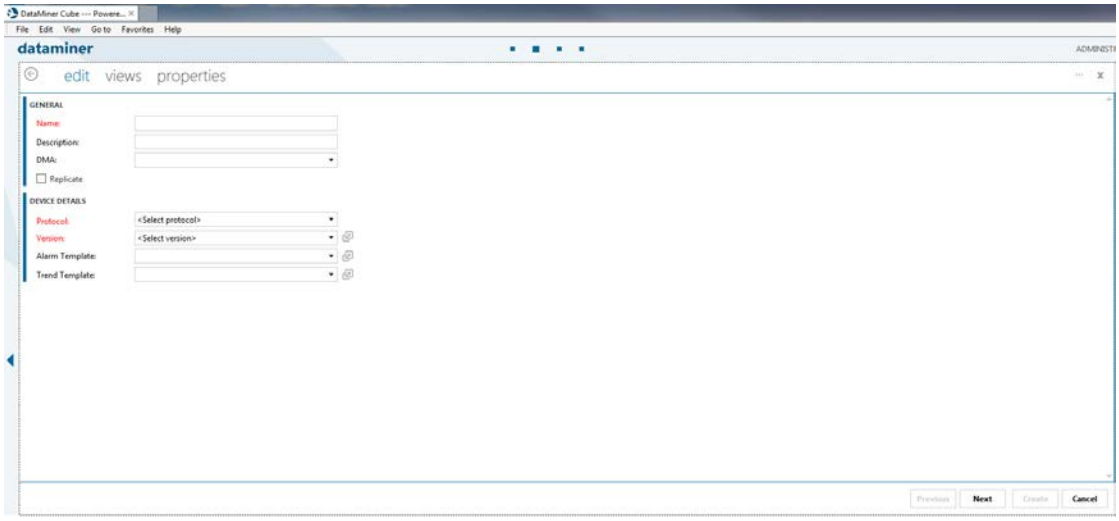


Figure 7-3. Edit Element Parameters

3. If the element is to be a replica of an element from another NetVue system, select the **Replicate** check box.
4. Depending on the selected protocol, you might need to specify more options.
    - For **SNMP**, specify this information:
        - IP address
        - Network Interface (NIC)
        - Port Number (default = 161)
        - SNMP protocol settings:
            - Get community string (default = **public**)
            - Set community string (default = **private**)

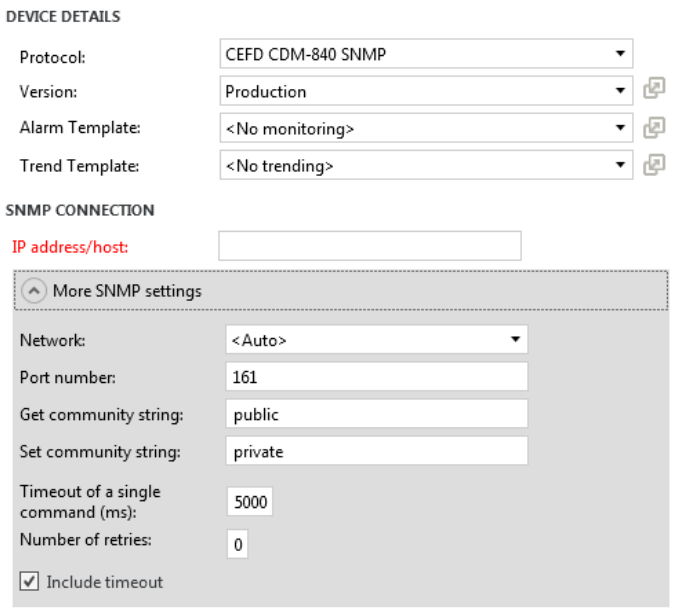


Figure 7-4. Edit SNMP Parameters

- For **Serial port**, specify this information:
  - Baud rate
  - Port number
  - Data bits
  - Stop bits
  - Parity
  - Flow control

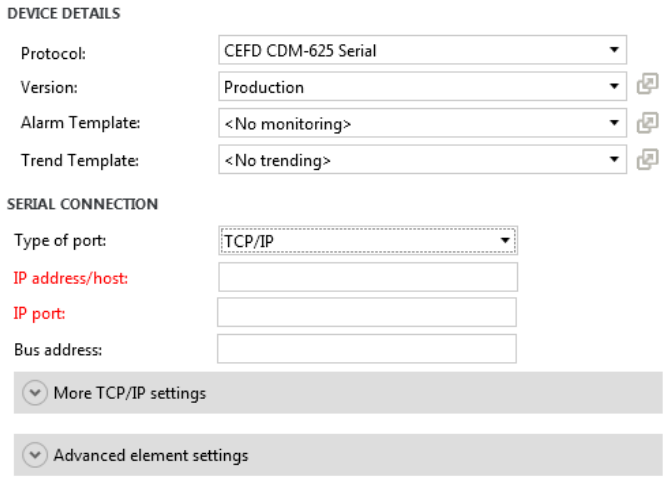


Figure 7-5. Edit Serial Parameters

- For **TCP/IP** or **UDP/IP**, specify this information:
  - Network Interface (NIC)
  - IP address of the element
  - IP port
- Specify the timeout settings per connection:
  - **Timeout of a single command (ms):** The period (in milliseconds) during which NetVue will wait for a response after sending a command to the element. The range for this setting is between **10 and 120,000 milliseconds**. If NetVue does not receive a response from the element within the specified period, NetVue will retry to send the same command.
  - **Number of retries:** The total number of times that NetVue will attempt to send the same command again in case the previous attempts were unsuccessful. The value range for this setting is between **0 and 10** retries. After sending the command for the specified number of retries, if NetVue still has not received a response from the element, it will move on and continue with the next command.
  - **Include timeout:** The element will timeout on a single command if this check box is selected.

5. Specify the advanced element settings:
   - **The element goes into timeout state when it is not responding for (sec):** When the element fails to respond to commands for longer than the number of seconds specified in this setting, NetVue puts the element in a timeout state. Range: **0 – 120 seconds**
   - **Slow poll settings:** When an element is in a timeout state, NetVue can force it to go into a slow poll mode. In this state, NetVue **will not** send any commands to the element. Instead, a simple ping command is sent at regular intervals. Once the element responds to the ping command, NetVue will again poll the element normally. To enable slow polling in case of timeout, select the check box and specify these two settings:
   - **The element...after:** This setting controls when the element will go into slow poll mode:
     - After a fixed number of seconds. Range: **1 – 300 seconds**
     - After having been put in a timeout state for a specific number of communication attempts Range: **1 – 500 attempts**.
   - **Ping interval:** The interval (in seconds) between two ping commands. Range: **1 – 300 seconds**.

Use extreme caution when changing these settings! Communications between NetVue and the element can be affected negatively. Communication interruptions or failure can occur.

   - **Enable SNMP agent:** Select this check box and specify the virtual IP address and the subnet mask in to be able to send SNMP **Get** and **Set** commands to the virtual IP address of the element.

- **Hidden:** Select this check box if the element must be hidden.
- **Read-only:** Select this check box if the element must be read-only. If this selection is made, the element parameters cannot be updated.
- **Element state:** Select the initial state of the element. By default, this setting is **Active**.

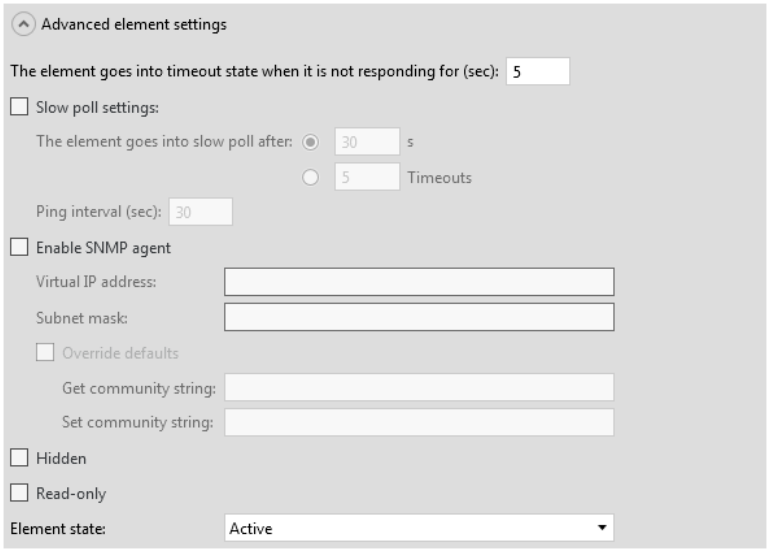


Figure 7-6. Advanced Element Settings

6. Click **Next** and specify the view(s) to which the element must be linked.

Figure 7-7. Element View Assignment

7. Click **Next** and specify any custom properties that are available for the element protocol.

Figure 7-8. Custom Element Properties

8. Click **Create** to add the element.

   If any required information is missing or incorrect, the **Create** button is disabled, and the label with the missing or incorrect information shows in red.

7.3.2 Duplicate an Element

To quickly add an element that is similar to an existing element, you can duplicate the existing element by using these steps:

1. Right-click the element in the Surveyor, and select **Duplicate**.

   A new card shows in the main view of NetVue. This new element already contains information from the element that was duplicated.

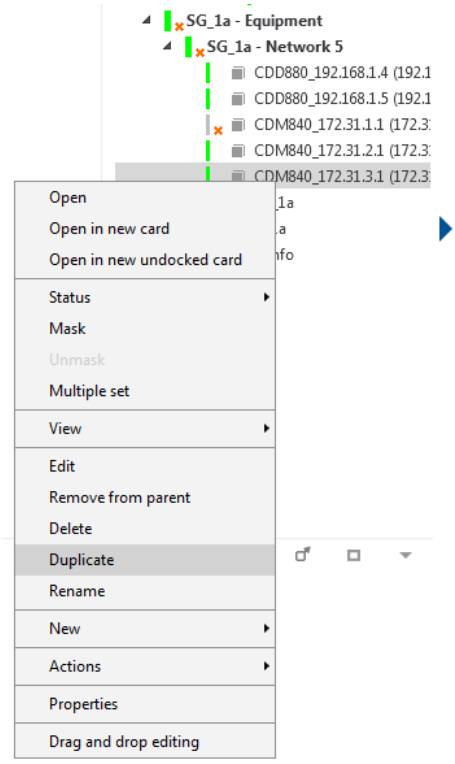


Figure 7-9. Duplicate an Element

2. Make any necessary changes in the card for the new element, and click **Create**.

7.3.3 Delete an Element

To remove an element, do these steps:

1. Right-click the element in the Surveyor, and select **Delete**.
2. In the pop-up confirmation box, click **Yes**.

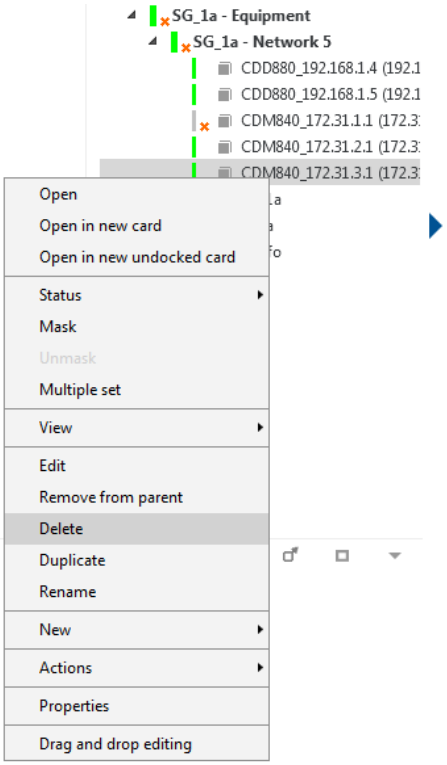


Figure 7-10. Delete an Element

7.4 NetVue Cube Element Cards

The NetVue element cards show information for one or more selected elements.

To see element cards, click the desired element(s) in the Surveyor.

The cards open in the main NetVue viewing area. The front of the element card shows a graphic representation of the element. The back of the element card can be quite different, depending on the element's protocol. However, these characteristics are consistent for all element cards:

- The bar at the bottom right of the element card shows the alarm state for the last 24 hours. Double-click the bar to see reports on the element's alarm state.
- The bar at the bottom left of the element card opens the alarm console in a new tab, if double-clicked.
- In the top left corner of the card, there is a drop-down list or tree view with the different pages for the card.

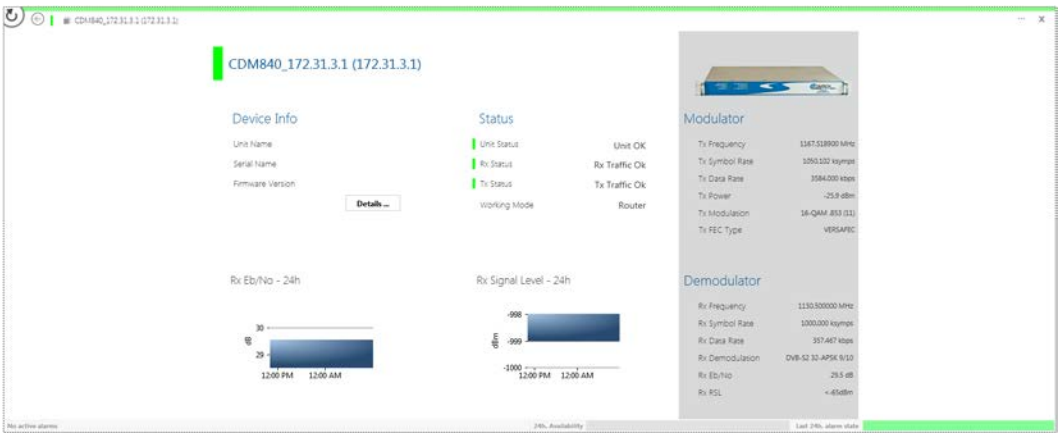


Figure 7-11. Element Card Front

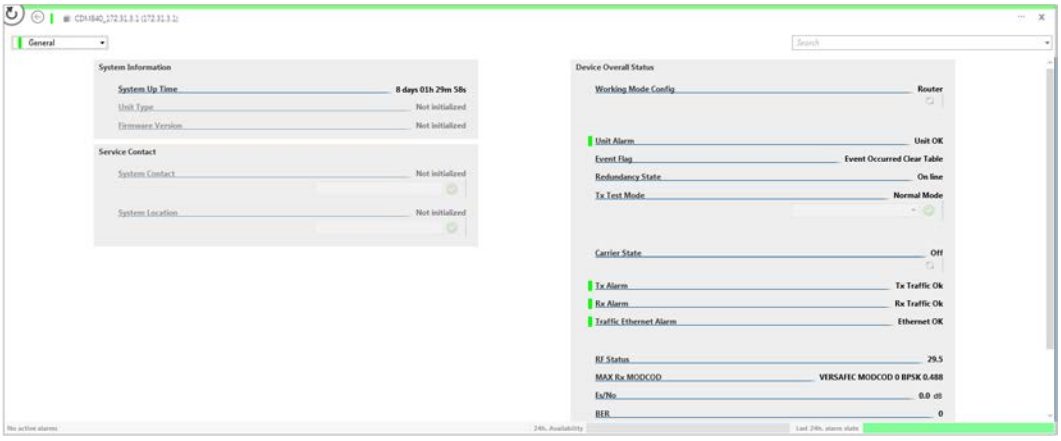


Figure 7-12. Element Card Back

To configure whether a drop-down list or a tree view is displayed, go to:

Settings > **Datadisplay** > **Page Selection Mode**

and choose a page selection mode.

Page	Description
General parameters	General parameters for the element, such as its lock status, number of alarms, connection state, etc.
Annotations	Any annotations that are available for the element, with the possibility to create or edit annotations as needed
Reports	A graphic representation of the alarm distribution, alarm events, alarm states and a timleline. You can set the period for which data shows: to the last 24 hours, one week to date or one month to date.
Documents	Any documents that are available either on NetVue in general, or for the element protocol. You can also add, edit or delete documents here.

7.5 Import and Export Elements in NetVue

This section describes the steps necessary to import and export elements in the NetVue Cube.

Only CSV files that have been created by NetVue during a previous export can be imported.

7.5.1 Import Elements from a CSV File

To import elements from a CSV file, do these steps:

1. Open the View card of the view where you want to import the elements.
2. In the top right corner of the View card, click the **…** icon and select **Import elements from CSV**.
3. In the **Open** dialog box, select the CSV file that contains the desired elements, and click **Open**.

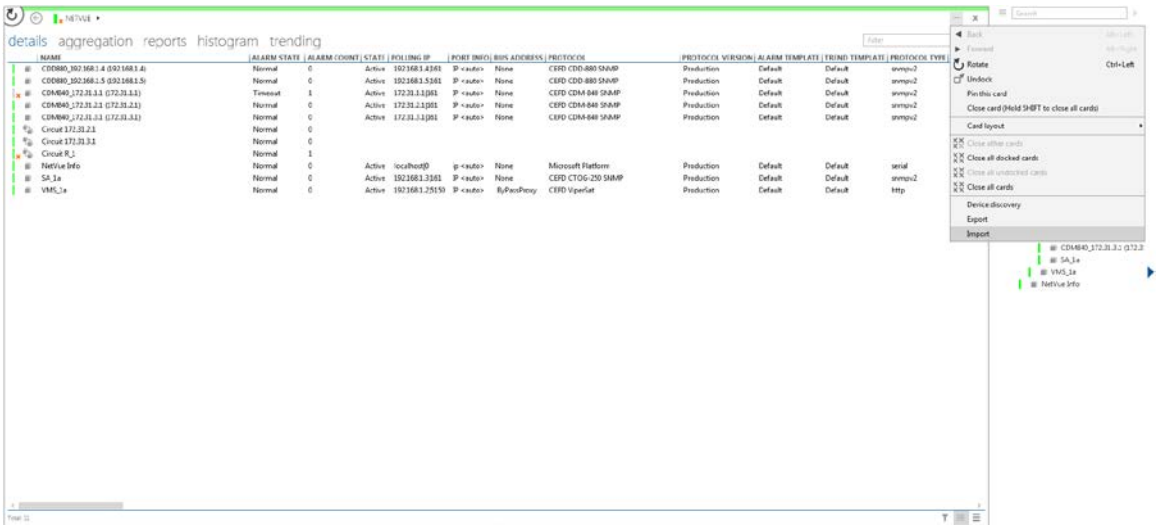


Figure 7-13. Import an Element

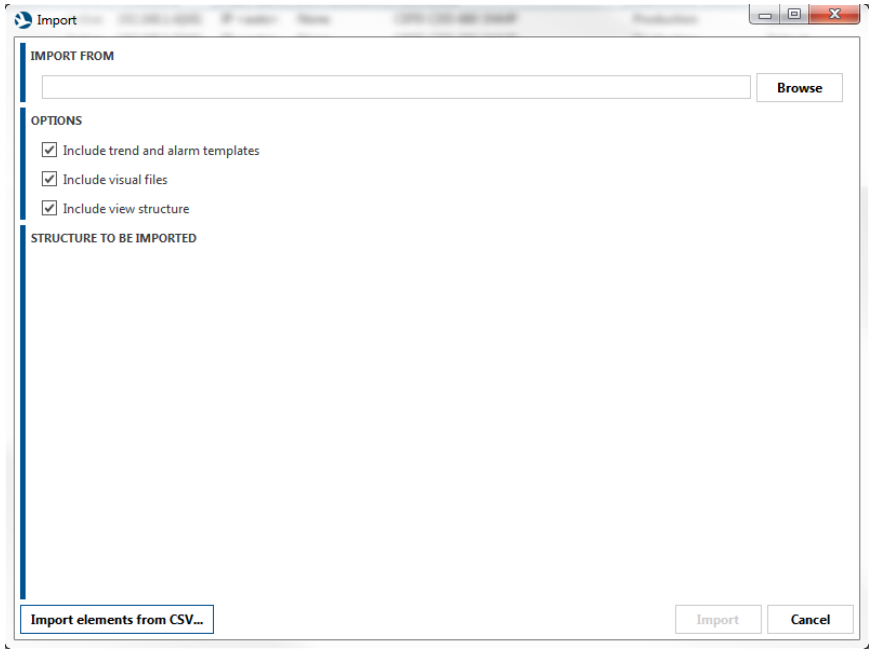


Figure 7-14. Import an Element from a CSV File

Alternatively, you can use the Surveyor right-click menu to import elements:

1. Right-click a view.
2. Select **Actions** > **Import**.
3. Click the **Import elements from CSV** button in the **Import** window.

7.5.2 Export Elements from a View Card

To export elements from a View card, do these steps:

1. Open the View card of the view from which you want to export the elements.

   - or -

   To export all elements within NetVue, open the root View card.

2. In the top right corner of the View card, click the **…** icon and select **Export all elements to CSV.**
3. In the **WHAT** section of the **Export** window, select what must be included in the export:
4. All data
   - Only IDs, with or without view IDs
   - Only IP addresses with hostnames, with or without IP addresses and polling IP addresses/Serial Gateways
5. In the **HOW** section of the **Export** window, select the type of export:
   - Export to CSV file
   - Copy to clipboard
   - Print
6. Click **Export.**
7. Depending on the type of export, these steps are necessary:
   - Indicate where the file is to be saved, for an export to CSV.
   - Click **OK** in a confirmation message, for a copy to clipboard.
   - Select the print settings, for a print.

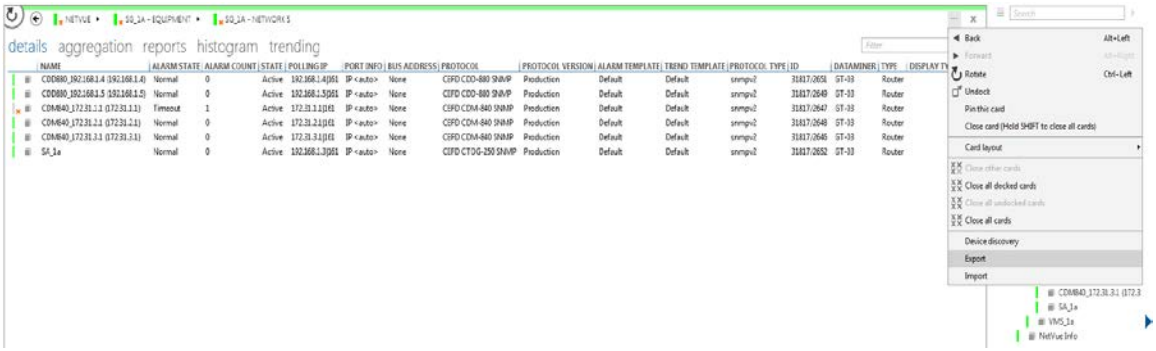


Figure 7-15. Export an Element

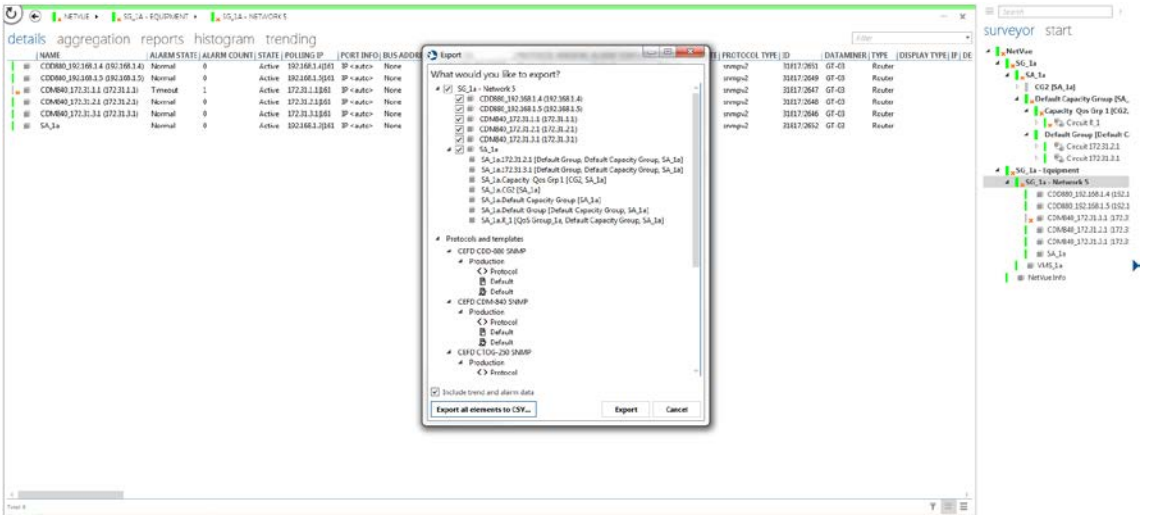


Figure 7-16. Export an Element to a CSV File

Alternatively, you can use the Surveyor right-click menu to export elements:

1. Right-click a view or element in the Surveyor.
2. Select **Actions** > **Export**.
3. Click the **Export all elements to CSV** button.

7.6 Replicated Elements

With element replication, elements managed by one NetVue system can be seen and manipulated in another NetVue system.

A replicated, foreign element is manipulated like a locally managed element. It can be assigned alarm templates, trend templates, etc., as well as be included in services.

Unlike a locally managed element, however, a replicated element is not polled. It simply inherits all parameter statuses from its real counterpart on the other NetVue system.

A replicated element will go into a timeout state when the source element goes into a timeout state and is not reachable. The default connection checking interval is 30 seconds.

7.6.1 .NET Remoting

All information about the remote element is retrieved by means of the .NET Remoting protocol. The default port is 8004.

To optimize communication, only parameter changes are sent to the replicated element.

7.6.2 Replicate Elements in NetVue Cube

To make an element act as a replica of a different element managed by another NetVue IMS, create a new replica element, or edit an existing replica element.

The input and output interfaces of the source element are replicated also. However, any element connections for the source element are not replicated.

If the Production version of the protocol on the remote NetVue IMS is different from that on the local NetVue IMS, only the statuses of the common parameters are transferred.

Security is defined on the remote NetVue IMS. Access to the remote element depends on the rights granted to the credentials that were used for log-on access to the remote NetVue IMS. Therefore, the element cannot be replicated if those log-on credentials do not have permissions to the view that contains the selected element.

To create a new replica element or to edit an existing replica element, do these steps:

1. Select the **Replicate** check box.
2. Enter the IP address or host name of the remote NetVue IMS that is hosting the source element to be replicated.
3. Enter the user name and password that the local NetVue IMS can use to log on to the remote NetVue IMS to retrieve the Parameter values from the remote source element.
4. Click **Retrieve elements.**
5. From the retrieved elements, select the source element to be replicated.
6. Continue creatiing or editing as you would typically.

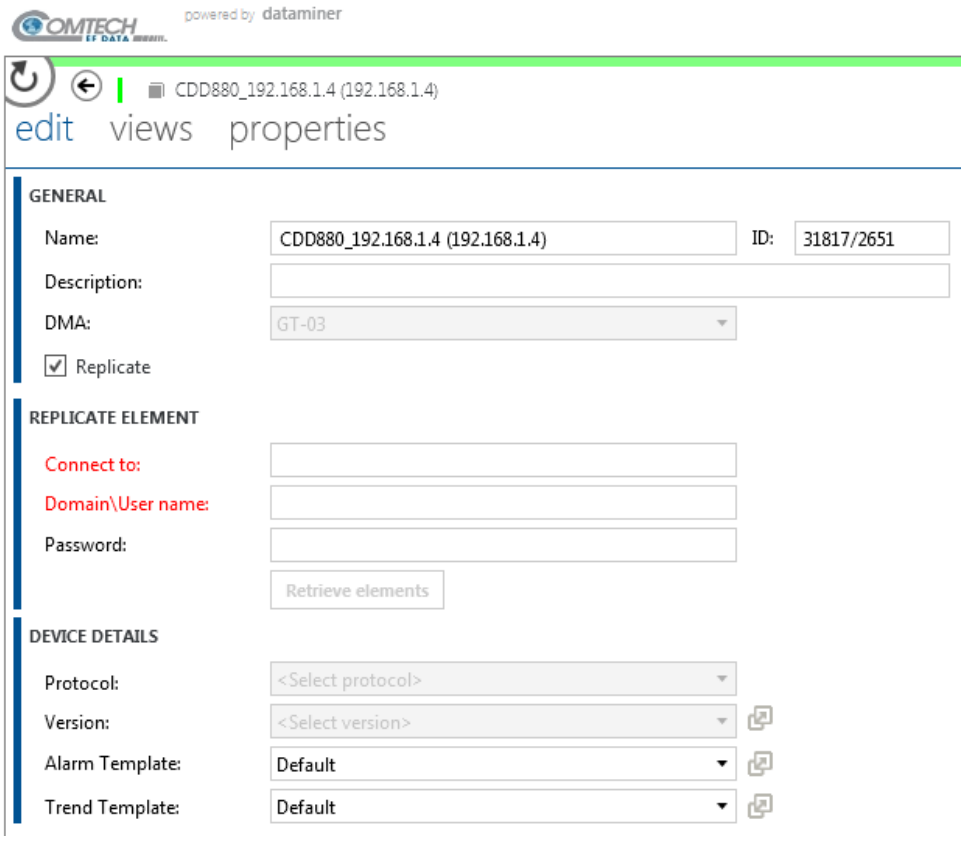


Figure 7-17. Replicate an Element

7.7 Locate Devices in the System to Add to NetVue IMS

NetVue Cube has a wizard you can use to discover devices in an existing infrastructure automatically. This is the Device Discovery wizard.

This wizard can discover devices within a specific IP range, and then immediately create the corresponding elements in the NetVue IMS.

A network discovery element is required in NetVue IMS for correct operation of the Device Discovery wizard. This is an element with the protocol **Skyline IP Network Discovery.**

To discover devices and create elements with the Device Discovery wizard, do these steps:

1. Open the View card where the new element is to be created.
2. Right-click the colored header bar

   or -

   Click the **…** button in the top right corner of the card.

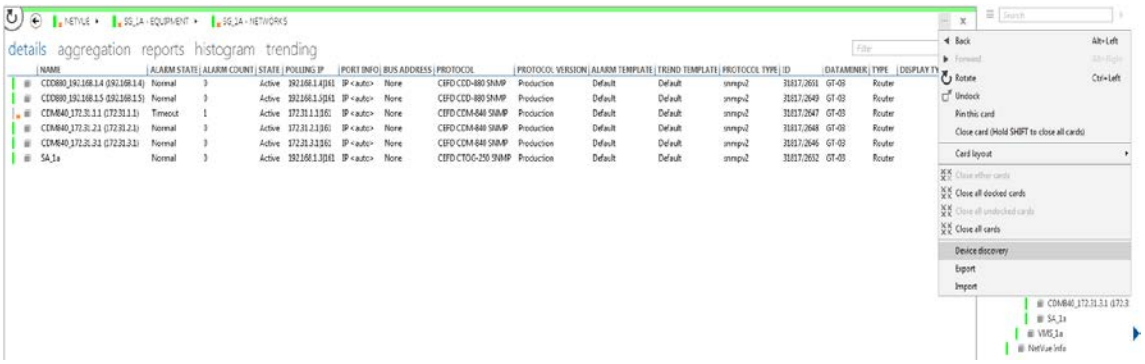


Figure 7-18. Device Discovery

3. Select **Device Discovery** to open the wizard.
4. Under **IP range**, enter the IP address range(s) to include or exclude.

   If the IP address is invalid, the Discover button is unavailable.

5. Under **Devices**, select the method by which the wizard looks for devices:
   - **Generic**: look for any device using SNMP and/or ping.
   - **Protocol-specific**: look for devices based on protocol.

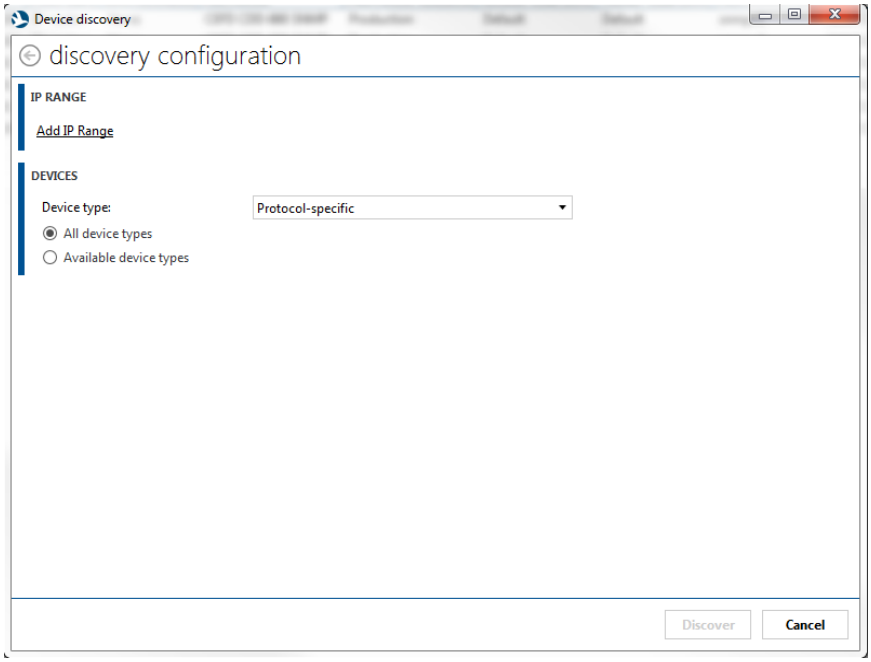


Figure 7-19. Device Discovery Pop-up Window

6. Click the **Discover** button.

   The Device Discovery wizard searches for devices within the IP range. This can take some time. If there are no devices within the specified range, a message tells you that no devices were found.

   Otherwise, a list of discovered devices is shown. If any devices have an IP address that matches one of the existing elements, they are shown in the color gray.

7. In the list of discovered devices, select the device(s) for which the element is to be created. If necessary, use the **Select all** and **Unselect all** buttons at the bottom.

   If many devices are found, it can be useful to sort them by clicking on the column header.

8. Click **Prepare for element creation**.

9. In the **element creation** window, enter the basic information required to create the element: **Name**, **Description**, **Protocol**, **Protocol Version** and **Get** and **Set Community String**.

   You can enter the name, description, protocol or protocol version for several elements at once. Select multiple elements in the list and click one of the information fields to open a** multiple edit **box. Enter or select the information for multiple selected elements.

10. Click **Create** to create the elements.

    The Device Discovery wizard shows a summary of the elements that were created.

7.8 Hidden Elements

Hidden elements are created mostly for internal purposes. They have no virtual IP addresses.

Typically, a hidden element extracts information from physical devices, which is then passed on to a virtual element.

For example, you can create a hidden IO gateway that reads analog and digital contacts. The gateway passes on the retrieved information to a virtual element that shows the parameters' values.

Hidden elements have no effect on the alarm state of a view, and are not considered in aggregation calculations.

7.8.1 Create Hidden Elements

To create a hidden element: simply create an element, but select the option **Hidden**.

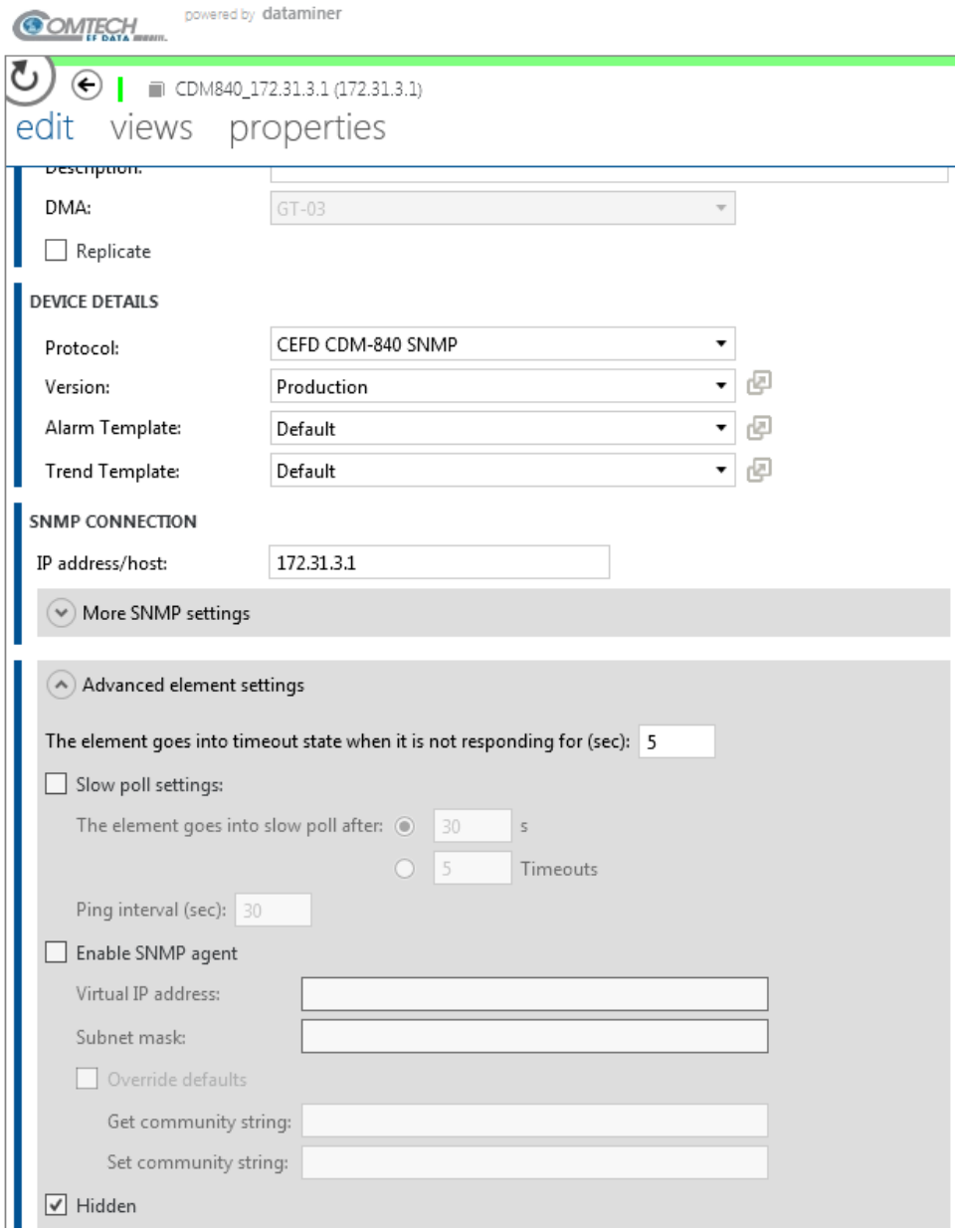


Figure 7-20. Hidden Option to Create a Hidden Element

7.8.2 View Hidden Elements

To see hidden elements in a NetVue Cube view, do these steps:

1. At the bottom of the text side of the View card, click the text that tells you which types of items are shown.
2. Select **Hidden Elements.**

7.9 Virtual Elements

The term virtual element is used for two different kinds of elements:

- Virtual elements in a redundancy group
- Virtual elements used for element connections

7.9.1 Virtual Elements in a Redundancy Group

When a redundancy group is created, a virtual element is created for each of the primary elements. The virtual element represents either the corresponding primary element or its backup, depending on which is operational. Typically, these elements have names within curly brackets, e.g., {Virtual Element 1}.

7.9.2 Virtual Elements Used for Element Connections

It is possible that not all parameters can be communicated through the regular connection for a particular element. For example, for an element with an SNMP connection, there may be a few sensors that require an extra element to communicate their readings to NetVue. In that case, a virtual element can be created that combines a number of parameters from different real elements. In contrast to those real elements, the virtual element does not represent a physical device.

You can use a virtual element to combine multiple elements into a single virtual element. This is known as element consolidation. For example, combine a TX element and an RX element into one virtual RX/TX element.

A virtual element is based on a virtual protocol. This is different from a normal protocol. A virtual protocol is just a list of parameters to be included in the virtual element. When a virtual element is added, the parameters listed in the virtual protocol are linked to their counterparts in the real elements.

A virtual element can also have new parameters, which often contain the result of a mathematical calculation based on the values of one or more parameters from real elements. For example, the output and input levels from a real element could be retrieved to calculate the transmission loss and store the result in a new parameter of the virtual element.

7.9.3 Configure Virtual Elements in NetVue Cube

To configure virtual elements in the NetVue Cube, use the **Element Connections** app. Only elements with a virtual element protocol are shown in the app. The app has two tabs:

- The **configure** tab on the left is where you configure element connections.
- The **overview** tab on the right gives an overview of the existing element connections.

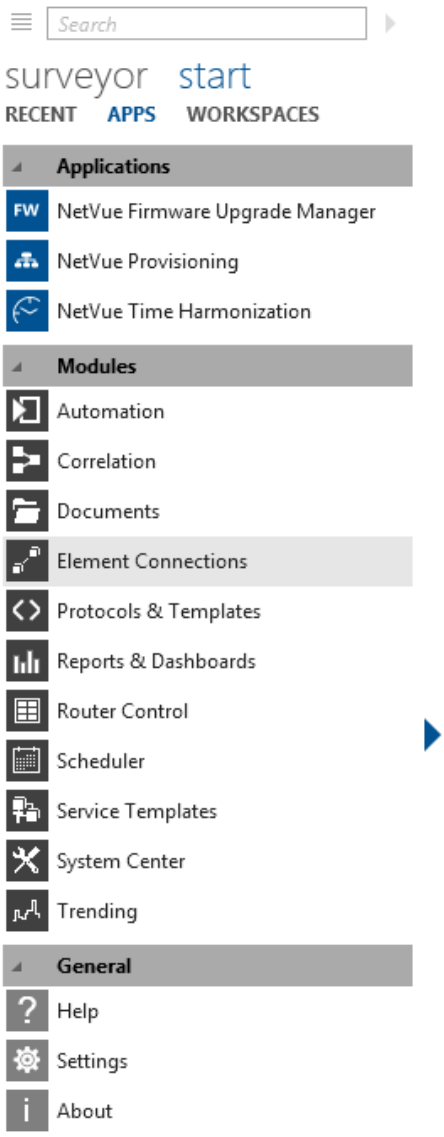


Figure 7-21. Element Connections for a Virtual Element

To configure virtual elements in the NetVue Cube, do the following steps:

1. Go to **Start > Apps > Element Connections**.
2. In the **configure** tab, expand the listed element that needs configuration of an element connection.
3. For each desired connection between a parameter of the virtual element and a parameter from another element:
    a. In the **Instance** column, select the table index, if necessary.
    b. In the **Linked element** column, select the element to link to the selected parameter.
    c. In the **Linked parameter** column, select the parameter to link to the selected parameter.
    d. In the **Linked instance** column, select the table index, if necessary.
    e. In the **Include element** column, clear the check box to make sure the state of the connected element does not affect the state of the virtual element. Otherwise, keep the check box selected.
4. Click the **Save** button at the bottom of the card.

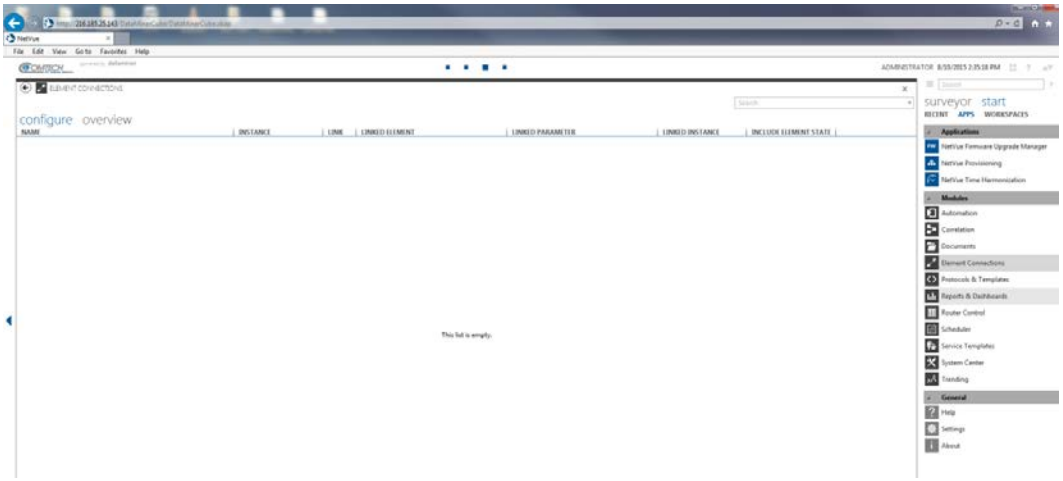


Figure 7-22. Element Connections Card

7.9.4 Dynamic Virtual Elements

A Dynamic Virtual Element (DVE) can be created when a large number of elements are combined. For example, this can be helpful when numerous cards are contained in one chassis, and every card must be a separate element.

A dynamic virtual element consists of one main parent DVE, from which child DVEs are generated dynamically. The parent DVE is responsible for all communication with NetVue IMS, and all parameters of child DVEs are delivered from the parent DVE.

7.9.4.1 Create a Dynamic Virtual Element

You create a parent DVE like a regular element. However, you assign a DVE protocol during creation.

In the parent DVE, all child DVEs appear as rows in a table. If a row is added, a new child DVE is added. If a row is removed, the corresponding child DVE is removed. Each of the child DVEs also counts as an actual element in the NetVue IMS.

Both parent and child DVEs must respect these NetVue element naming conventions:

- If a DVE name contains forbidden characters or leading or trailing dots or spaces, the name is changed automatically. An entry indicating this change is added to the **Element** log.
- If a DVE name is empty or not unique in NetVue IMS, the element is not created or renamed. A notice is generated that tells which primary key of the DVE table row contains the invalid element name. Additional information is logged in the SLErrors.txt file, under **Validate DVE Name**.
- Renaming a parent DVE causes the renaming of all child elements that have names that start with the name of the parent element.

New child DVEs are added in the same view as the parent DVE, except when a View column is specified in the DVE protocol. If there is a View column:

- If the View column is empty, the child DVE is put in the same view as the parent DVE.
- When a value is entered in the View column, the child DVE is put in the view(s) referred to by that value.
- When a value is replaced in the View column for an existing child DVE, the child DVE is moved to the specified view(s), and removed from all other views.

To avoid unnecessary view updates, specify the view(s) immediately when adding new rows to a DVE table with a View column.

7.9.4.2 Edit a Dynamic Virtual Element

The child DVEs get all characteristics, including their different protocols, from the parent DVE protocol. You cannot edit child DVEs directly. To edit a child DVE, you must change the protocol of the parent DVE.

As a consequence:

- You cannot set the state of a single child DVE. If you change the state of a parent DVE, all child DVEs change at the same time.
- You cannot delete a child DVE separately. Instead, you must delete a row in the table of the parent DVE.
- You cannot delete a DVE child protocol separately. However, when a main protocol is deleted, the child protocols are deleted also.

However, you can assign a separate trend template or alarm template to child DVEs, and you can edit properties separately.

7.9.4.3 Enable or Disabe the Creation of DVE Child Elements

You can enable or disable the creation of child elements by means of a setting in the element.xml file of a parent element.

By default, when a parent element is created, the creation of its child elements is enabled. To disable this function, add a **devcreate** attribute in the element.xml file, and set its value to FALSE.

Example:

```
<Element>
<Name dvecreate="FALSE">DVE Main Element</Name>
</Element>
```

When the setting for a parent element is disabled, all of its existing child elements are removed from the system and their element IDs are cleared. When the setting is enabled again for that same parent element, the child elements are be created with new element IDs.

Only DVE main elements that have element creation disabled can be added to a redundancy group.

7.10 Element Properties

By adding properties to views, elements, services and alarms, you can link additional information to NetVue items. This information can be shown in the Alarm console, and you can use it when creating filters and correlation rules.

Each property has a name, a value, and a type.

There are two types of properties:

- **Read-only:** The property and its value can be displayed, but not edited. Properties of this type are managed by the NetVue IMS.
- **Read-write:** The property and its value can be displayed and edited. Properties of this type are managed by NetVue users.

7.10.1 Manage Element Properties in NetVue Cube

This section describes the steps necessary for managing properties for elements in the NetVue cube.

7.10.1.1 Access the List of Properties Linked to a NetVue Element

To get access to the properties of an element:

1. Right-click the element in the Surveyor, or on the back of the View card.
2. Select **Properties**.

   The **Properties** window opens with a separate tab for **general** and **custom** properties.

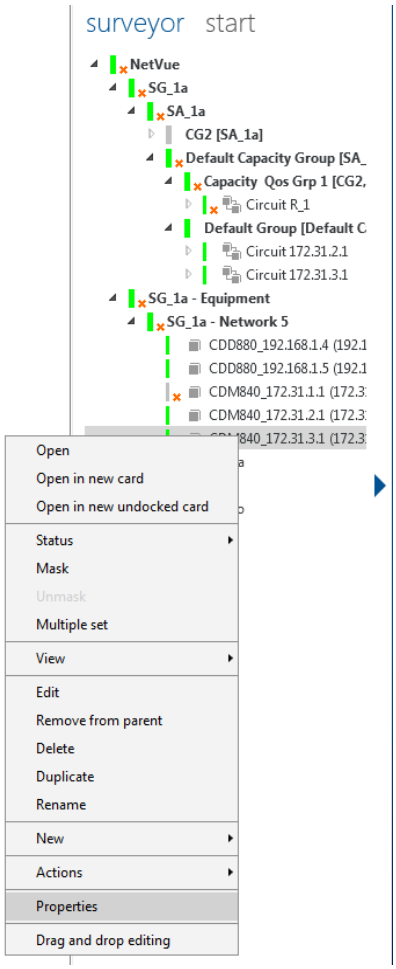


Figure 7-23. Access Element Properties

7.10.1.2 Add a Property to a NetVue Element

To add a property to a NetVue element:

1. Right-click the element to see the list of properties.
2. In the **Properties** dialog box, go to the **Custom** tab.
3. Click the cogwheel button in the bottom left corner, and select **Add.**

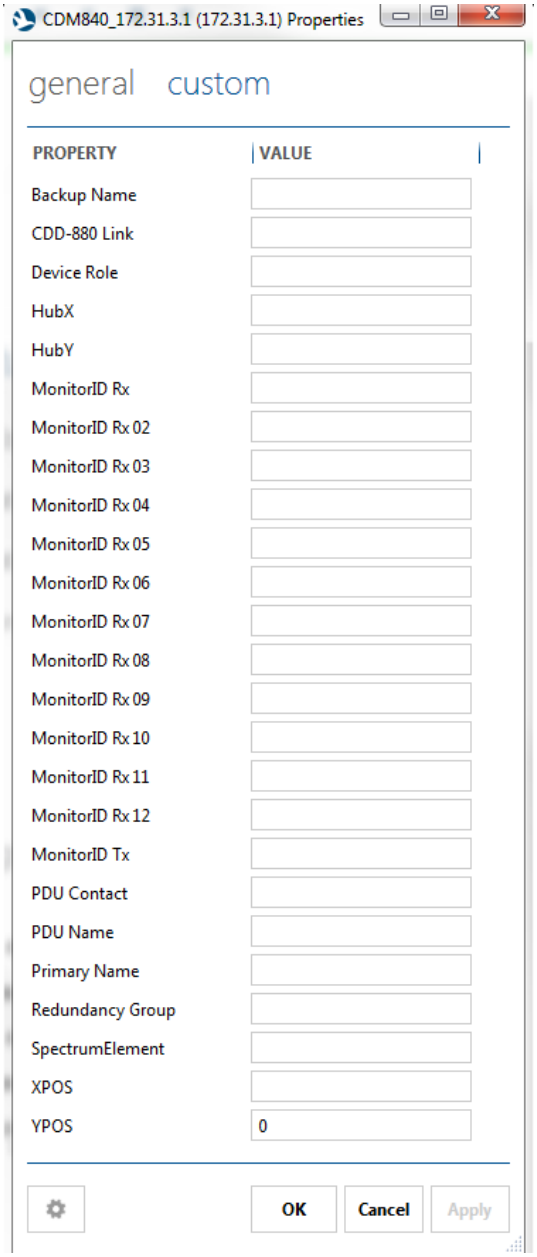


Figure 7-24. Custom Element Properties

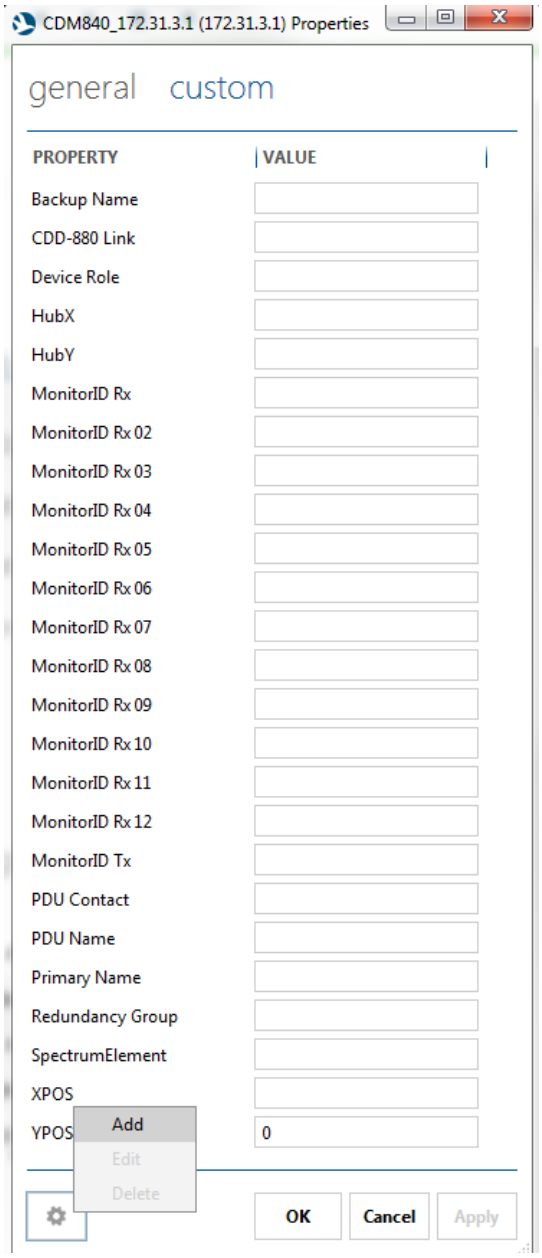


Figure 7-25. Add a Custom Element Property

4. Enter a name for the custom property.
5. Specify these options:
   - **Make this property available for alarm filtering:**

     Select this check box if you want the property to be used in the Alarm console, in filters and in correlation rules.
   - **Display this property in the Surveyor:**

     Select this check box if you want the property to be visible next to the NetVue element in the Surveyor.

- **No format specified:**

  If you do not want to restrict the allowed values, select this option.

- **Format (regular expression):**

  To restrict the allowed values by means of a regular expression, select this check box and enter a regular expression in the text box.

- **Possible values:**

  To specify a list of allowed values, select this check box and add all allowed values to the list.

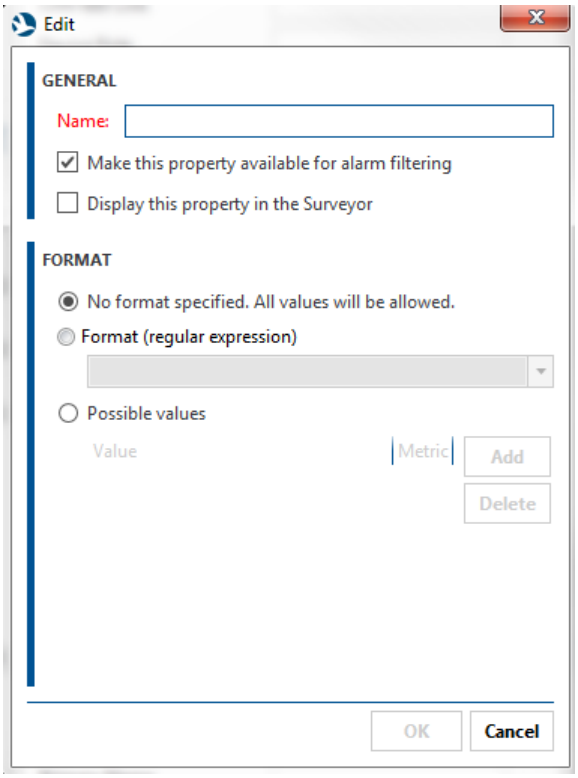


Figure 7-26. Custom Element Property Parameters

6. In the **Edit** dialog box, click **OK.**
7. In the **Properties** dialog box, click **OK.**

7.10.1.3 Edit a NetVue Element Property

To edit a property of a NetVue element:

1. Right-click the element to see the list of properties.
2. In the **Properties** dialog box, go to the **Custom** tab.
3. Select the property to be edited.
4. Click the cogwheel button in the bottom left corner, and select **Edit**.

   The same options are available as when adding a new property.

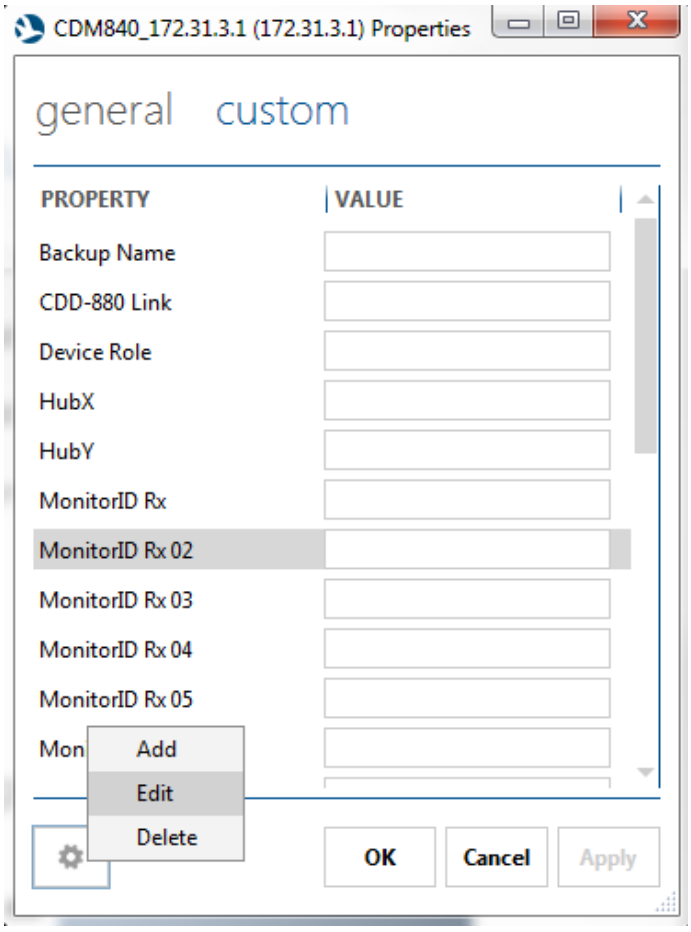


Figure 7-27. Edit Element Property

7.10.1.4 Delete a NetVue Element Property

To delete a property associated with a NetVue element:

1. Right-click the item to see the list of properties.
2. In the **Properties** dialog box, go to the **Custom** tab.
3. Select the property to be edited.
4. Click the cogwheel button in the bottom left corner, and select **Delete.**
5. Click **OK** to confirm.

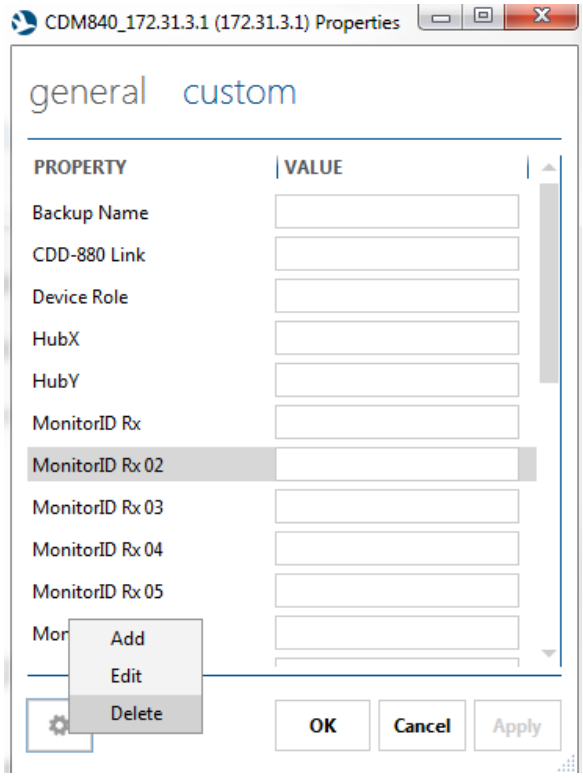


Figure 7-28. Delete Element Property

7.11 Update NetVue Elements

You can update a single element within NetVue, or multiple elements at once. This section describes the steps necessary to do both tasks.

7.11.1 Update a Single NetVue Element

To update one element:

1. Right-click the element in the Surveyor and select **Edit.**

   The same card opens as when a new element is created, but the already configured information is included.

2. Make any necessary changes to the information, and click **Apply.**

For a dynamic virtual element (DVE), to enable or disable child element creation, click Advanced element settings and select or clearEnable DVE child creation.

7.11.1.1 Rename an Element

To simply rename the element, right-click the element in the Surveyor, and select **Rename**.

7.11.2 Update Multiple NetVue Elements

To update a parameter value in multiple NetVue elements:

1. Right-click an element in the Surveyor and click **Multiple set.**
2. In the **Multiple set** dialog box, select the elements in which a particular parameter value is to be updated.
   - By default, the list contains all elements using the same protocol version as the selected element.
   - If an element is desired using a different protocol (version), select another protocol and/or protocol version in the drop-down boxes in the top left corner of the dialog box.
3. Click **Check all / none / invert** to select all elements, or select none of the elements, or invert your selection

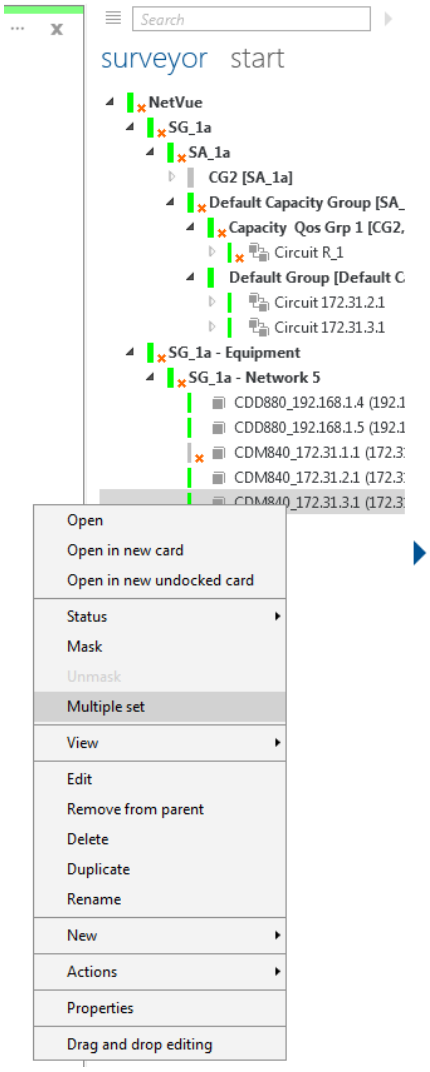


Figure 7-29. Update Multiple Elements

4. In the **Parameter** box, select the parameter to be updated.
    - In the **Parameter** box, if a dynamic table parameter is selected, you must specify a table key in the selection box under it.

When a parameter is selected, the current values of that parameter are retrieved for all listed elements, and then shown in the list.

5. In the **Value** box, specify the new parameter value.
6. Click the **Set** button.

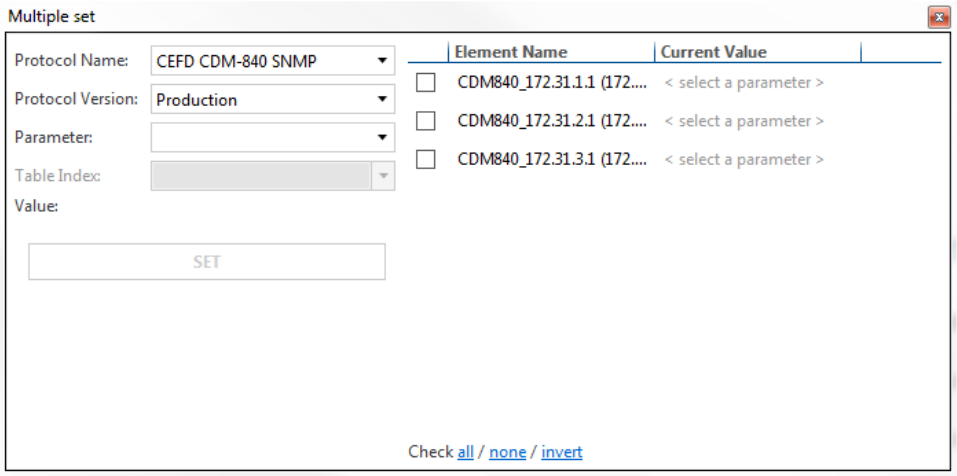


Figure 7-30. Update Multiple Elements Properties

7.12 Mask or Unmask an Element in NetVue

You can mask an element, so that any alarms on that element do not show in the active alarms. For example, do this to avoid unnecessary follow-up when an element is tested.

7.12.1 Mask an Element

To mask an element, do these steps:

1. Right-click the element in the Surveyor and select **Mask**.

   The **Mask** dialog box opens.

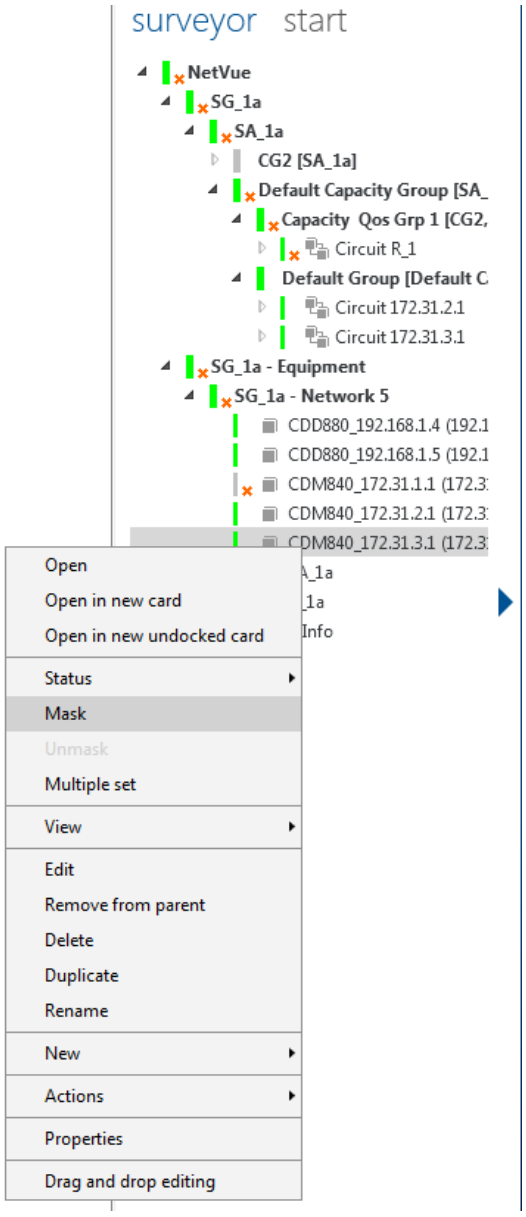


Figure 7-31. Mask an Element

2. Select a masking method:
   - To unmask an agent automatically after a fixed duration, select **Mask element for a limited period of time**, then select the time period to mask the element alarm.
   - To keep the element alarm masked until the NetVue user unmasks it, select **Mask element until unmasked.**
   - To keep the element alarm masked until the alarm clears, select **Mask element until cleared**.

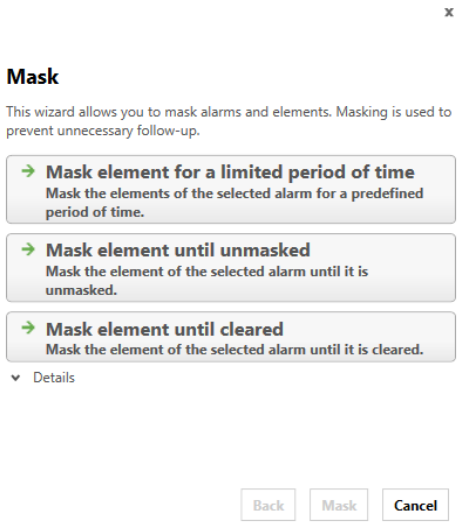


Figure 7-32. Element Masking Options

3. Optionally, a put comment in the dialog box to show a description for the masked alarm.
4. Click **Mask**.

   The element status indicator changes to a purple color, allowing you to identify elements that are in a masked state.

7.12.2 Unmask an Element

To unmask an element alarm:

1. Right-click a masked element in the Surveyor, and select **Unmask**.
2. Optionally, enter a comment in the dialog box.
3. Click **Unmask.**

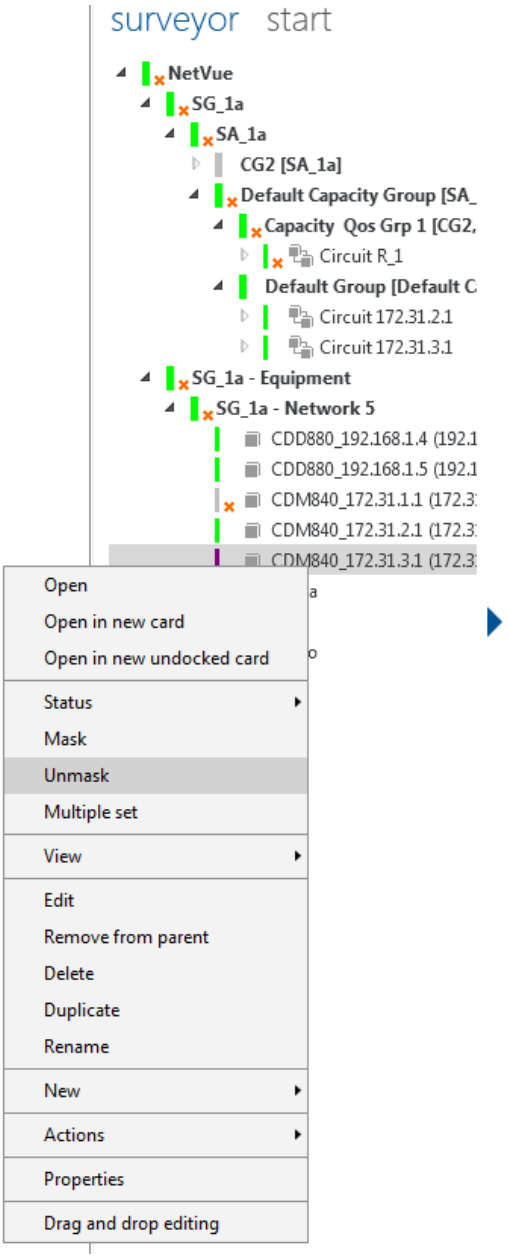


Figure 7-33. Unmask an Element

7.13 Check the Connection State of a NetVue Element

To check the connection state of an element in NetVue:

1. Open the element card by clicking the applicable element in the Surveyor.
2. Go to the **General parameters** page.
3. Scroll to the selection **Communication Info** at the bottom of the page.

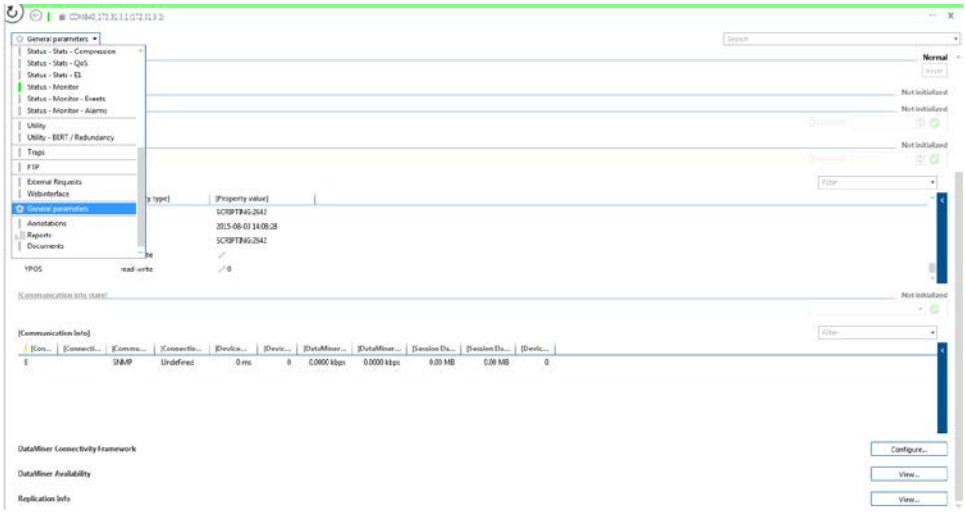


Figure 7-34. Element Connection States

The list shows information about the connection, such as the connection name, type and state.

Several connection states are possible:

Connection State	Description
Undefined	Initial state: No connection has been set up yet.
Responding	For a serial connection. Connection has been set up and communication is up and running.
Not responding	For a serial connection. Connection has been set up, but communication has stopped.
Connected	For a smart-serial connection. Connection has been set up.
Disconnected	For a smart-serial connection. Connection has been lost.

Chapter 8. PROTOCOLS

8.1 About Protocols

Protocols allow a NetVue Agent to communicate with any device from any vendor. Protocols are also known as drivers.

8.1.1 XML-based Protocol Descriptions

Each NetVue protocol is a comprehensive, XML-based description of a third-party protocol. In a NetVue protocol, you can specify all of the following information:

- Conditional device polling mechanisms
- Layout of the user interfaces, showing all relevant device data in real time
- Element Display
- Element Cards (NetVue Cube)
- Default port settings, Alarm thresholds, Parameter labels, etc.
- All information NetVue needs to build the MIB necessary for device communication via SNMP

8.1.2 Protocol Versions

On a NetVue System, you can install multiple versions of the same NetVue protocol in parallel.

Because of the advanced overlay design in NetVue, you can redefine some parts of a NetVue protocol without changing the protocol itself:

- Reuse your personal overlay files when you receive a new version of a protocol.
- Maintain multiple versions of each overlay file and apply them as you see fit.

8.1.3 Manage the Protocols

Manage the protocols in a NetVue system from the **Protocols** page in System Display.

1. Open the **Protocols & Templates** page.
2. In NetVue Cube, go to the top menu and choose **Start | Apps | Protocols &Templates**.
3. Choose from the list in the PROTOCOLS column:

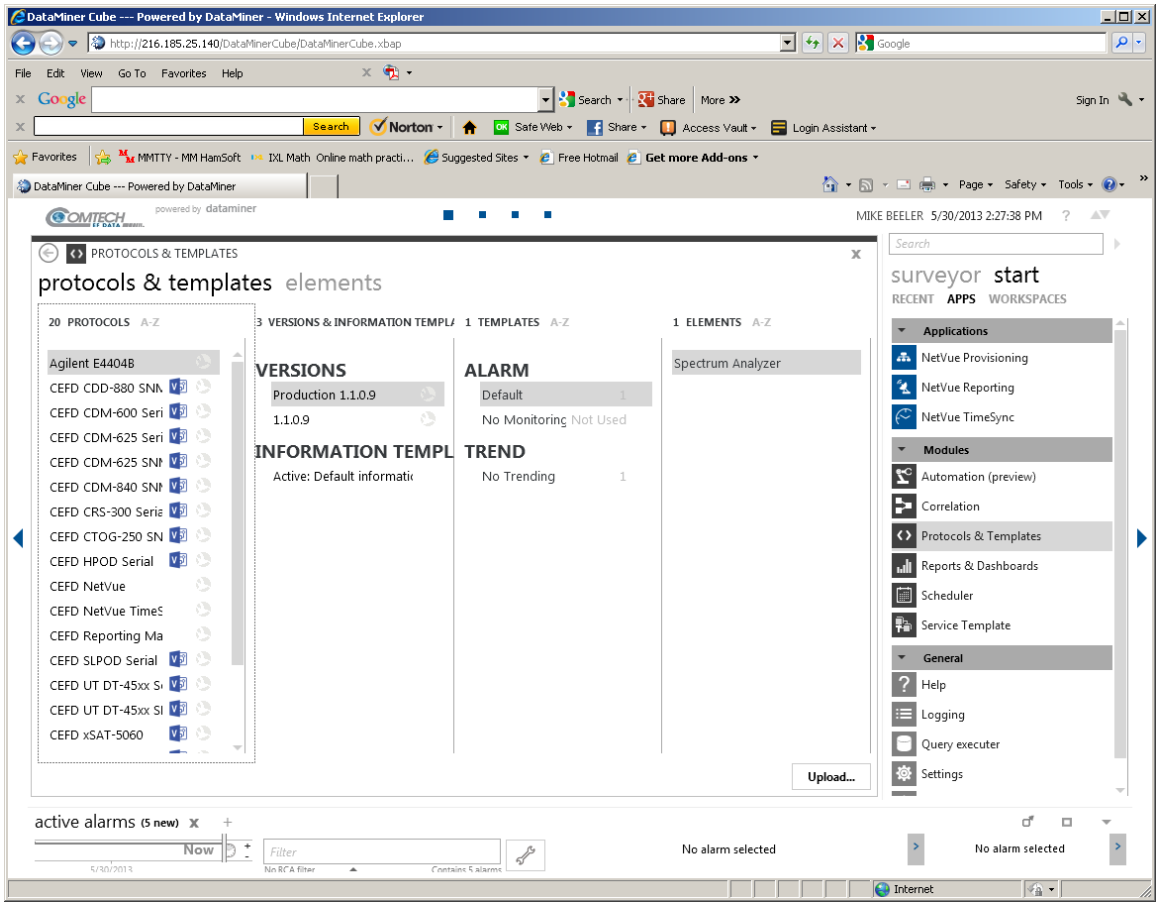


Figure 8-1. Protocols & Templates Page

8.1.3.1 Versions & Information Templates Column

This column shows the installed protocol and Production versions. The installed protocol version is associated with all the devices in the network automatically, using the related Production version.

Use a mouse right-click to do these tasks:

- **Open** a protocol
- **Delete** a protocol that is set as **Production**
- **Upload** (Add) a protocol version

8.1.3.2 Templates Column

The Templates column shows:

- Available Alarm and Trending templates
- Associations between protocol versions and templates

Use a mouse right-click to do these tasks:

- Open
- New
- Duplicate
- Delete
- Upload

8.2 Work with Protocols

In Cube, use the **Protocols & Templates** App to manage the protocols and customize the Alarm and Trending templates.

8.2.1 Add Protocols

1. In the right hand pane, click **Start**.

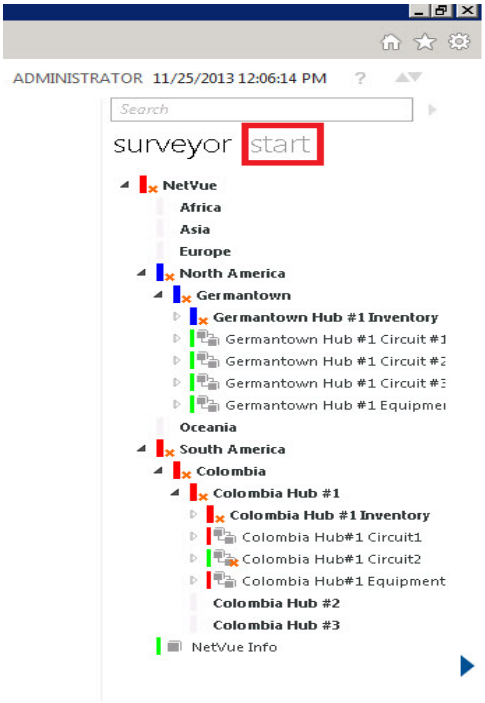


Figure 8-2. Start Selection

2. Select **Apps**, and then click **Protocols & Templates**.

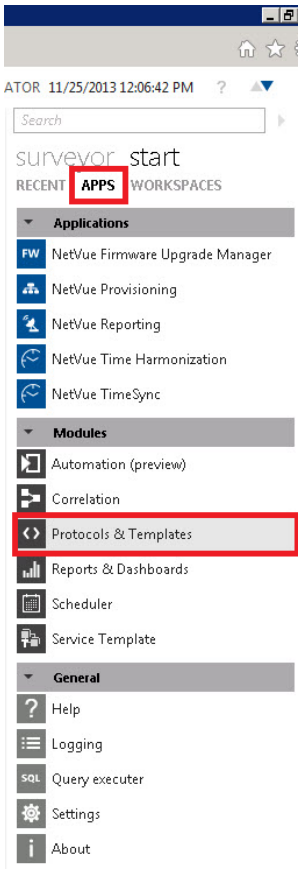


Figure 8-3. Protocols & Templates Selection

3. Right-click in the **Protocol** pane, select **Upload** and browse to the protocol XML file.

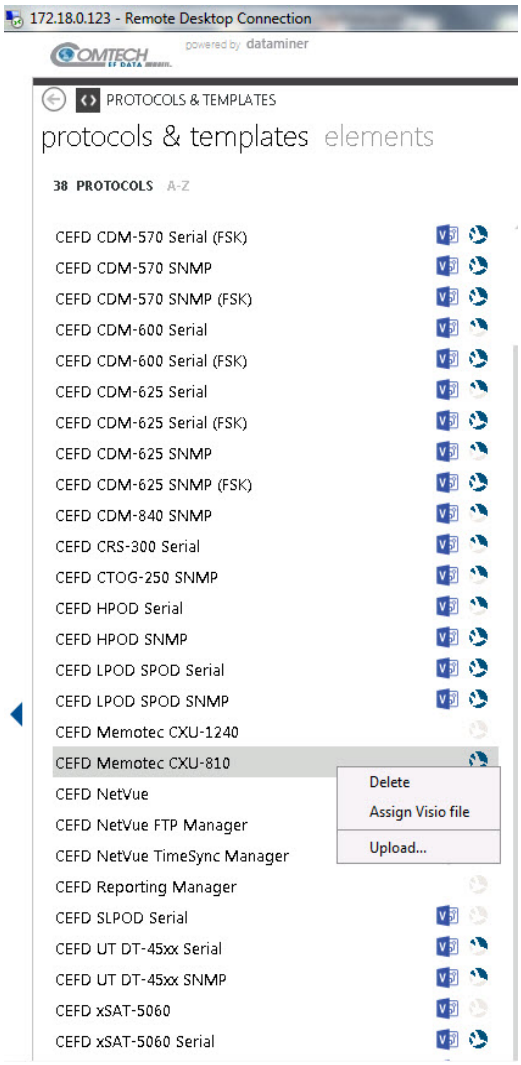


Figure 8-4. Upload Selection

8.2.2 Manage Protocol Versions

Production protocol is the default protocol for provisioned devices. You can specify other protocol versions for one device, or for a group of devices. This ability eases the rollout of new protocol versions into operations.

CEFD recommends that you evaluate a new protocol version on one or more devices before assigning it as the **Production** protocol for the whole network.

When you are ready to set the new protocol as the **Production** version, right-click on its version number and select **Set as production**. See Figure 8-5.

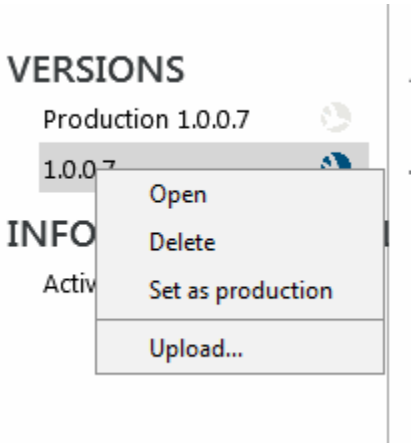


Figure 8-5. Protocol Version Management

8.2.3 Alarm and Trend Templates Association with Protocol

Every NetVue protocol version uses a separate set of Alarm and Trend Templates. Only the Production protocol has associated Default Alarm and Trend Templates.

When a new protocol version is first installed, it does not have associated Alarm or Trend Templates. However, once a new protocol version has been set as the Production version (see Section 8.2.1), it automatically adopts the Alarm and Trend Templates that were associated with the previous Production protocol.

In NetVue, a device can have no Alarm or Trend Templates. For such a device, history (trending data) is not kept and status changes do not cause alarms. On the screen, the color of this device is grey.

The quantity of associated devices shows to the right of the Alarm/Trend Template name. A list of these devices is in the right hand column. If an Alarm or Trend Template has no associated devices, **Not Used** shows instead of a number.

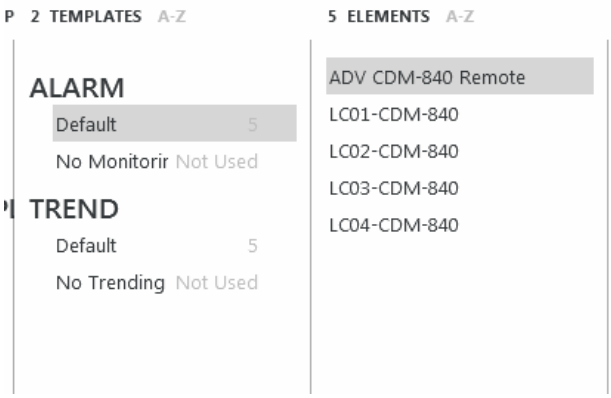


Figure 8-6. Alarm and Trend Templates

8.2.4 Protocol Editor Page

Double-click the protocol version to open the protocol editor page. This page shows the XML code for the protocol.

Do not change the XML code. The licensing mechanism protects this Skyline-signed code. Any change made to the code causes the protocol to stop functioning.

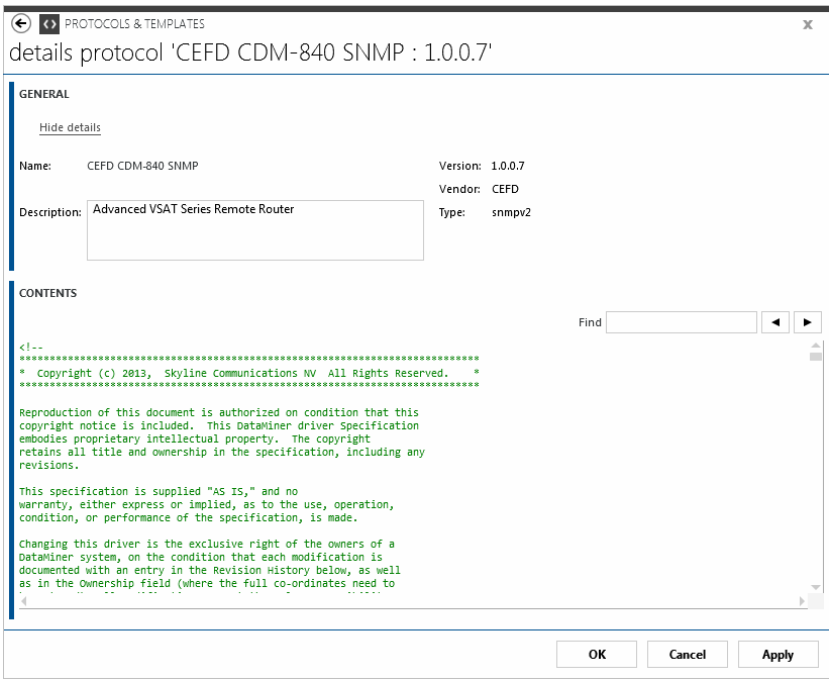


Figure 8-7. Protocol Editor Page

8.2.5 Alarm Template Editor Page

Double-click the Alarm Template name to open the template editor page.

The page shows only the parameters that are configured to generate an alarm. This is the default view.

To see the full list of parameters configured in the protocol, uncheck the **Only show monitored template parameters** box. See Figure 8-8.

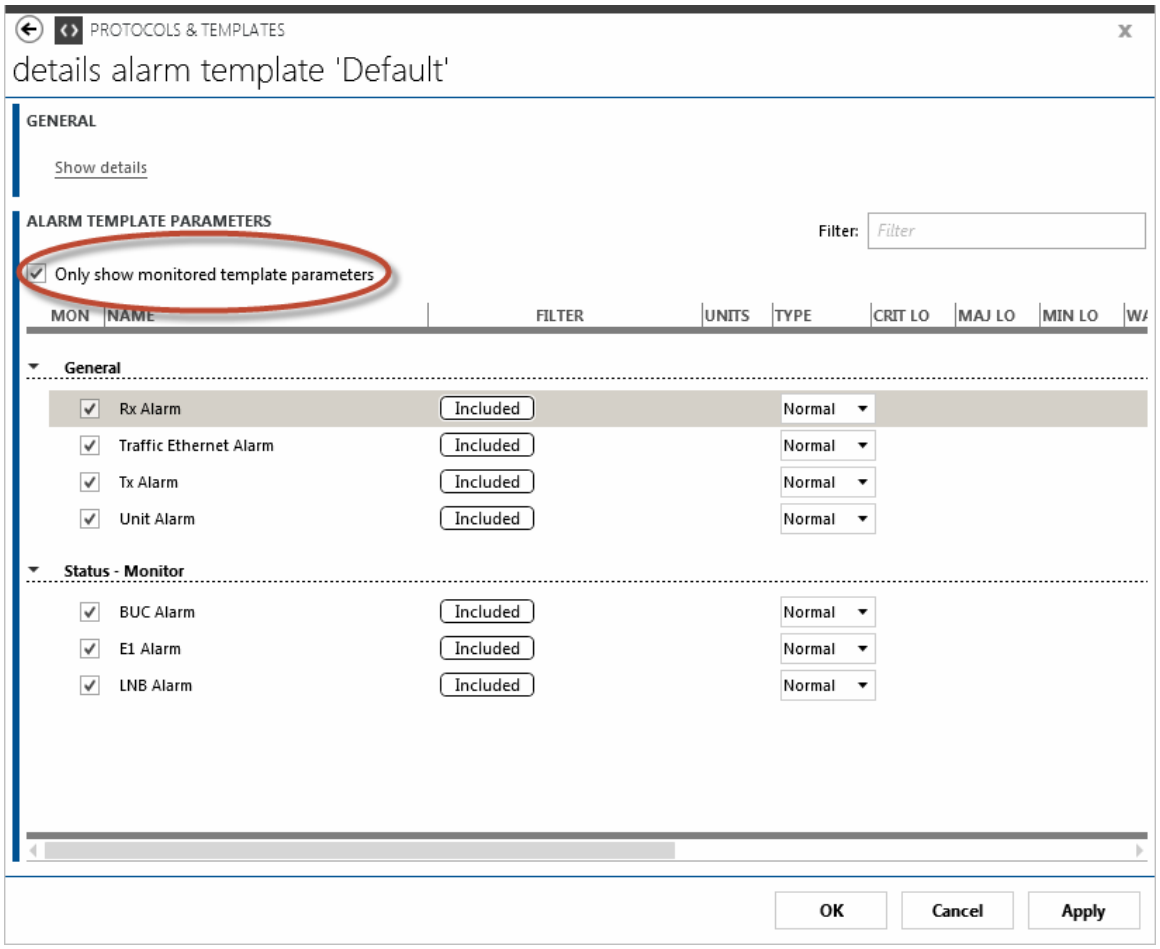


Figure 8-8. Alarm Template Editor Page

When you change the parameter selections and click **Apply**, the change is immediate.

Avoid causing problems in the operational environment. Copy the existing template to a new name, and then change the new template. Do not change the original template.

8.2.5.1 Duplicate an Alarm Template

1. Click a template's name.
2. Select **Duplicate**.
3. Enter a new name for the template copy.
4. Set the protocol version. See Figure 8-9.

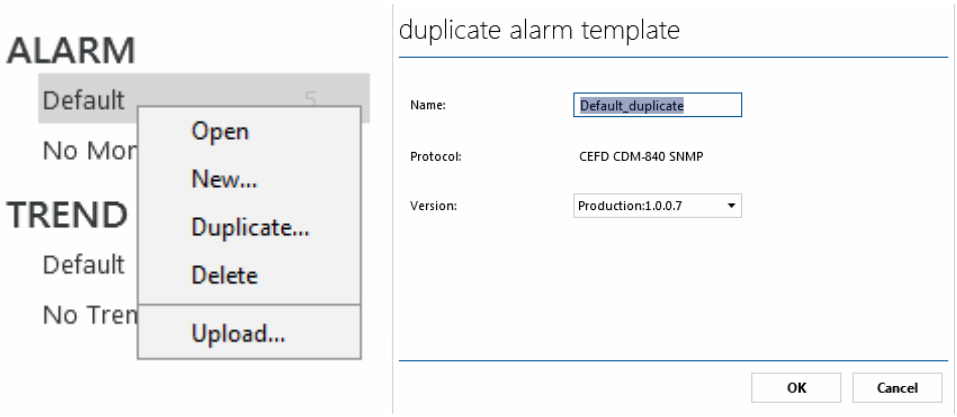


Figure 8-9. Duplicate Alarm Template

8.2.6 Add a New Element Manually

1. Left-click the **Surveyor** tab**.**
2. Right-click **NetVue** or a sub container.
3. Hold the mouse cursor over **New** to expand a new menu, then select **Element.**

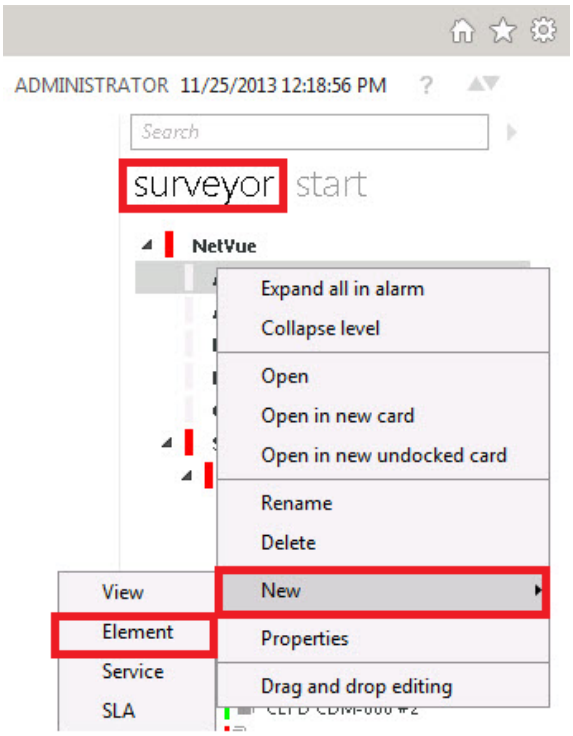


Figure 8-10. New Element Selection

4. Enter a **Name** for the element.
5. Select a **Protocol**. In this example, the NetPerformer protocol is selected.
6. Make sure the **Version** is the correct driver version.
7. Enter the **IP address** of the device.
8. Make sure all of the information is correct, and then click **Create**.

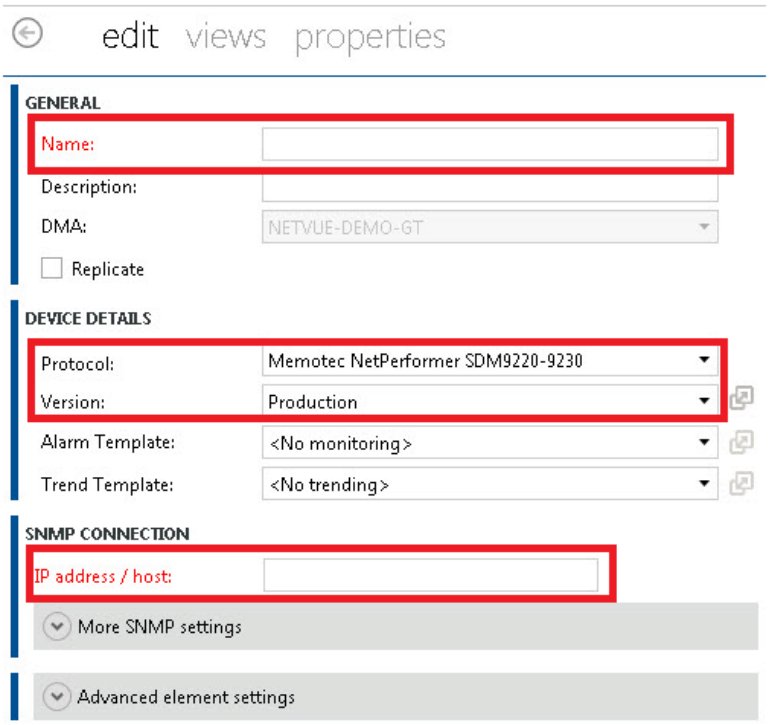


Figure 8-11. New Element Configuration

8.2.7 Remove a Microsoft Visio VDX File from a Protocol

1. In the **Protocol list** section, select the protocol.
2. At the bottom of the section, click **Remove vdx**.

8.2.8 Create an Information Overlay

1. In the **Protocol list** section, open the **Information** node of a protocol and select **Default Information**.
2. In the bottom-right corner of the **Information** tab, click **Save as**.
3. Enter the name of the new overlay file and click **Save**.
4. In the **Protocol list** section, select the newly created overlay file.
5. In the **Information** tab, make the necessary changes, and click **Save**.

8.2.9 Assign an Information Overlay to a Protocol Version

1. In the **Protocol list** section, open the **Versions** node of a protocol.
2. Select the protocol version to receive another information overlay assignment.
3. In the **General** tab, open the **Active information for this Protocol** selection box.
4. Select the information overlay.

Changing the information overlay is a protocol change. This change automatically causes NetVue to restart all Elements that use the changed protocol version.

BLANK PAGE

Chapter 9. ALARMS

9.1 Alarms

Your NetVue System continuously retrieves a wide variety of parameter values from all elements. When a parameter is monitored, each time a value is retrieved from an element, that value is compared to a user-defined threshold. Each time that threshold is violated, the NetVue System generates an alarm.

9.2 About Alarms

9.2.1 Alarm Types

Several types of alarms exist in NetVue. In addition to five alarm severity levels, there are also a number of special alarm types.

9.2.1.1 Alarm Severity Levels

There are four alarm levels, each indicated by a color, as well as one **Normal** level, which represents the expected value of a parameter during normal operations.

Table 9-1. Alarm Severity Levels

Severity Level	Default Alarm Color
Normal	Green
Warning	Blue
Minor	Cyan
Major	Yellow
Critical	Red

For the different alarm levels, you can assign high and low levels. For analog parameters, a high level alarm occurs when the parameter value exceeds the set alarm threshold, and a low level alarm occurs when the parameter falls below the set alarm threshold.

9.2.1.2 Special Alarm Types

Several special alarm types exist in NetVue:

- Alarms of the type **Error** and **Notice** refer to the functionality of the NetVue System itself.
- **Information** events are messages intended to inform users without raising an alarm.
- **Timeout** alarms indicate non-responding devices.
- **Masked** alarms, shown in purple, are hidden to prevent unnecessary follow-up.

9.2.1.2.1 Information Event

An information event is a message distributed throughout the NetVue System to draw attention to something. In the Alarm Console, these messages show in the default tab **Information Events**.

Typically, information events are broadcast to inform users when:

- A NetVue agent has been started or stopped.
- An alarm template has been changed.
- A protocol has been added or deleted.
- An Automation script has failed or finished successfully.

Default alarm color: gray - **gray**

You can also make NetVue generate Information Events when a discrete parameter reaches a user-defined value or when an analog parameter crosses a user-defined threshold.

9.2.1.2.2 Timeout

A timeout is a message that tells users when a timeout occurred for a particular element.

Timeout messages broadcast to tell users that a device no longer responds to the commands it receives from a NetVue agent.

Default alarm color: orange - **orange**

9.2.1.3 Alarm Type Priority

The different alarm types have their own priorities in NetVue.

Listed from highest to lowest priority:

Error, Timeout, Critical, Major, Minor, Warning, Masked, Normal, Notice, Information, Initial

Many different NetVue applications use these priorities:

- In the Surveyor, the icons get the alarm color with the highest priority
- In Alerter, the alarm with the highest priority is shown in a balloon first
- In the Alarm Console, if you sort alarms on severity, this order is used
- On the back of a view card, if you sort items in a view on severity, this order is used
- In the footer of a view card, the items in the view are shown in this order
- In Visual Overview, this priority determines the displayed alarm color

9.2.2 Alarm Linking

When the NetVue System detects that a parameter no longer has a normal value, it creates an alarm record with the following properties.

Table 9-2. New Alarm Properties

Property	Value
Owner	System
User Status	Not Assigned
Alarm Type	New Alarm
Status	Open

From that moment, every subsequent change to that alarm (severity changes, ownership changes, masking or unmasking, comments added, etc.) will cause the creation of a separate alarm record that replaces the original record.

As long as the parameter in question does not have a value that is considered normal, the **Status** property of these replacement records is **Open**. The moment the parameter has a normal value again, a final replacement record is created. The **Status** property of this last record will be "**Cleared**" or "**Clearable**", depending on the value of the "**AutoClear**" alarm setting.

Thanks to this method of alarm linking, almost every alarm in the NetVue System is represented by a series of linked alarm records that reflect an entire alarm life cycle.

9.2.3 Alarm Filters

NetVue uses the same standard filters throughout the system:

- To define the contents of alarm tabs in the Alarm Console.
- To define which alarms need to be forwarded to SNMP Managers.
- To define which alarms need a notification.

Alarm filters are stored in the NetVue System. They are always available, no matter from where you are in the system.

Three types of alarm filters are available:

- **Private**: a private filter is not available/visible to other users. This private filter is linked to your user account, and only available when you log on with that user account.
- **Public**: a public filter is available to other users and anybody can change this type of filter.
- **Protected**: a protected filter is available to other users, but only the user that created the filter can change it.

9.3 Alarms in the Cube

9.3.1 NetVue Cube Alarm Cards

An alarm card shows detailed information about an alarm. To open an alarm card in the NetVue Cube, right-click an alarm in the Alarm Console, and select **Open > Alarm Card**.

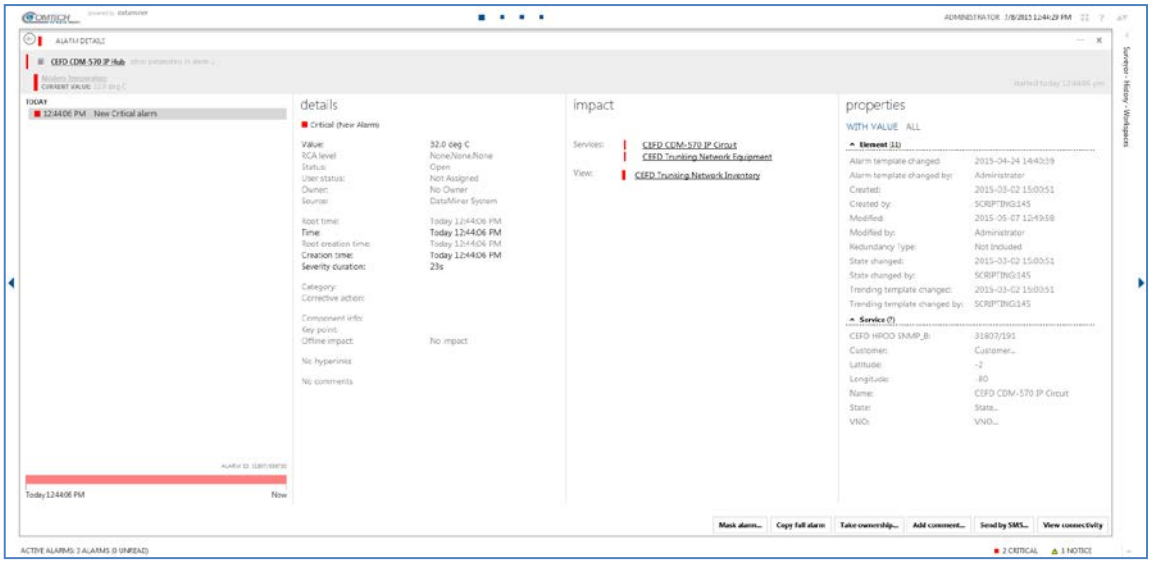


Figure 9-1. Alarm Card

The alarm card has three panes:

- The top pane shows general information about the alarm, such as which parameters are in alarm and when the alarm started.
- The pane on the left shows the history of the alarm. For correlated alarms, it also shows the source alarms.
- The large pane on the right has three tabs.

Table 9-3. Alarm Card

Tab	Description
Details	Details about the alarm, such as the current value of the parameter in alarm, the RCA level, the alarm status, any alarm comments, etc.
Impact	A list of all services and views the alarm has an impact on.
Properties	A list of properties that have been set for the alarm, or for views, elements or services it relates to.

At the bottom of the alarm card there can be several buttons:

Table 9-4. Alarm Card Options

Button	Description
Mask alarm	Allows masking of active alarms to prevent unnecessary follow-up, for instance when a device is intentionally manipulated for testing purposes
Unmask alarm	Unmasks an alarm that has previously been masked
Clear alarm	Allows the user to clear an alarm
Copy full alarm	Copies all properties of the alarm to the clipboard
Take ownership	Used to claim ownership of an alarm
Release ownership	Used to release ownership of an alarm, if you have previously claimed ownership
Forced release ownership	Forces the ownership of an alarm to be released, if a different user has previously claimed ownership
Add comment	Allows a user to add a comment, for instance, to communicate important information to other users
Send by SMS	Forwards an alarm record by SMS
View connectivity	Shows the connectivity chains of which the element is a part (one tab per chain)

Figure 9-2. Alarm Card Options

9.4 Change Ownership of Alarms

The **Alarm Ownership** feature allows unambiguous assignment of responsibility for individual alarm events, as well as tracking of those responsibilities.

When the NetVue System generates a new alarm event:

- The **Alarm Type** property is set to **New Alarm**
- The **Owner** property is set to **System**
- The **User Status** property is set to **Not Assigned**

9.4.1 Take Ownership of an Alarm

To show other users that you are aware of an issue and working on a resolution, you can take responsibility for an alarm record by taking ownership of it.

1. Right-click the alarm event in the **Active Alarms** tab of the Alarm Console, and select Take Ownership.

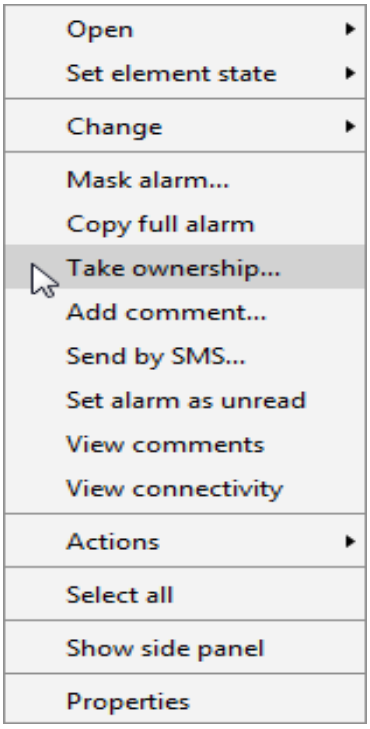


Figure 9-3. Take Ownership

2. In the **Take Ownership** window, enter a comment explaining why you are taking ownership of the alarm event.

Figure 9-4. Take Ownership Comment

When you take ownership of an alarm event, a new alarm record is added to the life cycle of that alarm event, and the property is set to **Acknowledged**. The new alarm records that are added to the life cycle of that alarm will have your user name in the **Owner** property.

9.4.2 Release Ownership of an Alarm

After having taken ownership of an alarm event, you can release ownership again in case you cannot resolve the alarm situation, or you no longer need to take ownership.

1. Right-click the alarm you currently own in the Alarm Console.
2. Select **Release Ownership**.

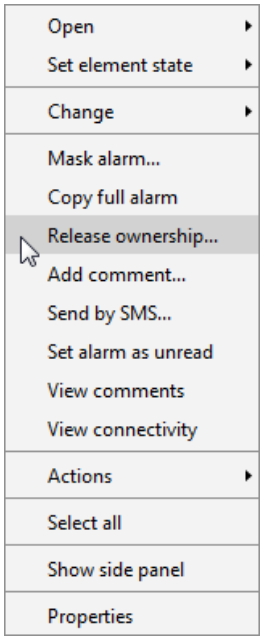


Figure 9-5. Release Ownership

By default, you can only release ownership of alarm events that you own. However, if you have the permission **Release ownership of another user**, you can release ownership of alarms that are owned by other users as well.

When you release ownership of an alarm event, an alarm record is added to the life cycle of that alarm event. Both the **Alarm Type** and **User Status** properties of that record are set to **Unresolved**. The **Owner** property of that record and all records added subsequently to the life cycle of the alarm will be set to **System,** until someone else takes ownership of the alarm.

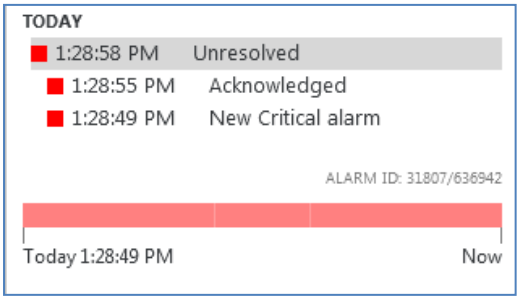


Figure 9-6. Alarm Life Cycle

9.4.3 Alarm Comments

Whenever users take or release ownership of alarm events, they can add a comment. Whether they do so or not, the NetVue System adds a comment automatically. This automatic comment shows who took or released ownership and when this occurred.

Figure 9-7. Alarm Comments

9.5 Mask/Unmask Alarms

Active alarms can be masked to prevent unnecessary follow-up.

You can mask Alarms that occur because a device is shut down for maintenance purposes, or its settings are changed for testing purposes.

This lets operators monitoring the NetVue System know that these alarms do not need intervention.

9.5.1 Mask an Alarm

To mask an alarm manually:

1. Right-click the alarm in the Alarm Console, and select **Mask alarm.**

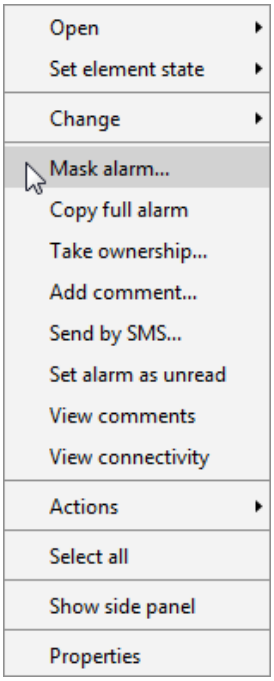


Figure 9-8. Mask Alarm

2. In the **Mask** dialog box, select whether to mask the alarm only, or to mask the element completely.

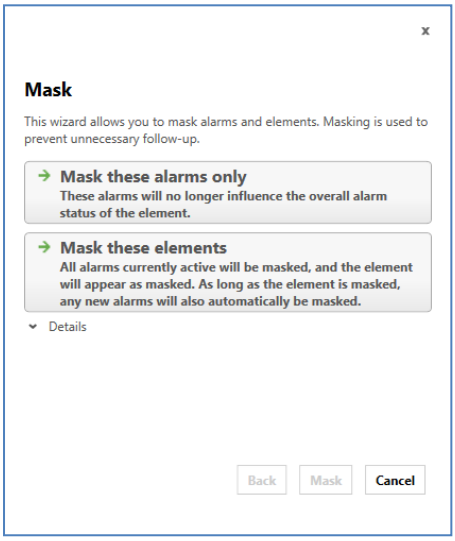


Figure 9-9. Mask Dialog Box

3. Choose the masking method:

   a. **Mask the alarm for a limited period of time**: You must specify the number of minutes during which the alarm is masked. After this time, it is unmasked automatically. Even if it is cleared and reoccurs afterwards, it remains masked for the specified time.

   b. **Mask alarm until cleared or unmasked**: This masks the alarm until it is cleared. When cleared, it is unmasked automatically.

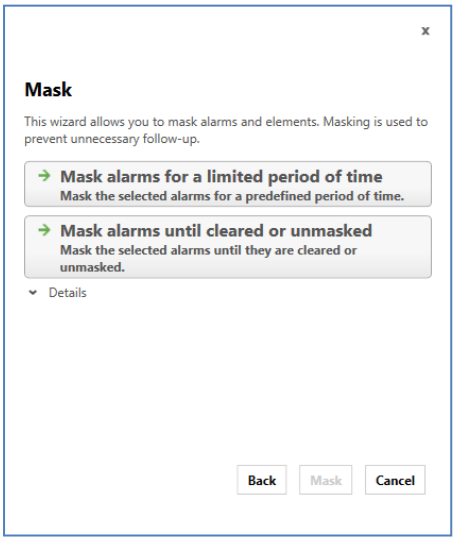


Figure 9-10. Masking Method

4. Enter a comment. It will be stored in the **Comment** field of the new alarm record.

A new alarm record is added to the life cycle of the alarm. Its status and alarm type are set to **Mask**. The masked alarm no longer shows in the **Active alarms** tab. Instead, it is added to the **Masked alarms** tab.

9.5.2 Unmask an Alarm

You can manually unmask masked alarms any time. You can mask alarms again, such as when you want to change the masking method.

To unmask an alarm manually:

1. Right-click the alarm in the **Masked alarms** tab of the Alarm Console.
2. If only the selected alarm is masked, select **Unmask alarm**.
3. If the element is masked, select **Unmask element**.

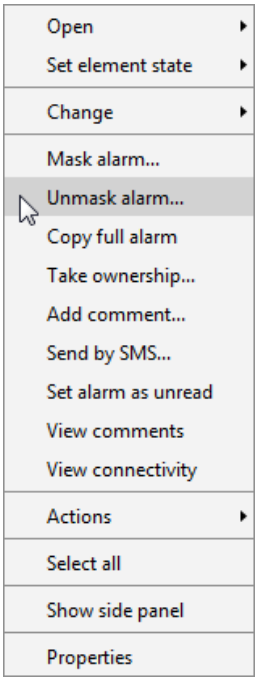


Figure 9-11. Unmask Alarm

4. Enter a comment. It will be stored in the **Comment** field of the new alarm record.

When you unmask an alarm, a new alarm record is added to its alarm life cycle. The status is set to **Open** and the alarm type is set to **Unmask**. The masked alarm no longer shows in the **Active alarms** tab. Instead, it is added to the **Masked alarms** tab.

9.6 Add Comments to an Alarm

To leave useful information for other users, you can add comments to alarm records.

However, you cannot add comments to cleared alarms, but you can see existing comments on cleared alarms.

1. Right-click the alarm in the Alarm Console.
2. Select **Add comment.**
3. Enter the comment in the dialog box and click **Add comment.**

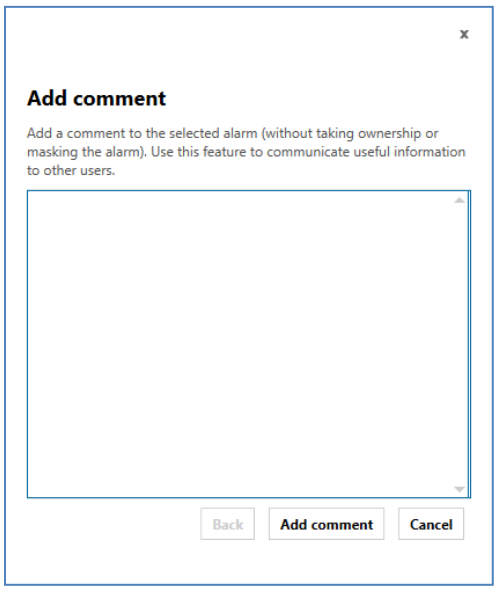


Figure 9-12. Add Comment

When you add a comment to an alarm, the new alarm record has its **Alarm Type** set to **Comment Added**. The comment is stored in the **Comment** field, along with your user name and the time stamp.

9.6.1 View Alarm Comments

There are several ways you can see comments on an alarm:

- Right-click the alarm in the Alarm Console, and then select **View comment.** (See Figure 9-13)
- Add the column **Comment** to the Alarm Console. (See Figure 9-14)
- Open the alarm card to read the comments at the bottom of the **details** tab. (See Figure 9-15).

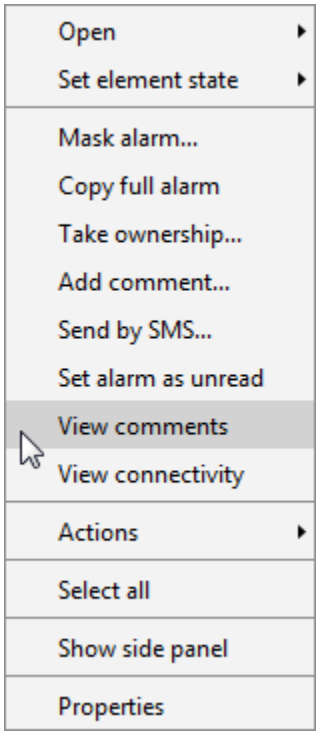


Figure 9-13. Right-click View

Figure 9-14. Comment Field

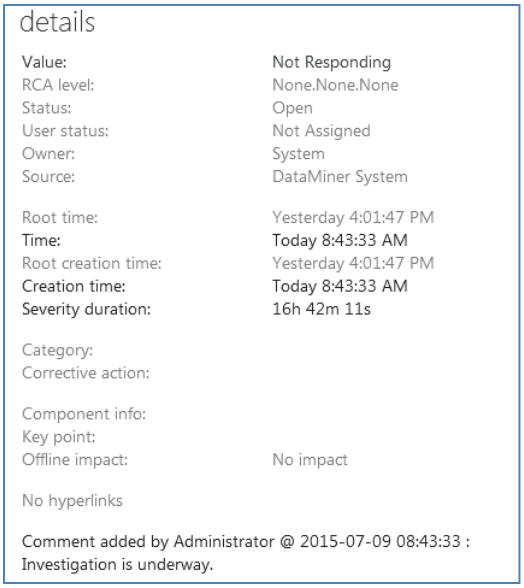


Figure 9-15. Details Tab

9.7 Change the Alarm Read Status

In the **Alarm Console**, a new, unread alarm record shows in bold typeface. When someone selects it for more than two seconds, it is considered read, and the bold typeface changes to regular typeface.

The read/unread status of an alarm is a user setting linked to the user account. As a result, read/unread statuses shown on your screen can differ from those shown on another user's screen.

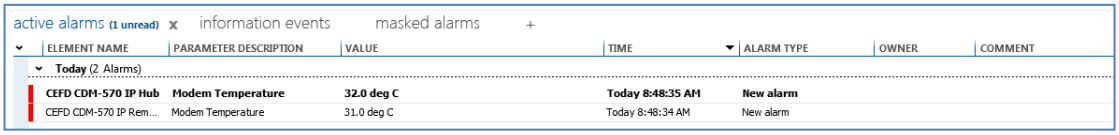


Figure 9-16. Read Status

Adjacent to the name of an alarms tab, the number of unread alarms shows in parentheses. For example, **active alarms (1 unread).**

To change an alarm record from **read** to **unread**, right-click the alarm record and click **Set alarm as unread**.

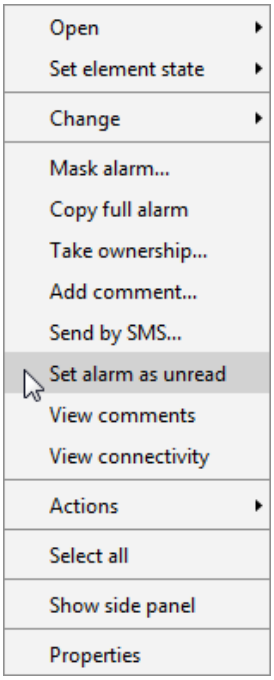


Figure 9-17. Set as Unread

9.8 Change Custom Alarm Properties

9.8.1 Add a Custom Alarm Property

1. In the **Alarm Console**, right-click the alarm and select **Properties.**
2. Go to the **custom** tab.

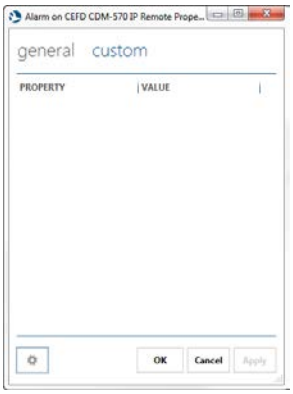


Figure 9-18. Custom Tab

3. In the lower left corner, click the settings button and select **Add.**

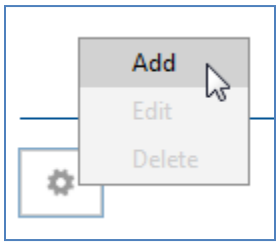


Figure 9-19. Add Custom

4. Enter a name for the new custom property.
5. Clear or select the checkbox **Make this property available for alarm filtering**, depending on whether you want to make it possible to use the property in Alarm Console columns, in NetVue filters and in NetVue Correlation.
6. Specify a property format.
    a. Select **No value format** if you do not want to restrict the property value in any way.
    b. Select **Format (regular expression)** to restrict the property value by means of a regular expression.
    c. Select **Possible values** and specify a number of allowed values.

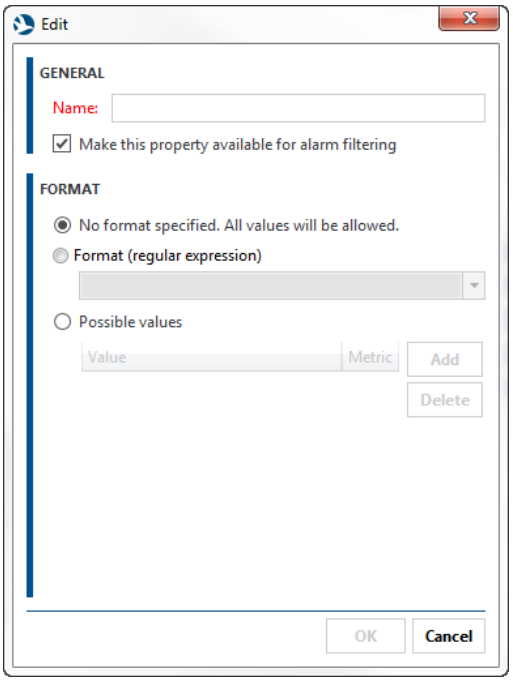


Figure 9-20. Edit Custom

9.8.2 Delete a Custom Alarm Property

1. In the **Alarm Console**, right-click the alarm and select **Properties.**
2. Go to the **custom** tab.
3. Select the property you want to delete.
4. In the lower left corner, click the settings button and select **Delete.**

9.8.3 Edit Custom Alarm Properties

If an alarm tab contains columns showing custom alarm properties, you can change the values of those properties:

1. In a column with a custom alarm property, click the pencil next to the property value
2. Enter the new value.

If no such columns are showing, you can still change any available custom alarm properties:

1. Right-click an alarm and click **Properties**.
2. In the Properties dialog box, select the **custom** tab.
3. Enter the property value and click **OK**.

You can edit advanced settings of a custom alarm property also, such as the property format:

1. In the Alarm Console, right-click the alarm and select **Properties**.
2. Go to the **custom** tab.
3. Select the property you want to edit.
4. In the lower left corner, click the settings button and select **Edit**.

9.9 Clear Alarms

On a NetVue agent, alarms are cleared automatically, by default. However, if you set the AutoClear system setting to **false**, then all alarms must be cleared manually.

9.9.1 Clear an Alarm Manually

To clear an alarm manually:

1. In the **Alarm Console**, right-click the alarm and select **Clear alarm.**
2. In the **Clear alarm** window, add a comment if necessary.
3. Click the **Clear alarm** button.

9.9.2 AutoClear Setting

You can configure the default **AutoClear** setting in the **C:\Skyline DataMiner\MaintenanceSettings.xml** file.

If you set **AutoClear** to **FALSE**, alarms will not be cleared automatically. Instead, someone must clear them manually.

9.10 Alarm Templates

An alarm template is an XML file that contains all alarm thresholds for all parameters defined in a particular NetVue protocol. The alarm template is an overlay file that overrides the default alarm thresholds in a NetVue protocol.

You can assign an alarm template to an element type. In other words, you assign the alarm template to all elements sharing the same NetVue protocol.

You can create unlimited alarm templates for every NetVue protocol. Maintain multiple alarm templates and switch among them easily. Change alarm thresholds quickly.

Additionally, combine alarm templates into template groups to build alarm template hierarchies. This allows alarm thresholds for one or more parameters to be overruled, without having to change the base template.

9.10.1 Manage Alarm Templates

9.10.1.1 Create an Alarm Template

To create a new alarm template:

1. Go to **Start > Apps > Protocols & Templates.**
2. In the first column, select a protocol.
3. In the second column, select a protocol version.
4. In the third column, right-click under Alarm, and select New.

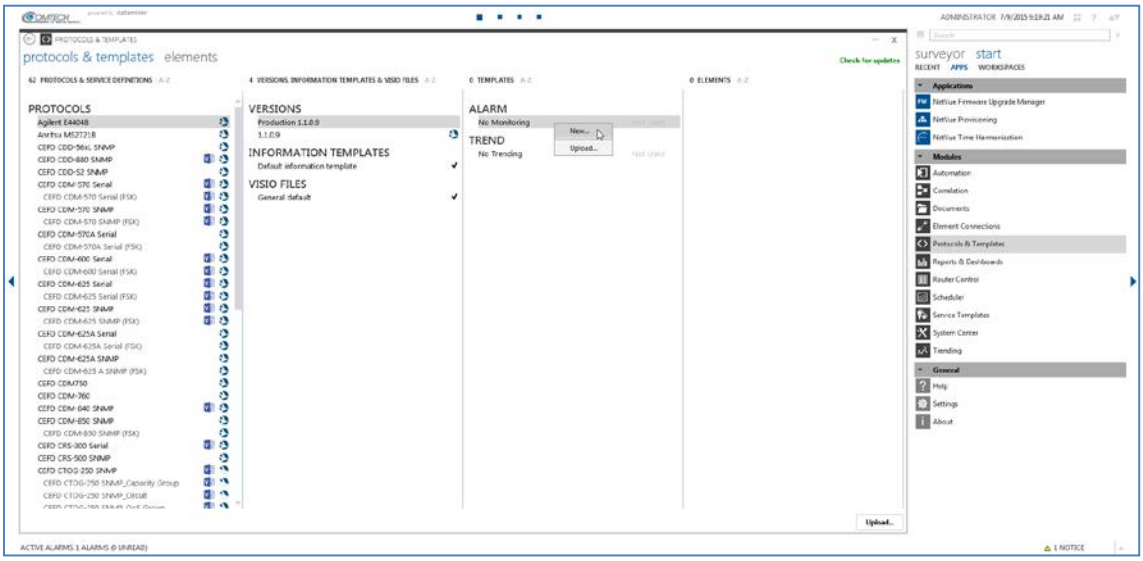


Figure 9-21. New Template

5. In the **New alarm template** dialog box:
    a. Keep **Alarm Template** selected.
    b. Enter a template name.
    c. Make sure the protocol and protocol version are correct. Change them, if necessary.
    d. Click **OK.**

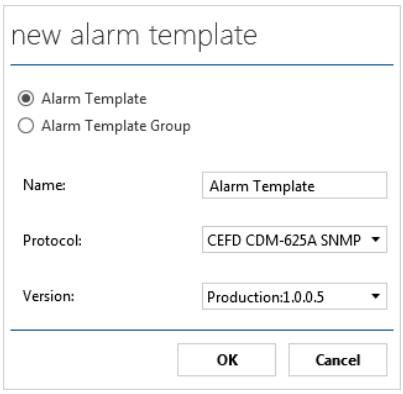


Figure 9-22. New Alarm Template

9.10.1.2 Upload an Alarm Template

To upload an existing alarm template for a particular protocol version:

1. Go to **Start > Apps > Protocols & Templates.**
2. In the first column, select the protocol.
3. In the second column, select the protocol version.
4. Under Alarm in the third column, right-click an alarm template and select Upload.
5. Browse to the applicable alarm template and click **Open.**

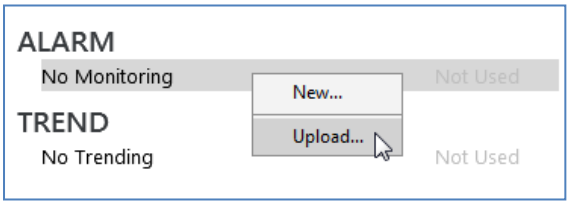


Figure 9-23. Upload Template

9.10.1.3 Assign an Alarm Template

There are two ways to assign an alarm template to an item:

1. In the Surveyor:
    a. Right-click the item that needs an alarm template assigned, and click **Edit.**
        i. In the **Edit** tab, go to the **Device Details.**
        ii. In the **Alarm Template** selection box, select the alarm template.
        iii. Click **Apply.**

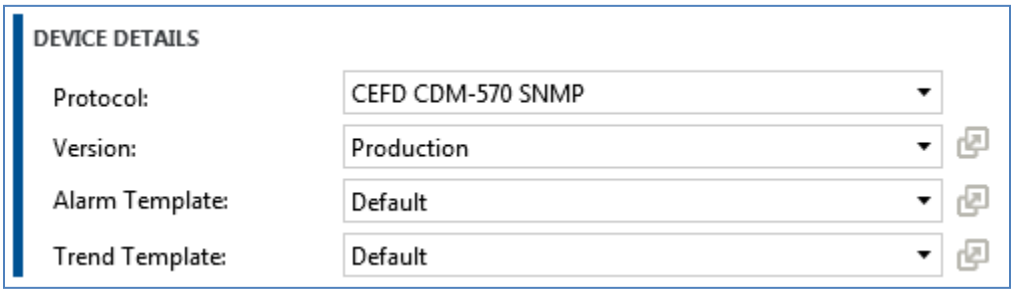


Figure 9-24. Assign Template (Surveyor)

2. In the Protocols & Templates app:
    a. In the first column, select the protocol of the item that needs an alarm template assigned.
    b. In the **Versions** section, select the protocol version of the item.
    c. In the **Alarm** section, select the alarm template.
    d. Right-click in the **Elements** section, and select **Assign template.**

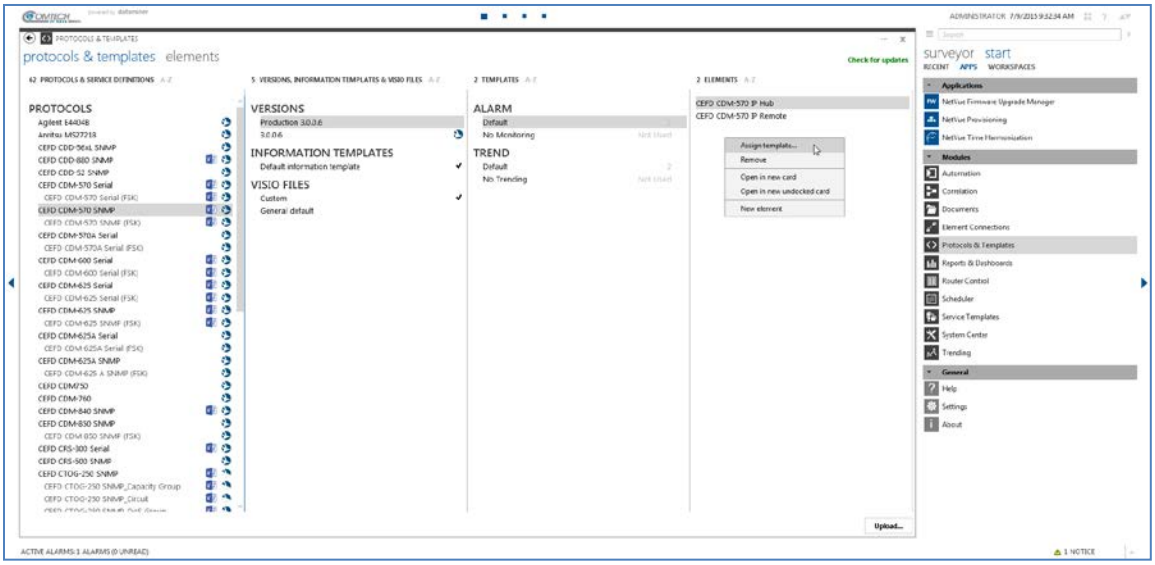


Figure 9-25. Assign Template (App)

    e. In the **Assign template** window, use the **Add >>** and **Remove >>** buttons to assign the template to specific items.

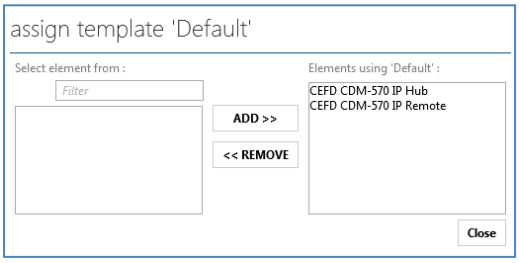


Figure 9-26. Assign Template Add/Remove Page

9.10.1.4 Delete an Alarm Template

To delete an existing alarm template for a specific protocol version:

1. Go to **Start > Apps > Protocols & Templates**.
2. In the first column, select the **protocol**.
3. In the second column, select the **protocol version**.
4. Under **Alarm** in the third column, right-click the alarm template and select **Delete**.

9.10.2 Configure an Alarm Template

To configure an alarm template, you must first open the template editor.

There are two ways to do this:

1. Go to the **Protocols & Templates** app, right-click the template and select **Open.**

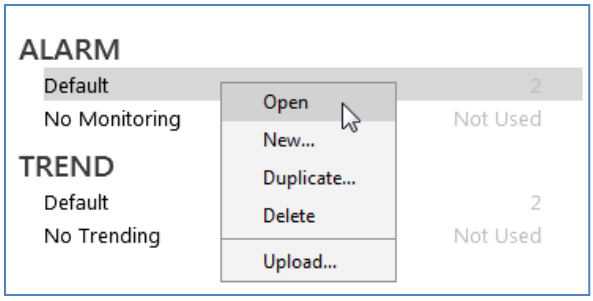


Figure 9-27. Configure Alarm Template - Open Template

2. Right-click an item in the Surveyor and select **View > Alarm template.**

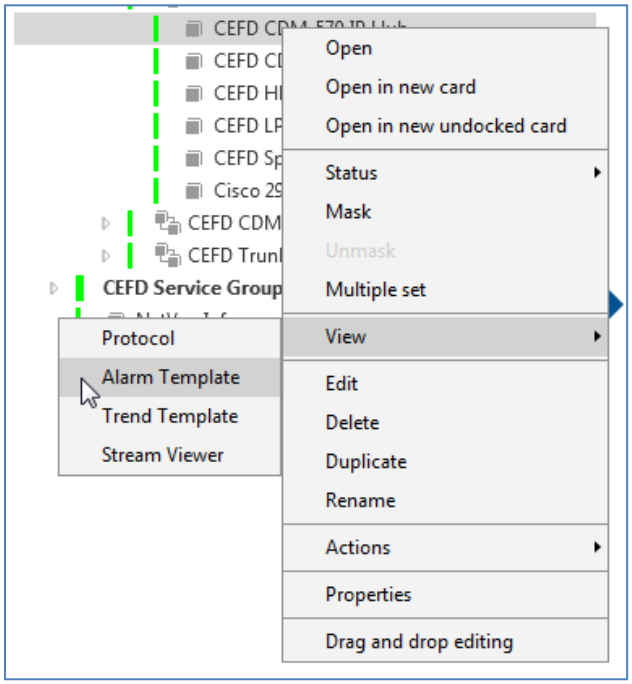


Figure 9-28. Configure Alarm Template - View Template

9.10.2.1 Configure Alarm Thresholds

To configure the alarm thresholds for analog parameters:

1. Enable alarm monitoring for a parameter:
    a. In the first column, select the check box next to the parameter.
2. Set alarm severities:
    a. Enter the values for alarm severities.
    For discrete or hybrid parameters, you can choose values from a drop-down list.
    b. You can specify multiple values per alarm severity.
    In this case, the existing alarm is updated with a new value each time it crosses a new threshold.
    c. It is not necessary to enter a value for each severity level.

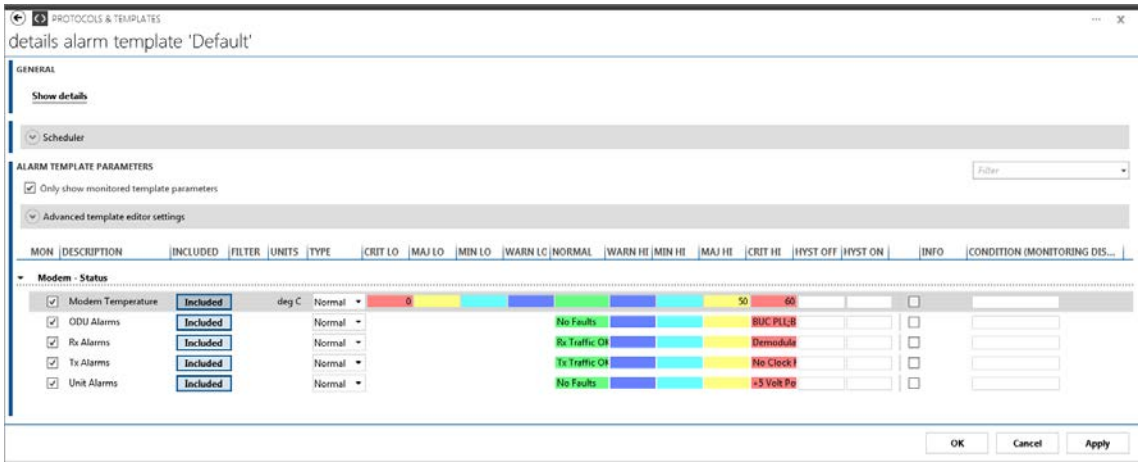


Figure 9-29. Configure Alarm Thresholds

9.10.2.2 Alarm Conditions

In the **Condition** column, you can add conditions for the alarm triggering of select parameters. By specifying such a condition, you can make sure that a parameter is not monitored when another parameter of the same element has a specific value or alarm state.

When you specify a condition for a parameter in an alarm template, that parameter is monitored only when the condition is false.

Click in the selection box in the **Condition** column to create and manage conditions.

1. Create a new condition:
    a. Select <New>. The window Add condition to [template name] opens.
    b. Enter a name for the condition next to Name.
    c. Click Select a filter to create a new filter.
    d. Set up the filtering parameters:
        i. To filter on severity, click **Value**, and select **Severity** instead.
        ii. Click **Equal to** and select one of the options: **Equal to**, **Not Equal to**, **Greater than**, or **Less than**.
        iii. Select or enter the severity or value.
    e. Optionally, click **Add filter** to create more filters and combine them using logical operators (AND, OR).
    f. When finished, click **OK**.

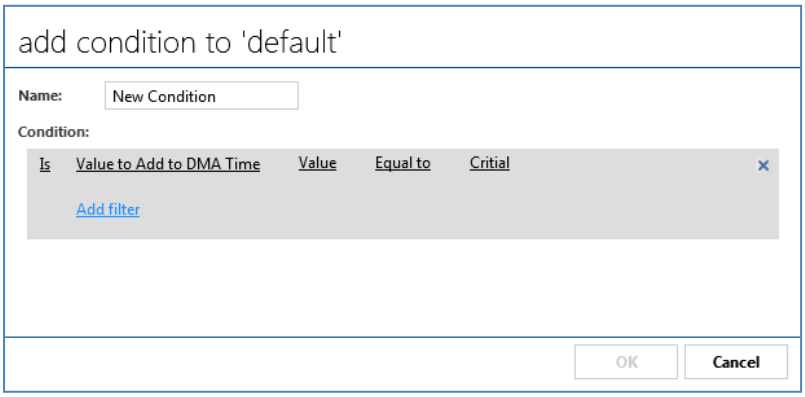


Figure 9-30. Add Alarm Condition

2. Select an existing condition, if available.
    a. If necessary, click the pencil icon next to the selected condition to modify it.
3. Remove a condition
    a. Select **<No condition>**, or click the x next to the condition.
4. Add an additional condition for the same parameter.
    a. Hold the mouse cursor over a condition, then click the plus sign **+** that shows next to the condition.

9.10.2.3 Set the Alarm AutoClear Options

For each parameter, you can set whether or not alarms are cleared automatically, or if the system default settings are applicable.

1. Click **Advanced template editor settings**.
2. Select the option Allow override of parameter autoclear.
   An extra column shows in the template editor.
3. To override the autoclear setting for a parameter:
   a. In the last column for that parameter, select **True** or **False**.

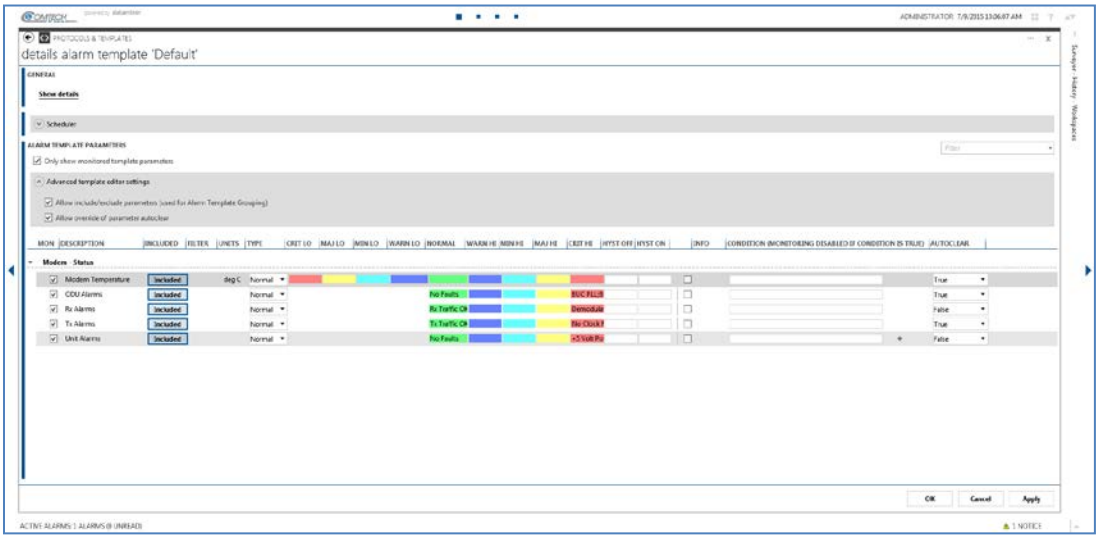


Figure 9-31. Alarm AutoClear Setting

9.10.2.4 Schedule an Alarm Template

In the NetVue Cube, you can schedule an alarm template so that it is active only at certain times. For example, you can use a schedule to make sure a specific alarm template is active only on weekdays.

To schedule an alarm template:

1. In the alarm template editor, click the down arrow that is adjacent to **Scheduler**. This expands the **Scheduler** section.
2. Select **Template is only active on**.
3. For every day, or time period on a day, that you want to schedule:
    a. Click **Add schedule.**
    b. Select a day of the week.
    c. Enter a time in the format HH:mm in the **begin** and **end** fields.

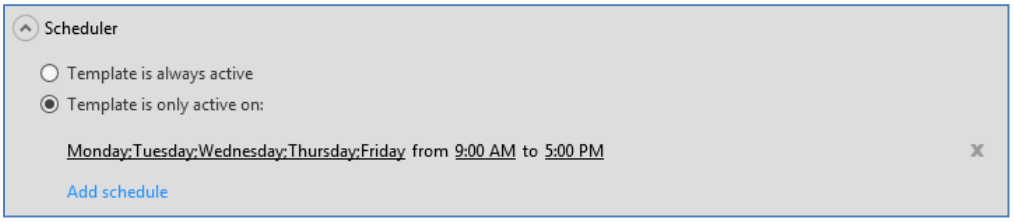


Figure 9-32. Alarm Template Scheduler

9.10.3 Change the Alarm Range for One Parameter

You can change the alarm range for a parameter quickly. Do this from the Alarm Console, or from a parameter card. From either location, you go to the ALARM RANGE editor.

1. In the Alarm Console:
    a. Right-click an alarm for a parameter.
    b. Select **Change > Alarm range.**

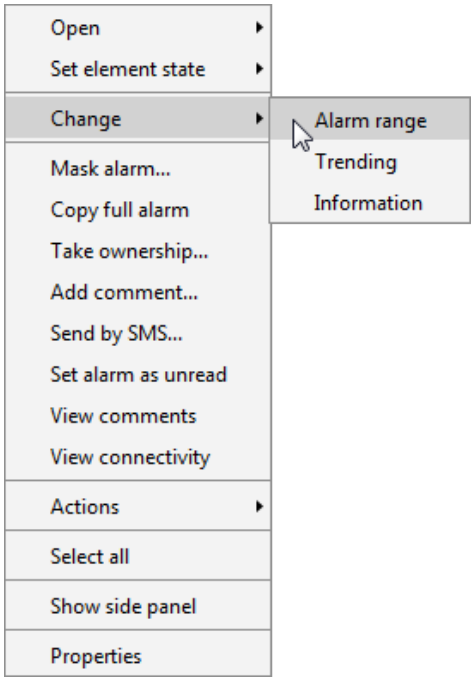


Figure 9-33. Change Alarm Range (console)

2. On a parameter card:
    a. Click the … icon in the top right corner.
    b. Select **Change alarm range.**

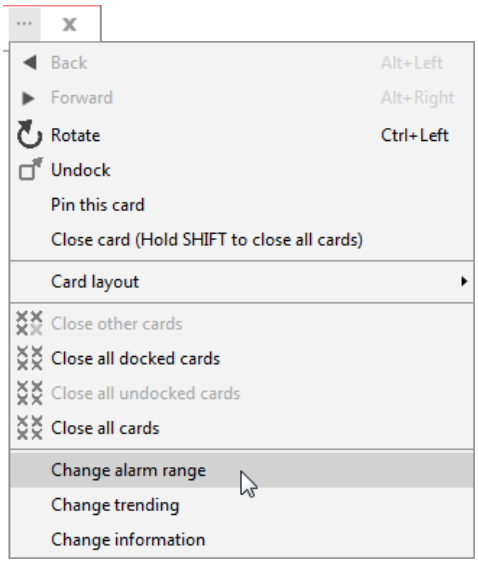


Figure 9-34. Change Alarm Range (card)

3. In the ALARM RANGE editor, you can do these tasks:
    - Clear the **Monitored** checkbox to stop monitoring the parameter.
    - Enter different values for the alarm thresholds.
    - Select **Info** and enter a parameter value. Whenever the parameter gets this value, an information event is generated.

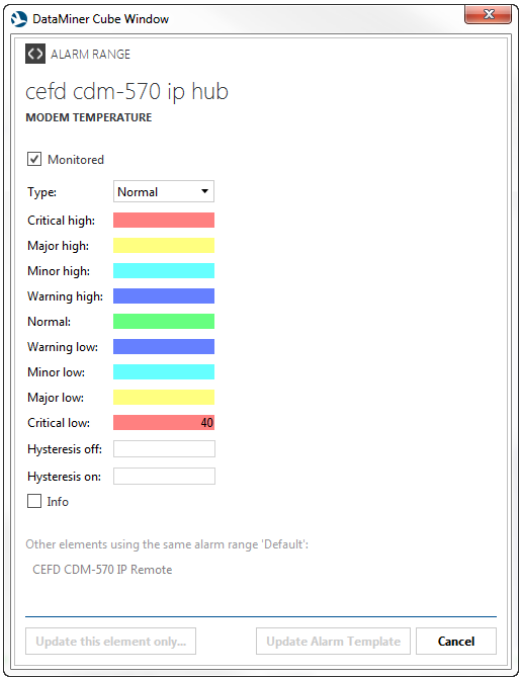


Figure 9-35. Alarm Range Editor

At the bottom of the window, an information message shows you other elements that use the same alarm range.

To save your changes, you have two options:

- To change the alarm range for all elements that use the same template, click **Update Alarm Template**.
- To change the alarm range for this element only, click **Update this element only**. In this case, a copy of the alarm template is made, and you must enter a name for this new alarm template.

9.10.4 Alarm Template Groups

You can combine Alarm templates into alarm template groups. Using these groups, you can build alarm template hierarchies. The hierarchies allow alarm thresholds for one or more parameters to be overruled, without any need to change the base template.

In this example of an alarm template group, assume that you create a template group with three alarm templates (1, 2 and 3). You assign this group to a protocol with five parameters (A, B, C, D and E).

The order of the alarm templates in a template group is very important, because every alarm template in the template group overrules the one below it.

This table shows which parameters will be monitored and how.

Table 9-5. Alarm Template Groups

Template Group	Parameter A	Parameter B	Parameter C	Parameter D	Parameter E
Template 1	Unspecified	Unspecified	Not Monitored	Unspecified	Unspecified
Template 2	Not Monitored	Unspecified	Monitored (Threshold 350)	Monitored (Threshold 400)	Unspecified
Template 3	Monitored (Threshold 100)	Monitored (Threshold 200)	Monitored (Threshold 300)	Not Monitored	Unspecified
Group Result	Not Monitored	Monitored (Threshold 200)	Not Monitored	Monitored (Threshold 400)	Not Monitored

In this example, Parameter C is monitored in both templates 2 and 3, with different threshold values. It is not monitored in template 1. Therefore, Parameter C will not be monitored, because template 1 overrules the other templates.

9.10.4.1 Create an Alarm Template Group

To create a new alarm template group:

1. Go to **Start > Apps > Protocols & Templates**
2. In the first column, select a protocol.
3. In the second column, select a protocol version.
    a. For each alarm template to be added to the group:
    b. Right-click the alarm template you want to add, and select **Open.**
    c. Click **Advanced template editor settings.**
    d. Select **Allow include/exclude parameters (used for Alarm Template Grouping)**.
    An extra column, **Included**, shows in the template editor.
    e. In the **Included** column, click the **Included** button for each parameter that must be included in the alarm template group.
    f. Click **OK.**

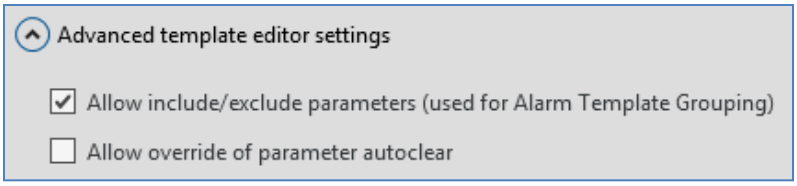


Figure 9-36. Include Group

4. In the Protocols & Templates app:
    a. Right-click in the third column, under **Alarm**.
    b. Select **New.**
5. In the **New alarm template** dialog box:
    a. Select **Alarm Template Group.**
    b. Enter a template group name.
    c. Make sure the protocol and protocol version are correct. Change them, if necessary.
    d. Click **OK.**

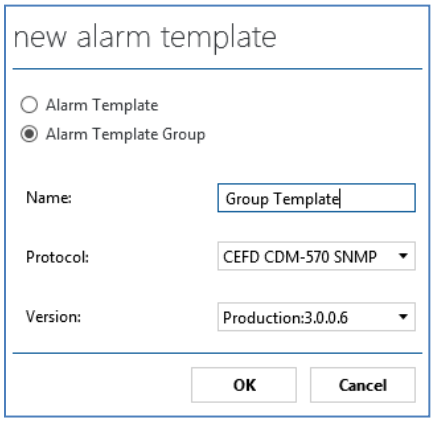


Figure 9-37. New Template Group

6. In the template group editor, click **Add Alarm Template**.
7. Repeat until all necessary templates are included in the group.
8. To change the order of the templates:
    a. Hold the mouse cursor over an alarm template.
    b. Click the small up and down arrows.
9. To remove an alarm template from the group:
    a. Hold the mouse cursor over the alarm template.
    b. Click the **x**.
    c. Click **OK**.

Chapter 10. REPORTS & DASHBOARDS

10.1 NetVue Reporter

In the NetVue Cube, built-in reports are available on several types of cards, as well as in the Reports & Dashboards app. In addition, you can create custom reports with the report template builder.

NetVue Reporter is a powerful, web-based tool that allows you to generate graphical reports showing a multitude of statistical data and operational metrics.

With a click of a button, you can get an overview of the top ten devices generating the majority of alarm messages, detailed information about the duration of alarm events, the distribution of alarms over time, etc.

In addition, thanks to a comprehensive library of JScript functions, report data can be incorporated into an existing third-part web environment. This allows operators, for example, to publish network management information onto intranet web pages without the need to grant users access to the actual network management environment.

10.2 Reports Page on a Card

Many cards in the NetVue Cube have a Reports page.

- On a View or Service card, go to the data display side of the card, and select **Reports**. (See Figure 10-1.)
- On an Element card, go to the data display side of the card, and choose **Reports** from the drop-down menu. (See Figure 10-2.)
- For reports on one particular parameter, on the data display side of an Element card, double-click a parameter and then go to the **Details** tab. (See Figure 10-3.)

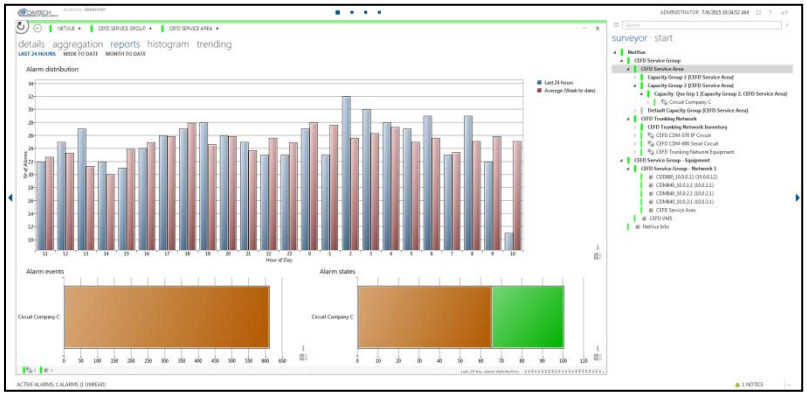


Figure 10-1. View/Service Reports

Figure 10-2. Element Reports

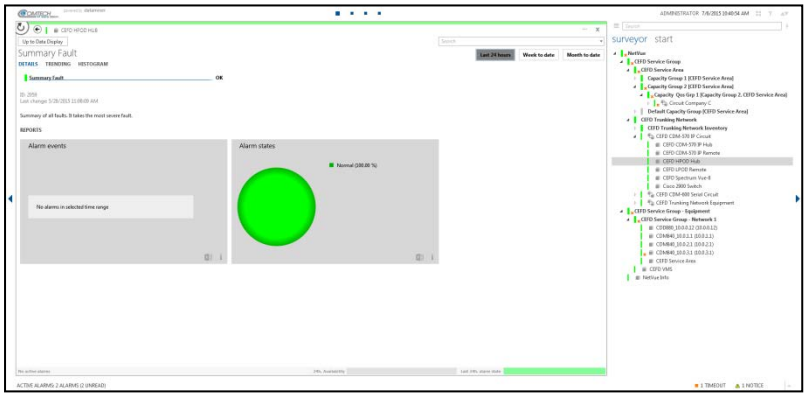


Figure 10-3. Parameter Reports

10.2.1 Reports Page Overview

On the Reports page, depending on the type of card, a number of graphs can show alarm information for a particular time span.

- **Alarm distribution** – colored bars show the actual alarm distribution compared to the average distribution
- **Alarm events** – visual representation of the number of alarm events. On a View card, a graph is shown for each element with alarm events in the given time span.
- **Alarm states** – visual representation of the dominant alarm states. On a View card, a graph is shown for each element with alarm events in the given time span.
- **Time line** – a bar with the alarm colors of alarm events as they occurred in the given time span. This graph is not included on View cards.

To change the time span represented in the graphs, click one of the buttons at the top right of the screen:

- Last 24 hours
- Week to date
- Month to date

Figure 10-4. Time Span

In the bottom right corner next to each of the graphs, an "i" icon is shown. Hold the mouse cursor over the icon for more information about the graph.

10.2.2 Export the Report Information

For each of the graphs, you can export the information as a .csv file.

To do so:

1. Click the spreadsheet icon in the bottom right corner next to the graph.
2. Browse to the location where you want to save the exported file and click **Save**.

10.3 Built-in Reports

To see the built-in reports in the Cube:

1. Go to the **Reports** app.
2. Go to **Start > Apps > Reports & Dashboards.**

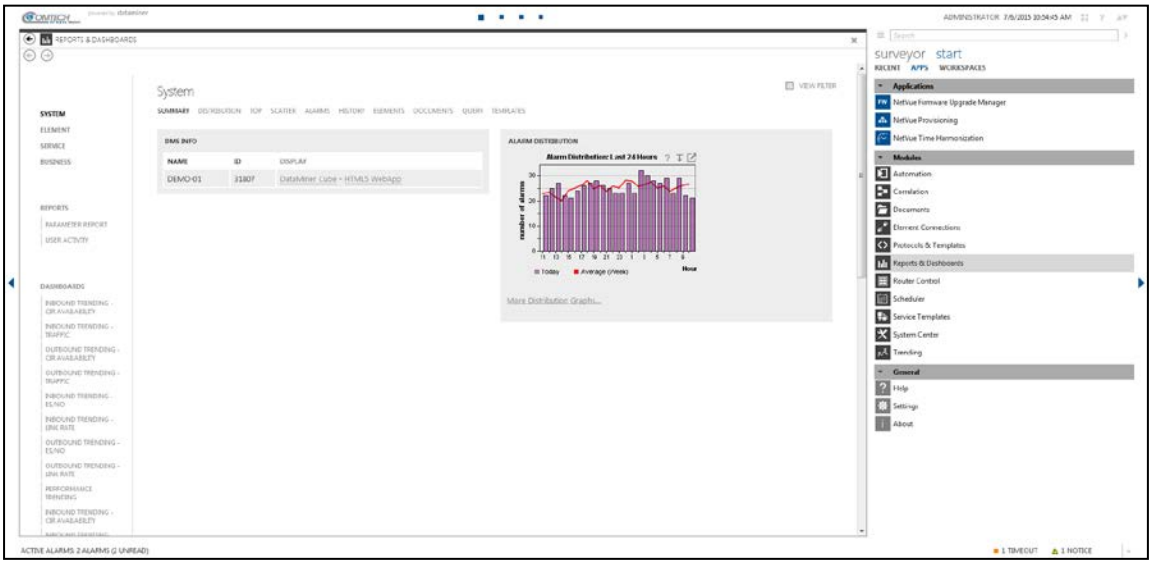


Figure 10-5. Reports & Dashboards

In the navigation menu on the left, you can see an overview of the available reports and dashboards. The four pages at the top of the navigation menu contain the built-in reports: System, Element, Service and Business. With the view filter in the top right corner, you can show information for certain views only.

The Reports section below the built-in reports contains custom report templates, and allows the creation of report templates.

10.3.1 System Reports

The System page has 10 tabs:

- **Summary** – shows an overview of your NetVue agents and an alarm distribution graph. Click **More Distribution Graphs** to go to the **Distribution** tab.
- **Distribution** – an alarm distribution graph that can be set to include particular severities and element types, in a particular time range. You can choose to show data from the **Last 24 Hours**, **Yesterday**, a **Week to Date** or a **Month to Date**. Depending on the selected time range, you can also choose an average range to show in the graph as a reference.
- **Top** – overview of the elements that generated the most alarms and were in an alarm state for the longest period of time. The graphs can be set to include particular severities and element types, in a particular time range. For the time range, a wide range of options is available, including a custom time range.
- **Scatter** – shows a comparison of the different alarm events versus the alarm states. The graph can be set to include particular severities and element types, in a particular time range. For the time range, a wide range of options is available, including a custom time range.
- **Alarms** – lists all active alarms in your NetVue system. You can select to include all severities, or only some of the severity levels.
- **History** – overview of alarms in a custom time range. It is possible to include only certain severities and alarm types. You can also filter on parameter name, using wildcards if necessary.
- **Elements –** lists all elements in your NetVue system, each with their current alarm status, and a link to open the element card in a separate window. You can select to see all elements, or only the elements that are currently active.
- **Documents –** lists all documents available in your NetVue system.
- **Query –** shows a status report for a number of parameters from all elements based on a selected protocol.
- **Templates –** links to the custom report templates section.

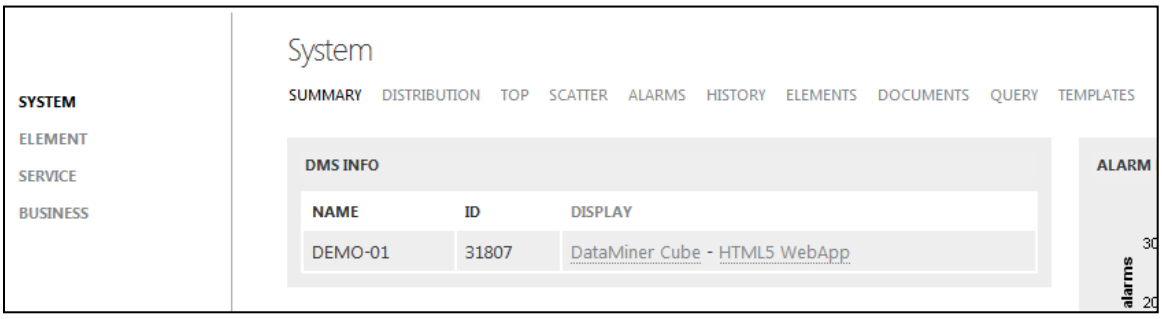


Figure 10-6. System Reports

10.3.2 Element Reports

To see report information on the **Element** page, you first select an element. Later, you can select a different element by clicking **CHANGE** to the right of the element name in the header.

Once an element has been selected, 11 tabs are shown:

- **Summary** – shows element information and any annotations for the element.
- **Distribution** – an alarm distribution graph that can be set to include particular severities in a particular time range. You can choose to show data from the **Last 24 Hours**, **Yesterday**, a **Week to Date** or a **Month to Date**. Depending on the selected time range, you can also choose an average range to show in the graph as a reference.
- **Severities –** overview of alarm events and alarm states, in a selected time range. You can choose to show these for the full element or for a particular parameter. For the time range, a wide range of options is available, including a custom time range.
- **Alarms –** lists all active alarms on the element. You can select to include all severities, or only some of the severity levels.
- **History –** overview of alarms in a custom time range. It is possible to include only certain severities and alarm types. You can also filter on parameter name, using wildcards if necessary.
- **Status –** overview of the status of the element's parameters. For elements with several pages, a quick menu is shown on the right side of the reporter interface, which allows you to quickly go to the parameters of a particular page.
- **Parameter –** shows the current value and last change for a selected parameter, along with a trend graph for the last hour and the last 24 hours.
- **Top –** overview of the parameters that generated the most alarms in a selected time range. For the time range, a wide range of options is available, including a custom time range.
- **Trending –** shows trending information for a selected parameter in a selected time range. For the time range, a wide range of options is available, including a custom time range. The trend graph can be customized to show average trending only, or to show minimum and maximum values as well.
- **Documents –** lists all documents available for the selected element. You can choose to see all documents, or only protocol-specific documents.
- **Spectrum –** shows any available Spectrum Analyzer buffer traces.

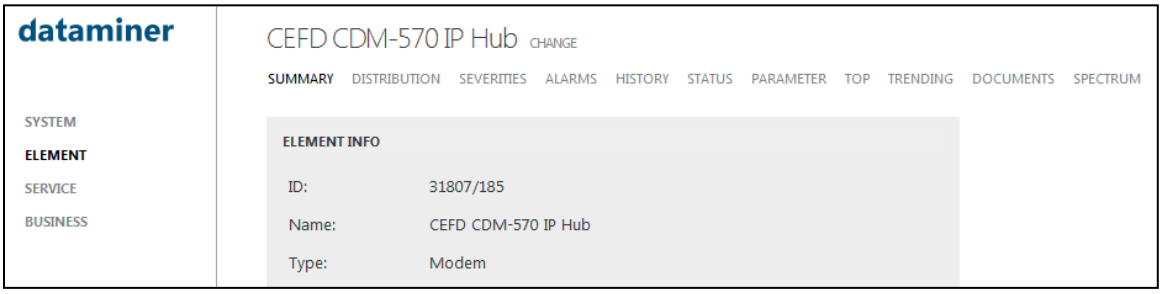


Figure 10-7. Element Reports

10.3.3 Service Reports

To see report information on the **Service** page, you first select a service. Later, you can select a different service by clicking **CHANGE** to the right of the service name in the header.

The **Service** page has 6 tabs:

- **Summary** – shows service information and any annotations for the service.
- **Distribution** – an alarm distribution graph that can be set to include particular severities in a particular time range. You can choose to show data from the **Last 24 Hours**, **Yesterday**, a **Week to Date** or a **Month to Date**. Depending on the selected time range, you can also choose an average range to show in the graph.
- **Severities –** overview of alarm events and alarms, in selected time range. For the time range, a wide range of options is available, including a custom time range.
- **Alarms –** lists all active alarms on the service.
- **History –** overview of alarms in a custom time range. It is possible to include only certain severities and alarm types. You can also filter on parameter name, using wildcards if necessary.
- **Top –** overview of the elements that generated the most alarms in a selected time range. For the time range, a wide range of options is available, including a custom time range.

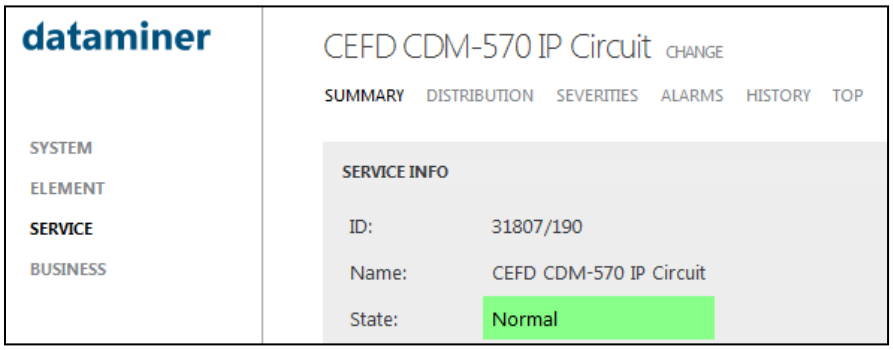


Figure 10-8. Service Reports

10.3.4 Business Reports

The Business page shows a variety of reports for a particular SLA.

If there is more than one SLA available, you choose the SLA you wish to see. Later, you can select a different SLA by clicking **CHANGE** in the header to the right of the SLA name.

You can choose from 11 tabs at the top of the page:

- **Summary** – shows general information on the SLA and the service, as well as a graph showing the distribution alarms.
- **Distribution** – an alarm distribution graph that can be set to include particular severities in a particular time range. You can choose to show data from the **Last 24 Hours**, **Yesterday**, a **Week to Date** or a **Month to Date**. Depending on the selected time range, you can also choose an average range to show in the graph.

- **Severities –** overview of alarm events and alarm states for the SLA, in a selected time range. You can choose to show a particular element, SLA availability, or SLA compliance. For the time range, a wide range of options is available, including a custom time range.
- **Alarms –** lists all active alarms pertaining to the SLA.
- **History –** overview of alarms in a custom time range. It is possible to include only certain severities and alarm types. You can also filter on parameter name, using wildcards if necessary.
- **Service History –** allows you to have an SLA recalculated for any period in the past and make the results available in a report.
    - Indicate the start and end time for your report, the severities to be included, the alarm types to be included, and optionally, a parameter name filter.
    - Click the **Load** button.
    - Click the **Generate Report** button in the bottom right corner.
- **Status** – overview of the status of the SLA, as you would otherwise find by opening the SLA itself.
- **Parameter** – generate reports for particular parameter, but selecting the parameter in the drop-down menu.
- **Top –** overview of the parameters that generated the most alarms in a selected time range. For the time range, a wide range of options is available, including a custom time range.
- **Trending –** shows trending information for a selected parameter in a selected time range. For the time range, a wide range of options is available, including a custom time range. The trend graph can be customized to show average trending only, or to show minimum and maximum values as well.

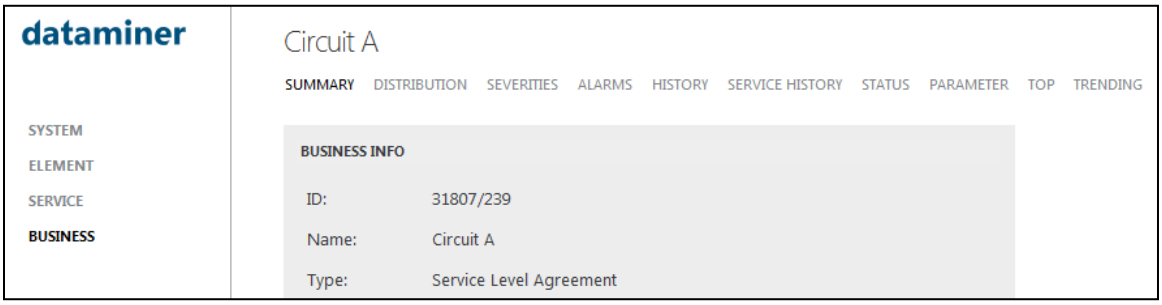


Figure 10-9. Business Reports

10.3.5 View Filter

With the **View Filter**, you can show reports that only contain information about items located in a particular view or one of its sub-views.

1. In the top right corner, select **View filter**.
2. Click **switch**.
3. In the **View Selection** dialog box, select a view.

10.4 Custom Report Templates

It is possible to create new custom report templates in the NetVue Cube. They can be used to:

- Generate reports in the Reports & Dashboards app.
- Send email reports with other NetVue apps.

10.4.1 Access the Report Templates

To go to the report templates page:

1. Open the **Reports & Dashboards** app
2. Go to **Start > Apps > Reports & Dashboards**
3. In the navigation menu on the left, click **Reports**.

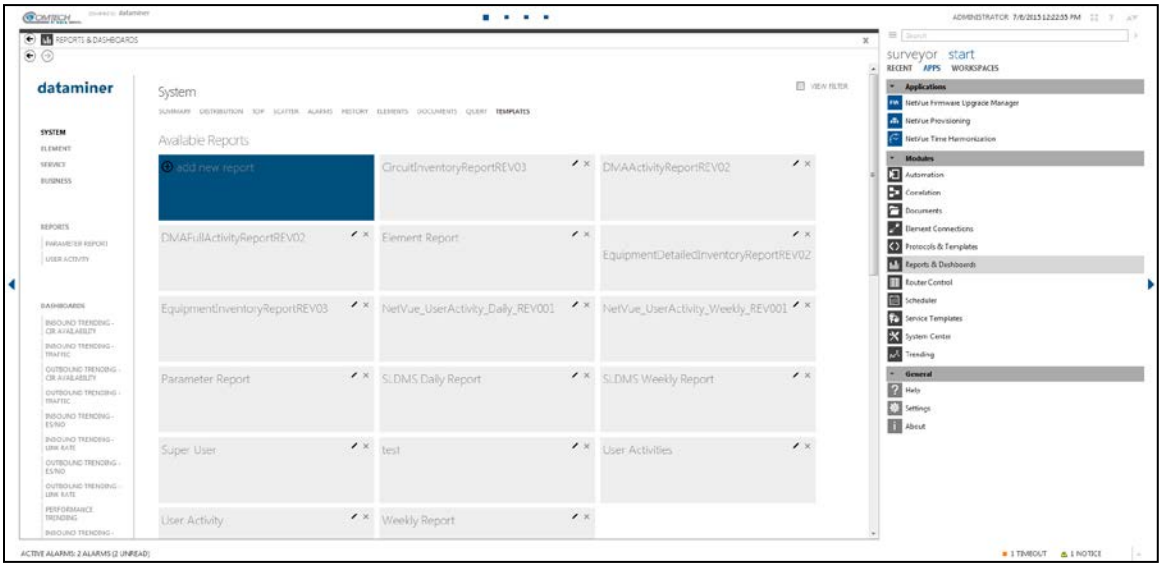


Figure 10-10. Report Templates

On the report templates page, you can:

- Edit report templates, by clicking the pencil icon in the top right corner of the template.
- Delete report templates, by clicking the x in the top right corner of the template.
- Add new report templates.
- Generate reports based on custom templates.

10.4.2 Adding a New Report Template

1. On the report templates page, click **add new report**.
2. Enter the template name and the template description.
3. Select the template type:
    a. One single element/service, or
    b. Multiple elements/services
4. In the **Navigation Menu** box, select one of these options:
    a. **Not Displayed** – the report template will not be shown in the navigation menu of the Reports & Dashboards app.
    b. **Link to Template** – in the Reports & Dashboards navigation menu, a link to the report template will be shown.
    c. **Link to Report** – in the Reports & Dashboards navigation menu, a link to the report itself will be shown.
5. Click **View advanced options** to configure these advanced options:
    a. If you want the report to use the element descriptions instead of the element names, select **Use element descriptions instead of names**.
    b. To sort elements in the report, select **Sort elements**.
    c. To use an alternative header in the report, select **Use alternative header**. The alternative header contains only the company logo.
    d. To attach a spreadsheet document to the report, select **Attach Excel/OpenDocument Spreadsheet**. This .ods document will contain a separate worksheet for every table or graph in the report.
    e. To attach a zip file with a .csv export for each table or graph in the report, select **Attach CSV data files**.
    f. To make sure elements without data are not shown, select **Hide elements without data**.
6. In the **Template Layout** section, add the necessary building blocks and configure their settings.
7. To add a building block, select one from the list and click **Add Block**.
8. If necessary, change the order of the added building blocks by clicking the up or down arrows in the top-right corner of each building block.
9. When the report template is ready, click **Save Template**.

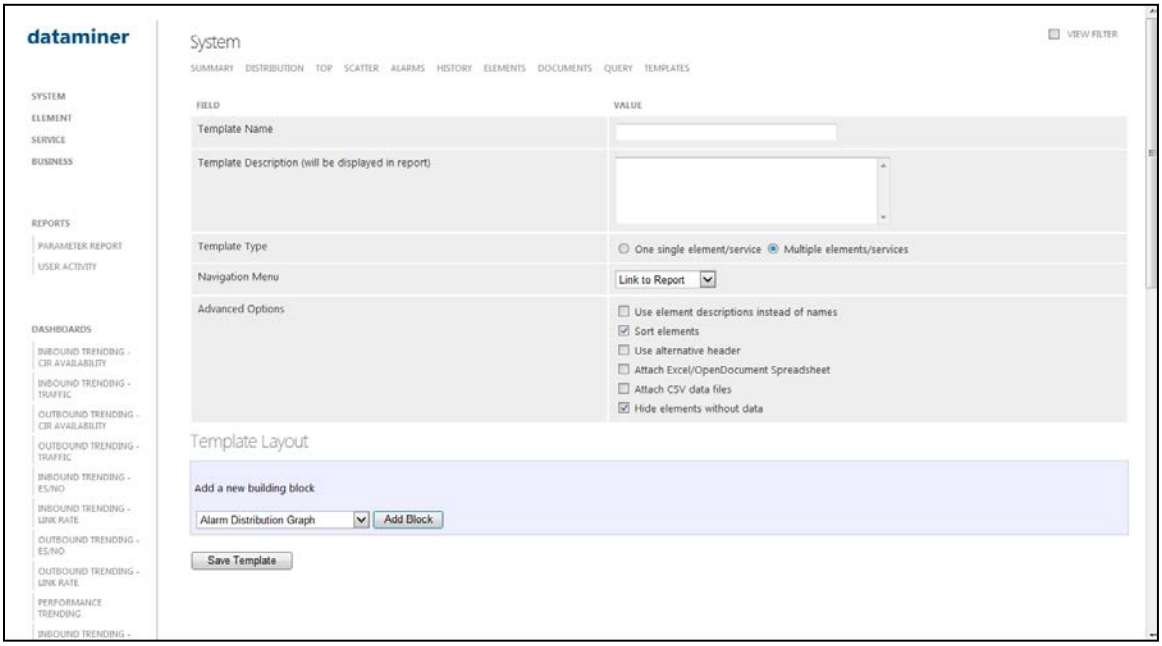


Figure 10-11. Custom Template

10.5 Report Template Components

10.5.1 Components for Single Element/Service

For one single element or service, these building blocks are available:

Alarm Distribution Graph – a graph showing the distribution of alarms over a selected time span, with several options:

- You can choose to show data from the **Last 24 Hours, Yesterday, a Week to Date or a Month to Date**.
- Depending on the selected time range, you can select different possibilities for the average range that will be shown as a reference in the graph.
- It is possible to include only certain severities.

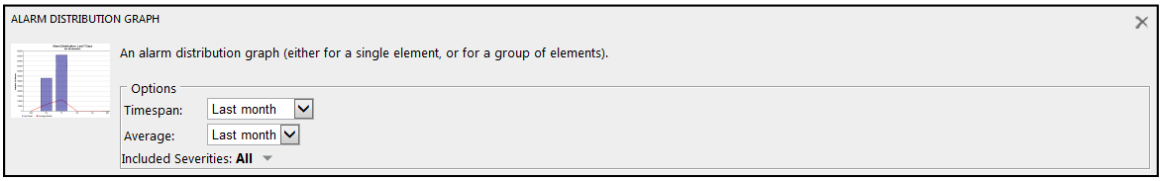


Figure 10-12. Alarm Distribution Graph

Alarm List – an overview of an element's active alarms or historical alarms with these options:

- You can choose from different time spans: **Active**, to show only active alarms, **Last Hour, Last 24 Hours, Yesterday, Week to Date, Month to Date, Previous Month** or **Year to Date**.
- It is possible to include only certain severities and alarm types.
- To include certain parameters only, you can filter on parameter name.
- You can choose to sort the list either by element name or by alarm time.

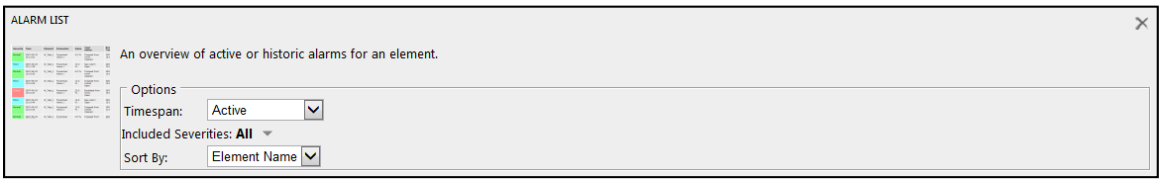


Figure 10-13. Alarm List

Alarm State – a pie graph showing how long an element or service has been in each alarm state. You can choose from many different time spans, or set a custom time span.

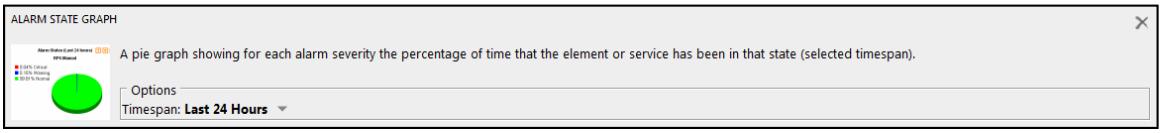


Figure 10-14. Alarm State

CPE – is available only in a NetVue system with CPE implementation. These items can be shown with this component:

- A status report, which can show a list with connected objects on the lower topology levels, and the real-time values of specific KPIs. Optionally, this can include the average and minimum/maximum trending values for a selected time range, and a link to the CPE interface.
- A trend graph for one or more KPIs. Different options are available as to the time range for the graph, and you can choose whether to include average trending only, or to include minimum and maximum values.
- A heat map, with different options for the time range and different layout options: **Highlight Highest Values, Highlight Lowest Values**, and **Apply Alarm Template**.
- A top X list of alarm states or alarm count. This is an overview of the items that either had the highest number of alarm events or spent the most time in an alarm state. These options are available:
    - o You can choose from many different time spans, or set a custom time span.
    - o You can exclude or include certain alarm severities.
    - o A textual overview can be included; it can be sorted by name or by rank.
    - o The list can be limited to the top 10, 20, 30, 40 or 50 objects.

When you generate a report with this component, you can then:

- Select the topology fields for which you want to create a report.
- Specify particular KPIs or objects on the lower topology levels.
- For selected KPIs, determine whether to show the average, minimum, maximum or real-time value.

Figure 10-15. CPE

DMS Status – general information about the NetVue system: the information will show:

- An overview of the total number and the number of active elements and services per NetVue agent
- An overview of the total number and the number of active elements and services in the entire NetVue system
- NetVue version number and build ID

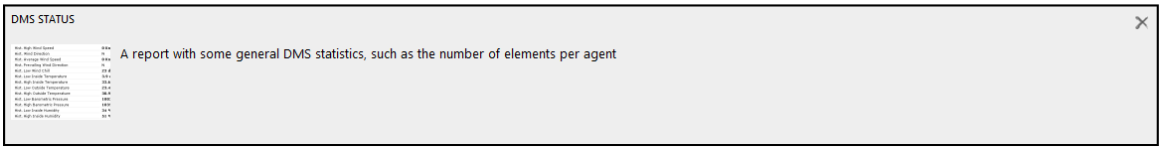


Figure 10-16. DMS Status

Element/Service Info – general information about the element or service

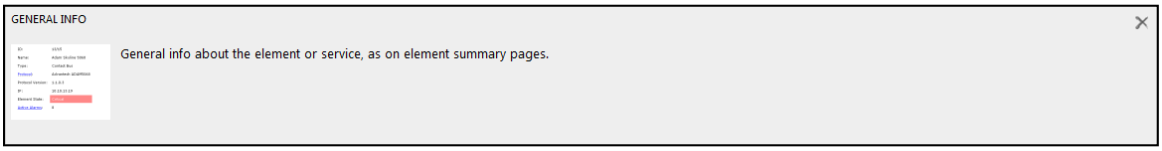


Figure 10-17. Element/Service Info

Heat Map – a heat map with average trend values: these options are available:

- You can choose from different time spans: **Hour, Day, Week, Month** or **Year**.
- You can choose from three options for the way the colors will be applied: **Highlight Highest Values, Highlight Lowest Values** and **Apply Alarm Template**.

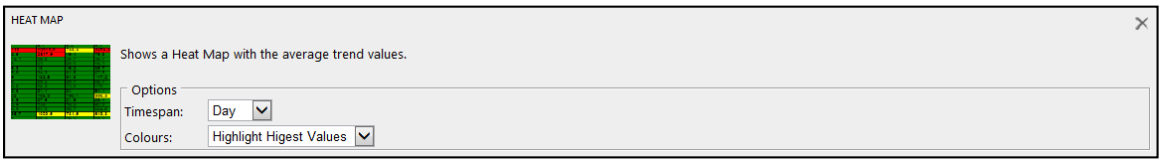


Figure 10-18. Heat Map

Info Table – a list of active alarms or list of documents for the element, depending on your selection

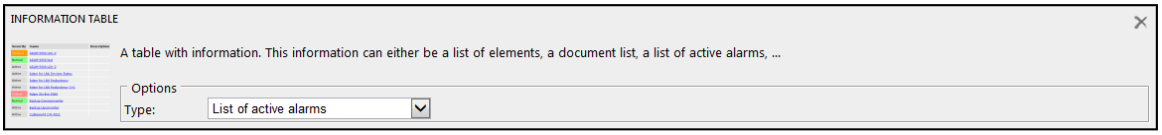


Figure 10-19. Info Table

New Alarm Types – a pie graph showing the number of alarms for each alarm severity; choose from many different time spans, or set a custom time span.

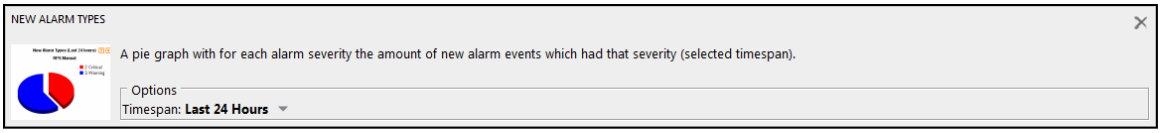


Figure 10-20. New Alarm Types

Parameter Reports – a parameter report with current reading and trending information for each parameter contained in the report. Each parameter will be shown with a background color matching its alarm state.

Figure 10-21. Parameter Reports

SLA Historic Service Alarm List – only applicable for SLA elements; shows a table with an overview of historic service alarms for the SLA. Above this table is a summary of the total affected and total violation time, the minimum and measured availability, etc. These options are available:

- You can choose from different time spans: **Active**, to show only active alarms, **Last Hour, Last 24 Hours, Yesterday, Week to Date, Month to Date, Previous Month** or **Year to Date**.
- It is possible to include only certain severities and alarm types.
- To include certain parameters only, you can filter on parameter name.

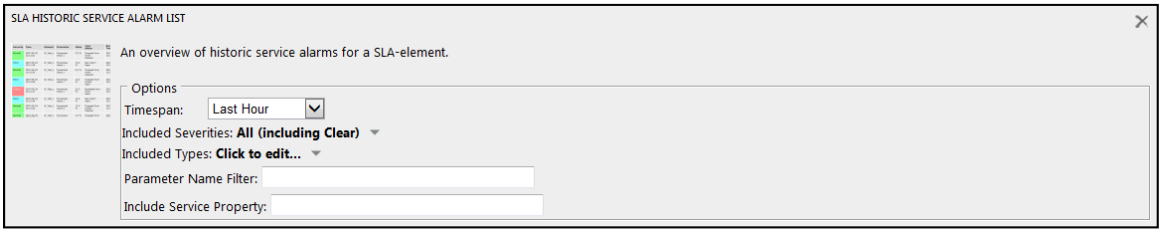


Figure 10-22. SLA Historic Service Alarm List

Spectrum Buffers – only applicable for Spectrum Analyzer elements; shows the contents of the last measured trace for each of the available spectrum monitor buffers.

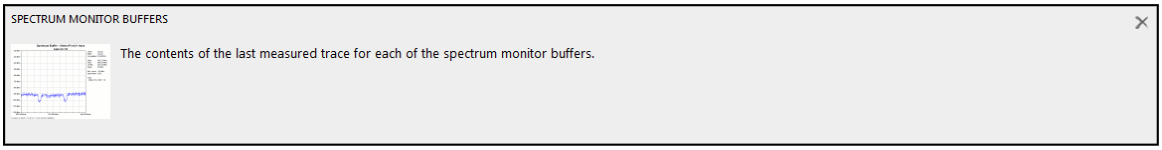


Figure 10-23. Spectrum Buffers

State Timeline – a timeline showing the alarm state of the element or service in the selected time span; these options are available:

- You can choose from many different time spans, or set a custom time span.
- You can choose to include a **Textual Overview**.
- You can choose to show only the **Textual Overview**, instead of the timeline.

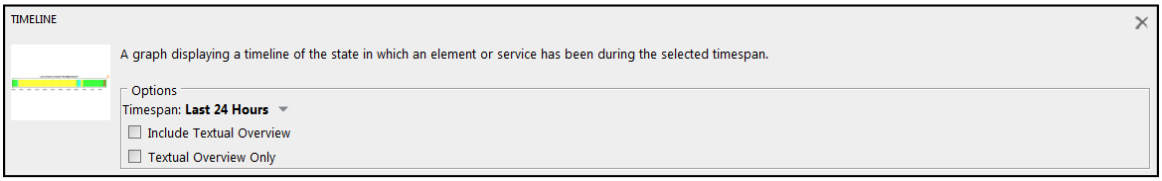


Figure 10-24. State Timeline

State Timeline (Parameters) – a timeline showing the alarm state of the selected parameters in the selected time span; these options are available:

- You can choose from many different time spans, or set a custom time span.
- You can choose to include a **Textual Overview**.
- You can choose to show only the **Textual Overview**, instead of the timeline.

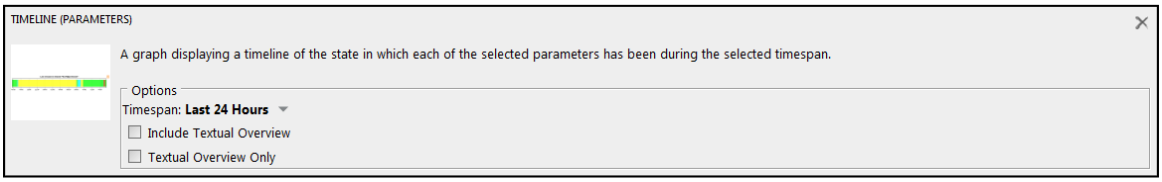


Figure 10-25. State Timeline (Parameters)

Status Report – an overview of the status of each parameter; parameters that are in an alarm state will have a matching background color. For parameters that have average trending enabled, a clickable link will allow you to go to the trend graph for those parameters.

These options are available for this component:

- Select **Limit to selected parameters** to allow the user to select which parameters to include when configuring a mail report. For table parameters, only those columns and rows that match the selected parameters will be included.
- When the **Limit to selected parameters** option is enabled, an additional option becomes available: **Allow trending avg/min/max to be included**. Select this option and specify a time span. When configuring the report, the user will be able to select which trending columns should be shown: **Avg**, **Min** and **Max**, **Realtime,** or any combination of these.

- To make sure that parameters that are not initialized are not shown in the report, select **Hide "Not Initialized" Parameters**.
- To add tables as an Excel attachment to an email report, select **Add tables as Excel attachment also**. The report will then have a link to the Excel file next to all of its status report tables. Only one Excel file, named ExcelTableData.xls, will be included in the email report, with different tables on different worksheets in the file.

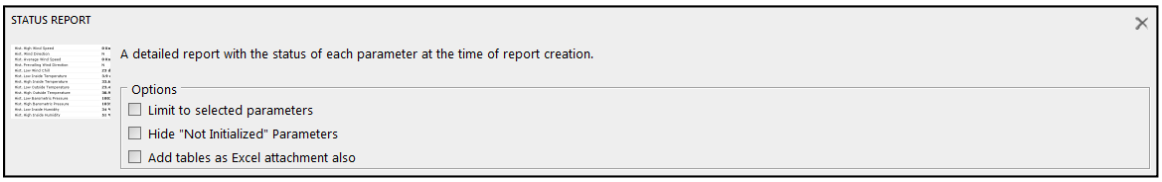


Figure 10-26. Status Report

Status Query – an overview of parameter states of all elements using the same protocol as the current element; these options are available:

- To add columns with the minimum/maximum/average trending information for some parameters, select **Allow trending avg/min/max to be included**, and select a time span for the trending.
- To add a pie chart for the first parameter in the status query, select **Add pie chart for first parameter**.

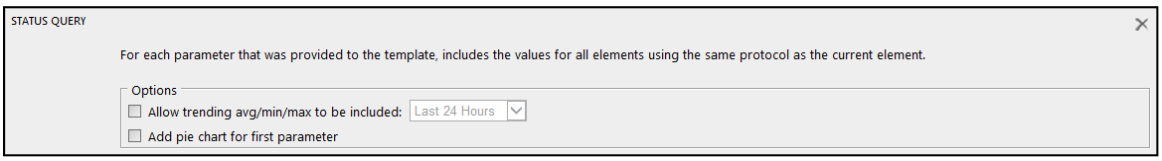


Figure 10-27. Status Query

Trend Graphs – shows a trend graph per parameter, with these options:

- You can choose from different time spans: **Active**, to show only active alarms, **Last Hour, Last 24 Hours, Yesterday, Week to Date, Month to Date, Previous Month** or **Year to Date**.
- You can choose to include average trending only, or to show minimum and maximum values.
- To add an overview comparing the data with a previous time span, select **Include overview instead of TOC**.

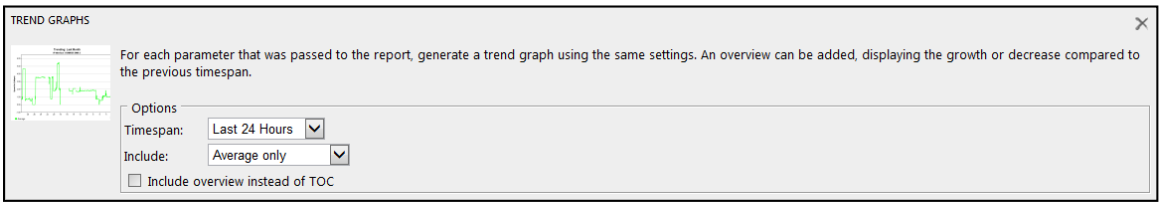


Figure 10-28. Trend Graphs

Top Parameters – an overview of the parameters that had the most alarm events in a selected time span. These options are available:

- You can choose from many different time spans, or set a custom time span.
- The list can be limited to 10, 20, 30, 40 or 50 parameters

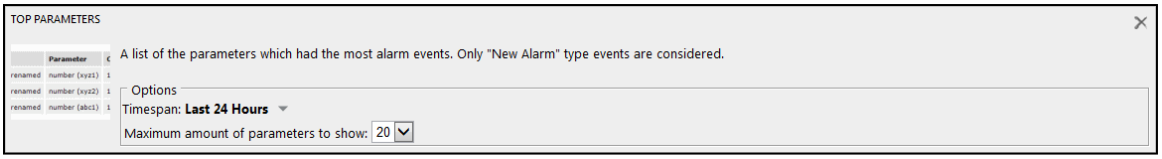


Figure 10-29. Top Parameters

Visual Overview – the visual overview for the element or service

Figure 10-30. Visual Overview

10.5.2 Components for Multiple Elements/Services

For multiple elements or services, these building blocks are available:

Alarm Distribution Graph – a graph showing the distribution of alarms over a selected time span, with several options:

- You can choose to show data from the **Last 24 Hours, Yesterday, a Week to Date** or **a Month to Date**.
- Depending on the selected time range, you can select different possibilities for the average range that will be shown as a reference in the graph.
- It is possible to include only certain severities or element types.

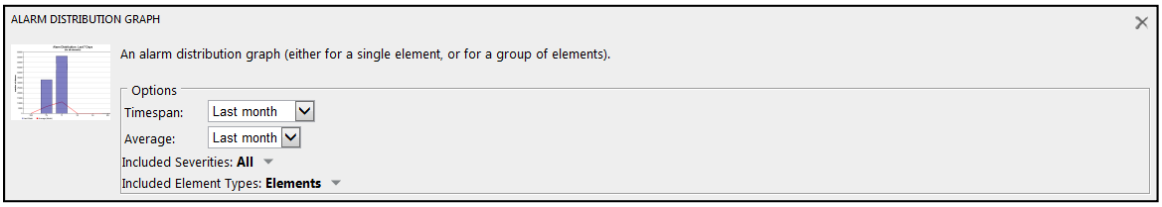


Figure 10-31. Alarm Distribution Graph (Multiple)

Alarm Scatter Graph – a graph comparing the different alarm events versus the alarm states for a selected time span; these options are available:

- You can choose from many different time spans, or set a custom time span.
- It is possible to include only certain severities or element types.
- To include a textual overview, select **Include Textual Overview**. You can then select how the overview is sorted, by: **Name**, # **Events** or **Duration**.

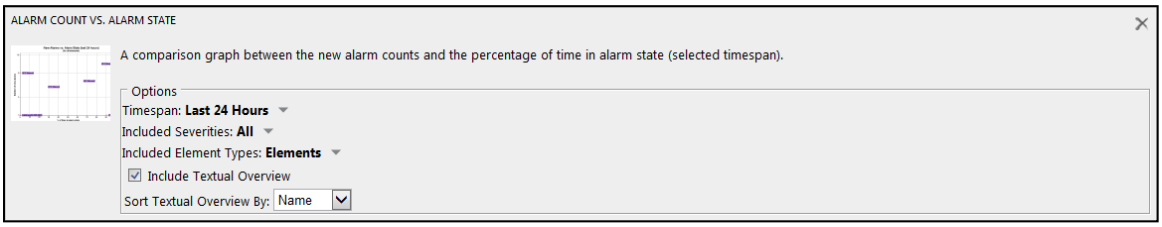


Figure 10-32. Alarm Scatter Graph

DMS Status – general information about the NetVue system; the information shows:

- An overview of the total number and the number of active elements and services per NetVue agent
- An overview of the total number and the number of active elements and services in the entire NetVue system
- NetVue version number and build ID

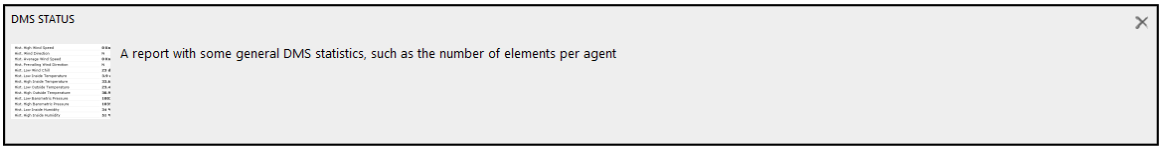


Figure 10-33. DMS Status (Multiple)

Element/Services Container – is a container for element-specific information. Within this container, you can add report components for single elements.

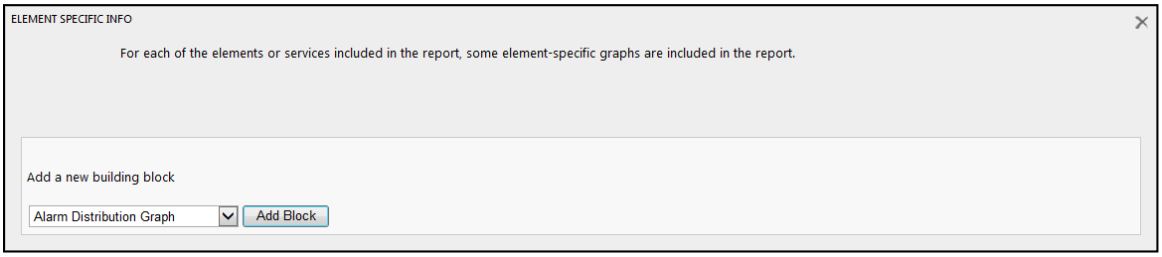


Figure 10-34. Element/Services Container

Info Table – a list of NetVue agents, elements, documents or elements with their state and active alarm count

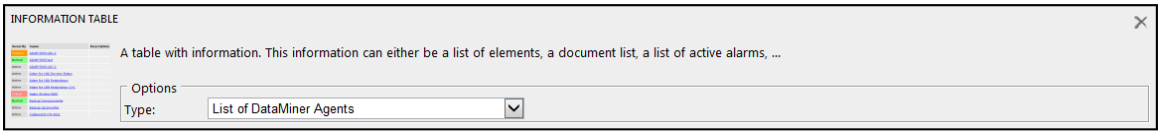


Figure 10-35. Information Table

SLA Historic Service Alarm List – is only applicable for SLA elements. This list shows a table with an overview of historic service alarms for several SLA elements. Above this list is a summary of the total affected and total violation time, the minimum and measured availability, etc. These options are available:

- You can choose from different time spans: **Active**, to show only active alarms, **Last Hour, Last 24 Hours, Yesterday, Week to Date, Month to Date, Previous Month** or **Year to Date**.
- It is possible to include only certain severities and alarm types.
- To include certain parameters only, you can set a filter on parameter name.

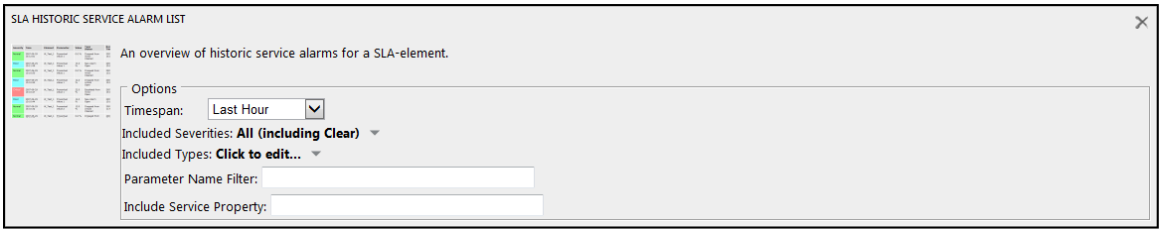


Figure 10-36. SLA Historic Service Alarm List (Multiple)

Top 10 States/New Alarm Count – is an overview of the elements or services that either had the highest number of alarm events or spent the most time in alarm state. These options are available:

- You can choose from many different time spans, or set a custom time span.
- It is possible to include only certain severities or element types.
- To include a textual overview, select **Include Textual Overview**. By default, this overview is sorted by rank; however, you can also select the option **Sort textual overview by name instead of rank**.
- The graph can be limited to 10, 20, 30, 40 or 50 elements.

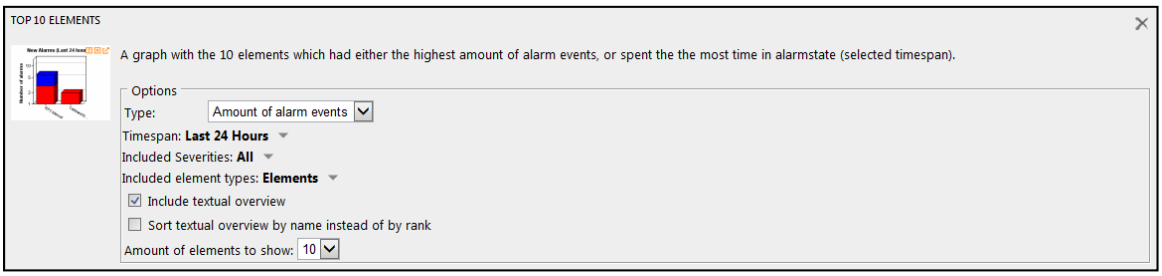


Figure 10-37. Top 10 States/New Alarm Count

Alarm List – an overview of an element's active alarms or historical alarms, with these options:

- You can choose from different time spans: **Active**, to show only active alarms, **Last Hour, Last 24 Hours, Yesterday, Week to Date, Month to Date, Previous Month** or **Year to Date**.
- It is possible to include only certain severities and alarm types.
- To include certain parameters only, you can set a filter on parameter name.
- You can choose to sort the list either by element name or by alarm time.

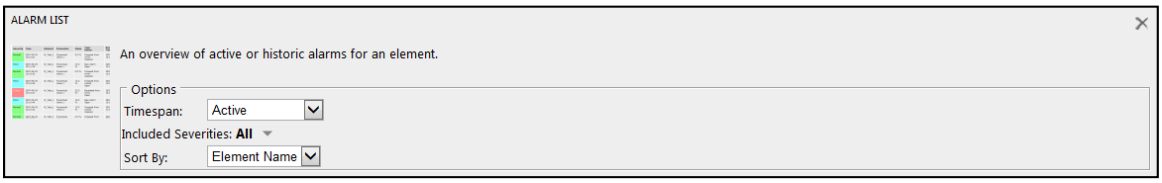


Figure 10-38. Alarm List (Multiple)

Aggregation – is a graph visualizing the data of one or more aggregation rules. These options are available:

- You can choose from these types of graph: a **Trend Graph, Bar Graph** or **Pie Graph**.
- For a trend graph, you can choose from different time spans: **Last Hour, Last 24 Hours, Yesterday, Week to Date, Month to Date, Previous Month** or **Year to Date**.
- For a trend graph, you can select to include only average trending, or to include minimum and maximum values.
- It is possible to show the graph for a view with or without its sub-views. To include sub-views, select **Include sub-Views**.

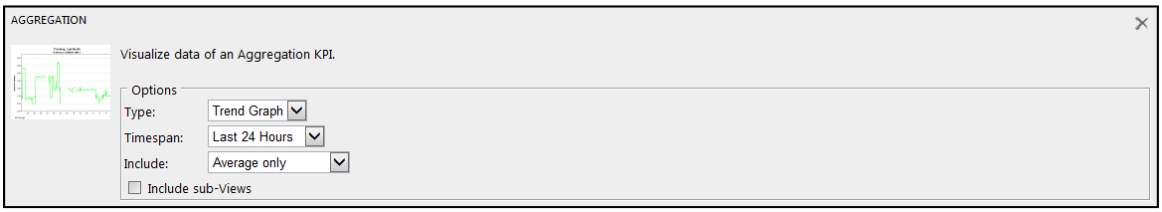


Figure 10-39. Aggregation

10.6 Canned Reports

The NetVue system includes a number of standard, pre-built reports, also known as canned reports. These reports give helpful details about the NetVue operations.

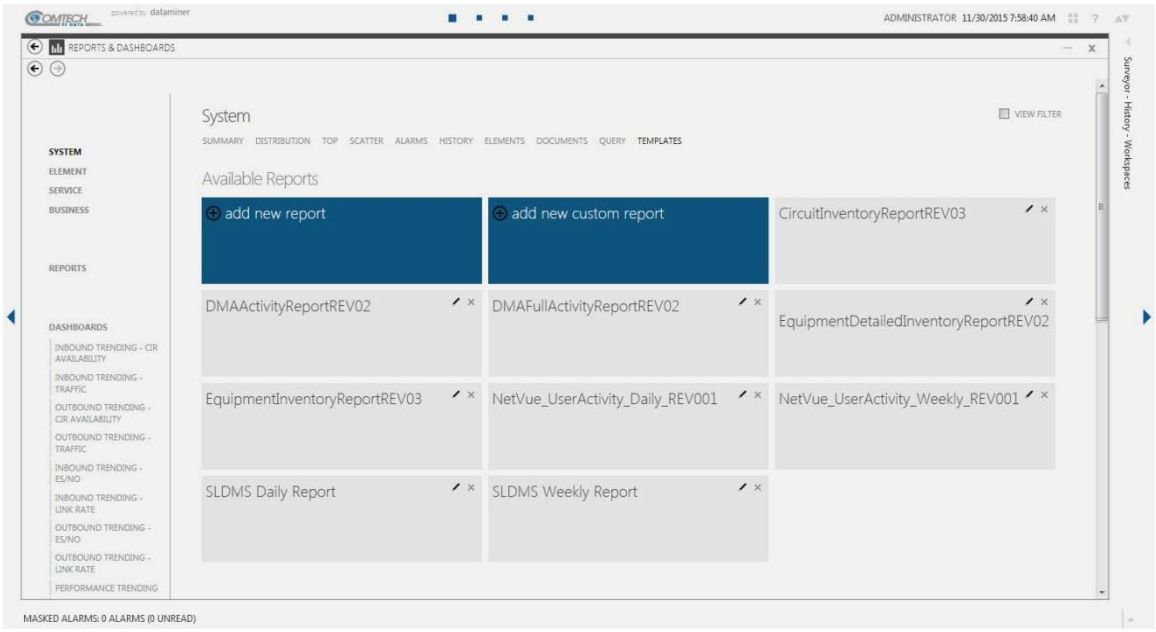


Figure 10-40. NetVue Reports

10.6.1 User Activity, Daily or Weekly Reports

- System-wide reports capture:
  - Log ins/outs of each user, just as they appear in the Event View
  - Maximum concurrent user occurrences during the time specified, with the actual date/time stamps
  - Any/all device configuration changes, just as they appear in the Event View

10.6.2 Inventory Reports

10.6.2.1 Circuit Inventory Report

- Summary of In and Out bits or bytes transferred over a polling period for both ends of circuit
  - Maximum In / Out
  - Minimum In / Out
- Summary of Eb/No over a polling period for both ends of circuit
  - Maximum In / Out
  - Minimum In / Out

- Summary of RSL over a polling period for both ends of circuit
  - Maximum In / Out
  - Minimum In / Out
- Event messages that are related to the circuit for both ends of circuit
  - Alarm
  - Disconnect
  - Lock/Unlock

10.6.2.1.1 Device Report

This reports the same data as the Circuit report, but for one end of the circuit only.

- Summary of In and Out bits or bytes transferred over a polling period for device
  - Maximum In / Out
  - Minimum In / Out
- Summary of Eb/No over a polling period for a device
  - Maximum In / Out
  - Minimum In / Out
- Summary of RSL over a polling period for a device
  - Maximum In / Out
  - Minimum In / Out
- Maximum polling delay (SNMP devices only)
- Event messages that are related to the device
  - Alarm
  - Disconnect
  - Lock/Unlock

10.6.2.2 Equipment Inventory Report, by Type

- License utilization:
  - Number of elements under management
  - Total elements available to be managed based on the current license
  - Table of devices sorted by:
    - Type (Modems, RF, etc.)
  - Each line in the table to include:
    - Serial Number
    - Firmware version number
    - MAC Address (if available)

10.6.2.3 Equipment Inventory Report, detailed

10.6.2.3.1 Event History (by)

- Choose grouping within the report:
  - By Name of device
  - Type of device
  - Circuit(s)
  - User(s)
- Define the time span of the report:
  - Last Month
  - Last 24 Hours
  - Last Hour

10.6.2.3.2 TimeSync Report

- Devices that are outside the configured window (+/- 2 seconds)
- Devices that have failed to comply with time synchronization
- Devices not configured to be time synchronized

10.6.3 Performance, DMA Activity Reports

- Maximum CPU (Windows, ESXi)
- Maximum I/O (Windows, ESXi)
- System Alarms (Windows, ESXi)
- Disk Space (Windows, ESXi)
- Shows Date/Time of MAX Events

10.6.4 Disk Space Monitoring

You must monitor available disk space on the NetVue agent. The performance report shows usage data for disk space.

NetVue alerts you when the available disk space is less than a specified critical level. Error log events show the exceeded limit.

By default, the disk space limit is 95%, but you can adjust it as necessary. Set the minimum disk space as shown in the alarm template.

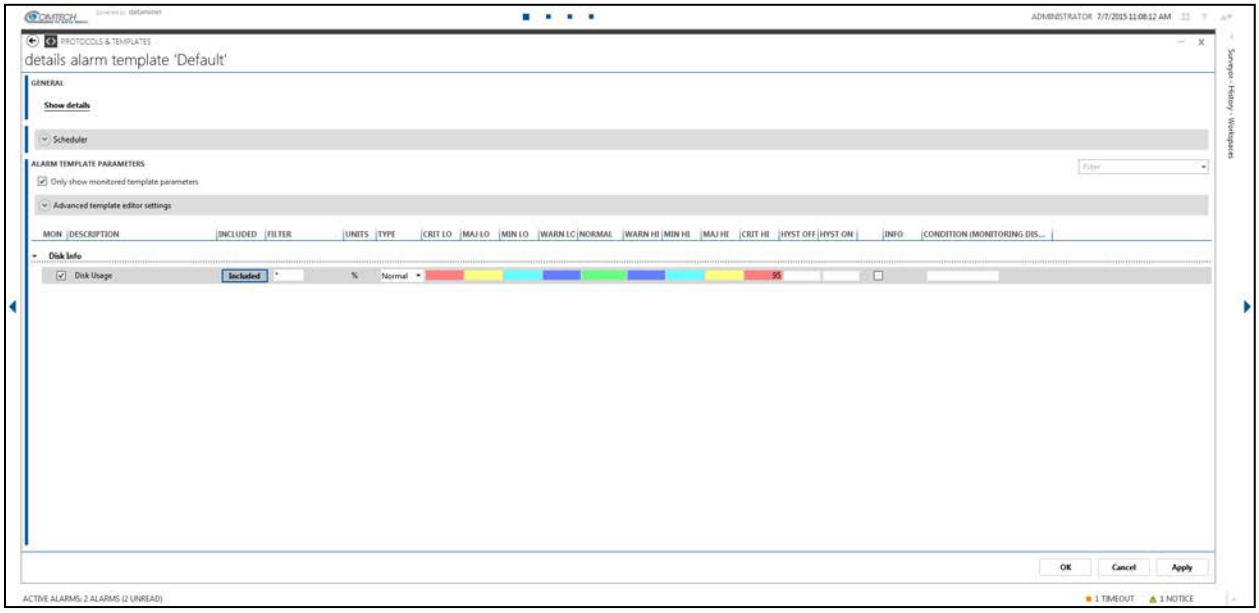


Figure 10-41. Alarm Template

10.7 Generate a Report with a Custom Report Template

Use custom report templates to generate reports that are sent by email. You can directly generate reports also, using the Reports & Dashboards app.

10.7.1 Generate a Report

To generate a report using the Reports & Dashboards app:

1. Go to the report templates page (see Section 10.4)
1. Click any of the available custom report templates.
2. To apply the default options saved previously for this report:
    a. Click **Load default options**.
    b. Skip to step 8.
3. Optionally, enter a title and message to show at the top of the report.
4. Select the views, elements, parameters, etc., as necessary for the report.
5. Choose whether to generate an HTML or PDF report.
6. Optionally, select to export tables and graphs as .ods, .csv or .xml, instead of generating a full report.
7. To keep these options as default options for the report, click **Save As Default Options**.
8. Click **Generate** to generate the report.

10.8 Email Reports

In NetVue Scheduler and NetVue Automation, you can cause NetVue to send email messages that include reports. These reports can be those created with NetVue Reporter or a third-party report editor.

By default, the email is sent in HTML format, using the template in C:\Skyline DataMiner\NotifyMail.html, but it can also be sent in plain text format.

The report content is included inside the message body, typically. However, you can choose to attach reports to email messages as separate PDF or MHT files.

10.8.1 Email Reports as Attachments

If you choose to send an email message as plain text instead of HTML, the report is attached to the email message as a separate file.

By default, the file is in PDF format. However, if you want the file to be in MHT format, include the text MHT somewhere in the email subject (e.g., between brackets).

Also by default, the file is named Report.pdf or Report.mht. To rename it, enter this code at the top of the message body:

attachName=ReportName;

ReportName is the name of the report without the .pdf or .mht extension.

10.9 NetVue Dashboards

NetVue Dashboards gives you access to the vast amount of valuable real-time and historical information available in your NetVue System.

You can design customized dashboards that consolidate all essential information and KPIs from devices, locations, services and SLAs available in the operational environment. You create dashboards using a comprehensive set of building blocks.

The dashboards are accessible through a platform-independent web interface. Any personnel, from engineering up to top-level management, can use them. Dashboards give a detailed inside view on the operations using an interactive, visually appealing and highly intuitive graphical interface. This interface can be accessed directly, or from within other NetVue applications. In the latter case, those applications feed the right information into the selected dashboard layout automatically.

10.9.1 Create a New Dashboard

To create a new dashboard in the NetVue Cube:

1. Go to **Start > Apps > Reports & Dashboards.**
2. In the column on the left, click **Dashboards.**
3. Under **Available Dashboards**, click **New Dashboard**. A new dashboard is added to the list below.

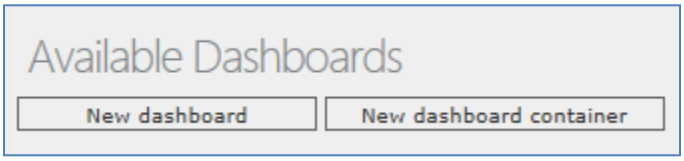


Figure 10-42. New Dashboard

4. Next to **Title**, fill in a title for the dashboard.
5. These configuration options are available also:
   a. To change the theme for the dashboard, click the **…** button next to **Theme**. This theme can be overruled by a personal theme.
   b. Next to **Description**, you can add a description with additional information about the dashboard.
6. You can select a folder for the dashboard using the drop-down list on the right. To create a new folder, select **<Create New>.**
7. To change the layout of the dashboard, click the **…** button next to **Layout**. Dashboard components can be shown in one to five columns, as an embedded component, in a raster, or a dynamic list.
8. There are two possibilities to save the dashboard:
   a. To configure the component of the dashboard later, click **Save Configuration**. (To edit the dashboard later, click the pencil icon in the dashboard list.)
   b. To configure the dashboard immediately, click **Save & Start Configuring Components**.

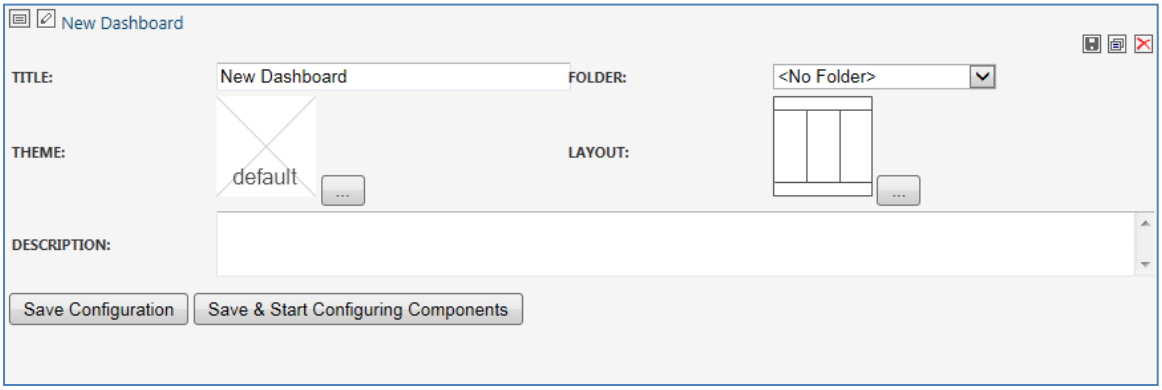


Figure 10-43. Creating a Dashboard

10.9.2 Configure Dashboard Components

To configure the components of a dashboard, you must first go to the dashboard editor. This can be done in two ways:

- After creating or editing a dashboard, click **Save & Start Configuring Components**, or
- Click an existing dashboard in the Reports & Dashboards app

In the dashboard editor, click **Actions** in the top right corner to get access to the various configuration options:

- Add/Remove Components
- Configure Components
- Feeds
- Settings

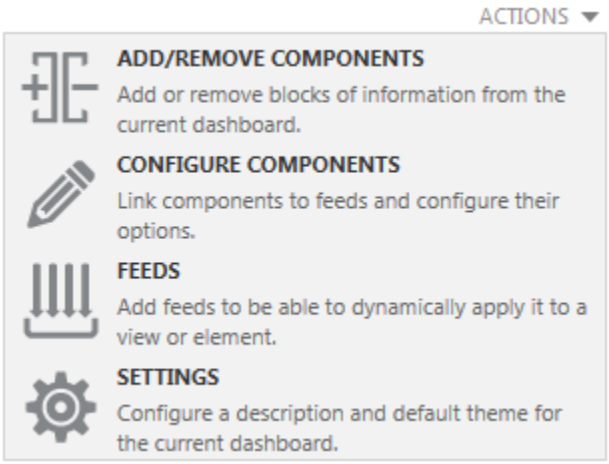


Figure 10-44. Dashboard Actions

10.9.2.1 Add/Remove Components

1. Go to **Actions > Add/Remove Components.**
2. Select a category from the list underneath **Add/Remove Components**.
3. Select one of the available components for the selected category.
4. Add the component to a zone of your dashboard:
    a. Use the **Add to** selection box and the **Add** button below the list.
    b. Or, drag the component to the zone.

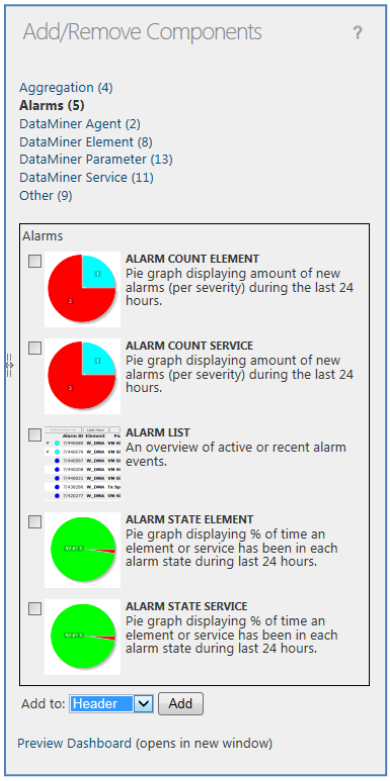


Figure 10-45. Add/Remove Components

5. To configure a component, click the **Configure** button underneath it.

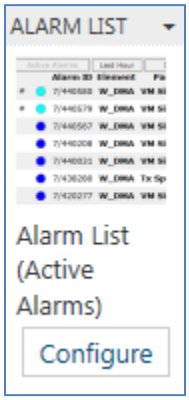


Figure 10-46. Configure button

10.9.2.2 Configure Components

1. Go to **Actions > Configure Components** and select a component.
2. Or, click the **Configure** button for one of the components.
3. In the **Feed** section of the configuration panel, choose what data the component will show. Depending on the type of component, you can choose a specific fixed input or configure a feed.
4. To configure a feed:
    a. Select an existing feed in the **Feed** selection box.
    b. Or, click **New.**
5. Click **Edit** to edit the feed. You will have the same options for editing as in the Feeds editor.
6. When finished, click **Save Feed** to save the changes.
7. Depending on the component type and the feed, you can select a specific element, parameter, service, etc., corresponding to the feed.

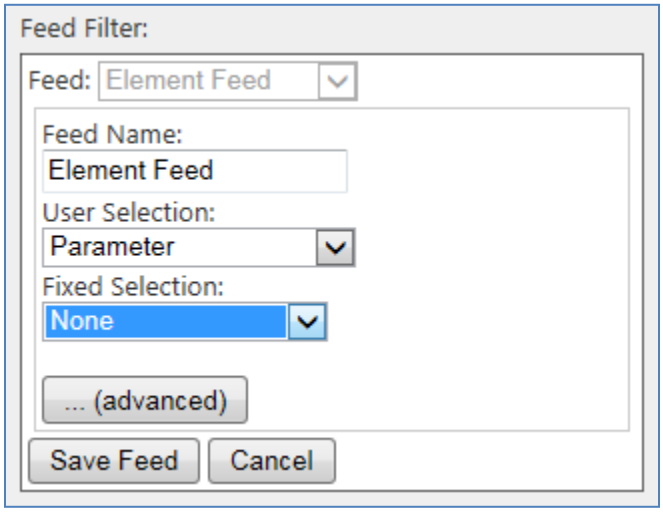


Figure 10-47. Feed Filter

8. In the **Options** section, set how the information should be displayed in the component. The available options depend on the type of component you chose. Some options return for most components:
    a. **Fixed Width** – specify a number of pixels for the width of the component.
    b. **Title** – change the title to show a different title above the component while it is being edited.
    c. **Display Title** – select to always show the component title on the dashboard.
    d. **Display Border** – select to include a border around the component.
    e. **Background Image** – click the **…** button to choose a background image for the component.
    f. **Background Mode** – use the drop-down list to choose how the background image is shown.
    g. **Text Color** – click the **…** button to set the text color of the component.
    h. Under **Extra CSS**, you can set advanced customizations.

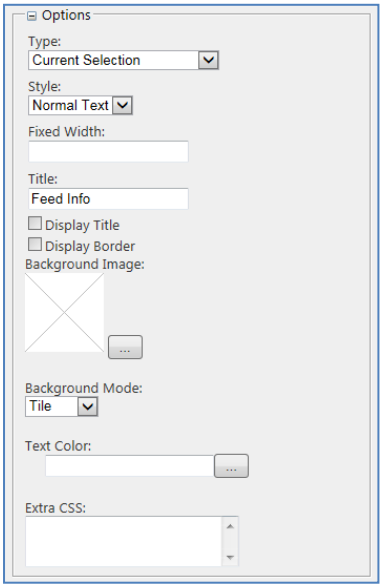


Figure 10-48. Options

9. Click **Apply** to save your changes.

10.9.2.3 Feeds

1. Go to **Actions > Feeds** to get access to the Feeds editor
    a. Click the pencil icon next to an existing feed in the top selection box, or
    b. Click **Add new feed** to configure a new feed.
2. Enter a name for the feed.
3. Select either a **User Selection** or a **Fixed Selection.**
4. If necessary, click **Advanced** to enter an Element mask that will limit the possible choices.
5. Click **Save Settings** to save the feed.

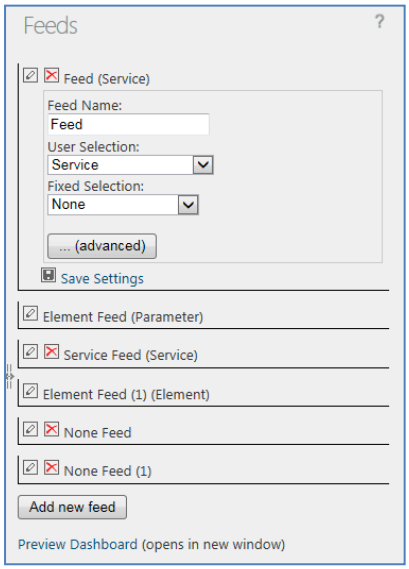


Figure 10-49. Feeds

10.9.2.4 Settings

Go to **Actions > Settings** to get access to the general dashboard settings.
You can configure several options here:

- To make the dashboard pop up in a smaller window, select **Popup as Mini Dashboard** and enter a width and height for the mini dashboard.
- Click the **…** button under **Background Image** to choose a background image for the dashboard.
- Choose a **Background Mode** to set how the background image is shown.
- Click the **…** button under **Text Color** to set the text color of the dashboard.
- Under **Extra CSS**, you can set advanced customizations.

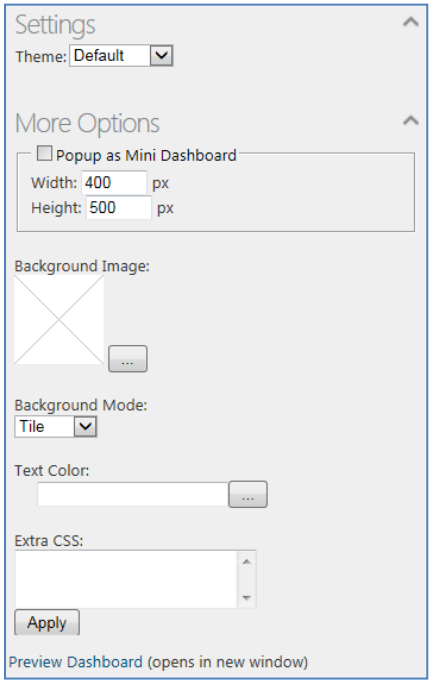


Figure 10-50. Settings

10.9.3 Create a Dashboard Container

It is possible to combine several dashboards in one dashboard container in the NetVue Cube. When you open the dashboard container, the different dashboards will be available as tab pages, so that you can easily navigate among them.

To create a new dashboard container in the NetVue Cube:

1. Go to **Start > Apps > Reports & Dashboards.**
2. In the column on the left, click **Dashboards.**
3. Under **Available Dashboards**, click **New dashboard container**. A new dashboard container is added to the list.
4. Next to **Title**, fill in a title for the dashboard container.
5. These configuration options are available also:
    a. Click the **…** button next to **Theme** to change the theme for the dashboard container. A personal theme can overrule this theme.
    b. Next to **Description**, you can add a description with additional information about the dashboard container.
    c. You can select a folder for the dashboard container in the drop-down list on the right. To create a new folder, select **<Create New>**.
6. Under **Included dashboards**, for each dashboard to be included in the container, select the dashboard in the drop-down list and click **Add**.
7. Click **Save Configuration** to save the dashboard container.

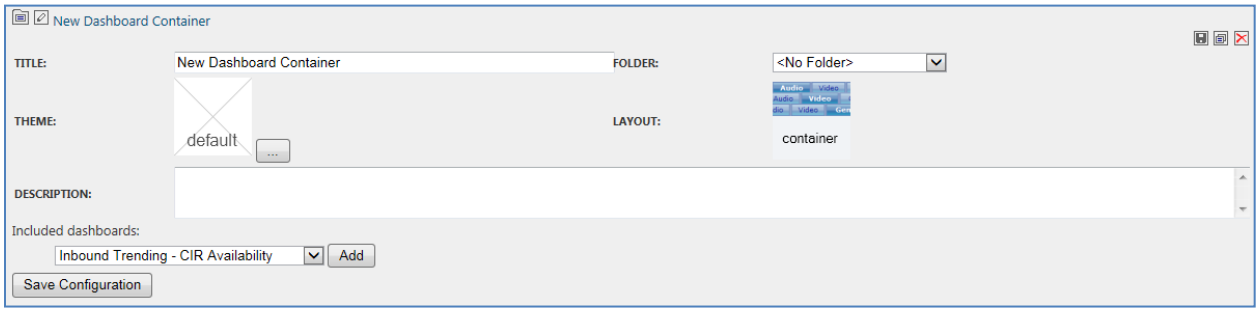


Figure 10-51. New Dashboard Container

10.9.4 Manage Dashboards

To see the existing dashboards and dashboard containers in the NetVue System:

1. In the NetVue Cube, go to **Start > Apps > Reports & Dashboards.**
2. In the column on the left, click **Dashboards.**

Under **Available Dashboards**, you will see a list of the existing dashboards and dashboard containers, where several actions are possible.

10.9.4.1 Activate / Deactivate a Dashboard

To activate a dashboard:

- In the list of dashboards, click the grayed-out Activate/Deactive icon to the left of the applicable dashboard.

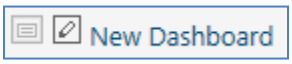


Figure 10-52. Active Dashboard

To deactivate a dashboard:

- In the list of dashboards, click the Activate/Deactivate icon to the left of the applicable dashboard.

Figure 10-53. Deactivate Dashboard

New dashboards are activated by default.

10.9.4.2 Editing a Dashboard

To edit a dashboard:

- In the list of dashboards, click the pencil icon to the left of the dashboard name.

  You have the same options as during dashboard creation.

10.9.4.3 Duplicating a Dashboard

To duplicate a dashboard:

1. In the list of dashboards, click the pencil icon to the left of the dashboard name.
2. Click the **Duplicate Dashboard** icon that shows to the right of the dashboard name.
3. To finish the duplicated dashboard, do the same steps as during dashboard creation.

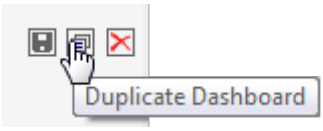


Figure 10-54. Duplicate Dashboard

10.9.4.4 Deleting a Dashboard

To delete a dashboard:

1. In the list of dashboards, click the pencil icon to the left of the dashboard name.
2. Click the red x icon that shows to the right of the dashboard name.
3. In the confirmation box, click **OK** to confirm the deletion.

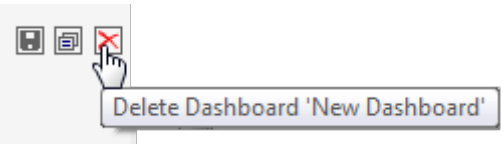


Figure 10-55. Delete Dashboard

Chapter 11. TRENDING

11.1 Trending

With NetVue trend graphs, you can see and compare trend data logged by the NetVue System. For performance reasons, trending activates for a limited number of parameters by default. NetVue administrators activate trending for a parameter only if it makes sense to do so.

11.2 Trending Techniques

There are two trending techniques:

1. **Real-time trending** – Logging of all values, in a sliding window of maximum 1000 hours

   In most cases, real-time trending is set to 24 or 48 hours.

2. **Average trending** – Logging of average values only, usually across longer time spans than those used for real-time trending.

   a. Last 48 hours, with 5-minute averages.

   b. Last week, with 5-minute averages (max. 2016 data points).

   c. Last month, with 5-minute averages (max. about 8640 data points).

   d. Last year, with 1-hour averages (max. about 8760 data points).

In case of average trending, NetVue stores the average value for a time slot, and the minimum and maximum value detected in that same time slot.

11.3 Trend Graphs

In the NetVue Cube, see trend information by drilling down for a particular parameter, or use the Trending app. You can combine trend information for several parameters in a trend group, then save it for further use.

11.3.1 View Trend Graphs

In the NetVue Cube, you can show trend information in a trend graph for any parameter that is being trended. You can go to the trend information from cards, or from the Trending app.

11.3.1.1 View Trend Information from a Card

To see trend information for a parameter:

1. Open the card that has the parameter for which you want to see trend data.
2. On the data display side of the card, go to the page that has the desired parameter.
3. Double-click the parameter, or click the trend icon next to the parameter.
    - The trending information for the last 24 hours is loaded in the main graph, and the information for the past week is loaded in the preview graph below that. Below the main trend graph, a colored bar shows the alarms happening at the time shown on the X axis.
4. Optionally, switch between different time spans for the main trend graph by clicking the buttons in the top-right corner:
    - Last 24 Hours.
    - Week to Date.
    - Month to Date.
5. To return to the card, click **Up to Data Display.**

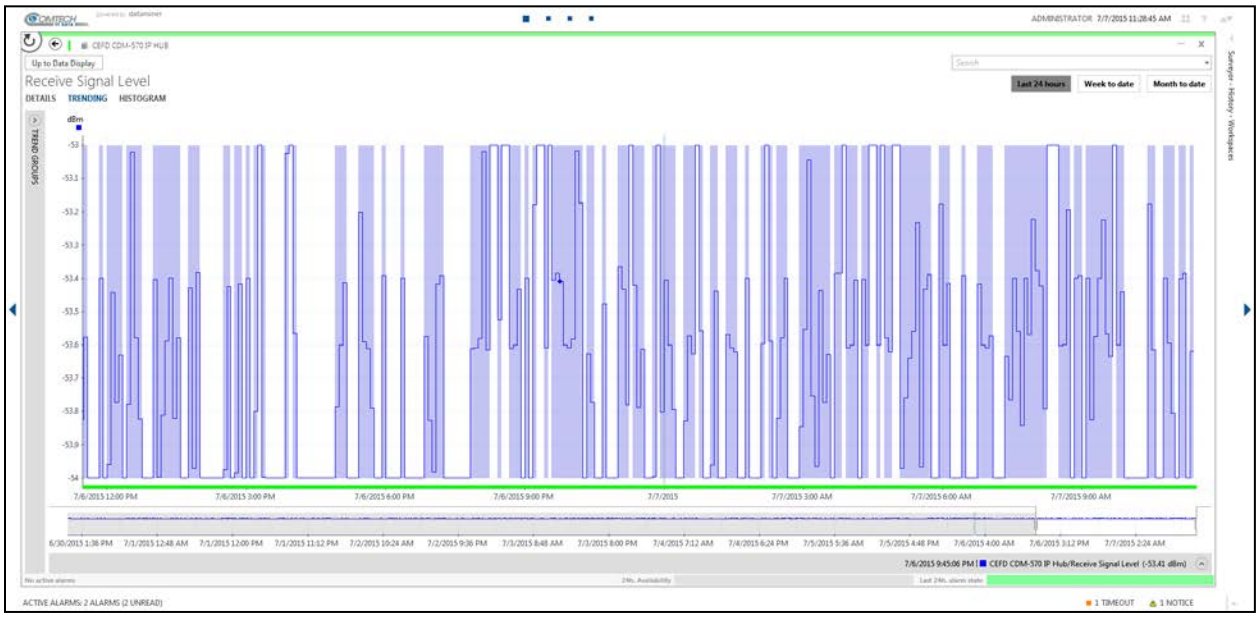


Figure 11-1. Card Trending Example

11.3.1.2 Showing Alarm Colors

In the user settings, you can configure the way alarm severity levels show in trend graphs.

To cause trend graphs to show alarm template colors:

1. Go to **Settings > Datadisplay.**
2. Select the user setting **Show alarm template colors on vertical axis.**

By default, the colors show in a colored line along the Y axis. Alternatively, colored bands can be shown behind the trend graph instead.

To switch between these settings:

1. Go to **Settings > Datadisplay.**
2. In the drop-down list next to **Display the alarm template in the trend graph**, select either **Line** or **Band.**

Figure 11-2. Show Alarm Colors Example

11.3.1.3 Go to Trending from the Trending app

The NetVue Cube has a Trending app, where you can see trending information for individual parameters and for groups of parameters.

To go to trend information from the Trending app:

1. Go to **Start > Apps > Trending.**
2. In the parameter pane at the bottom of the app, click **Add parameter.**
3. Select the element and parameter for which you want to see trending information. For a dynamic table parameter, specify the index also.
4. Click **Show trend.**

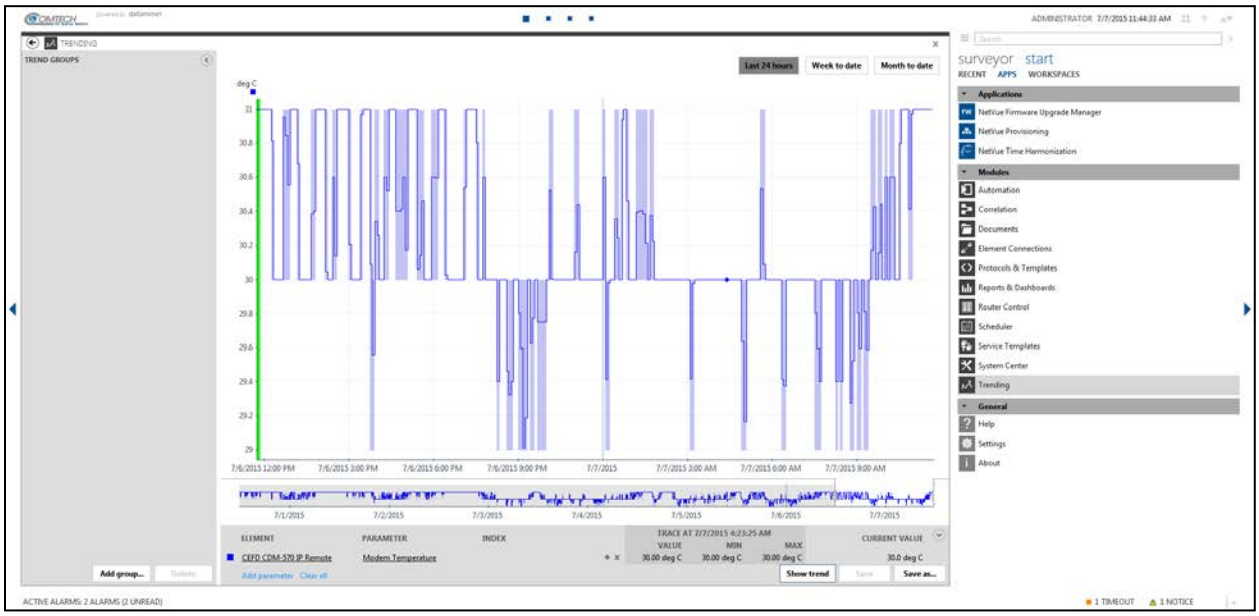


Figure 11-3. Trending App Example

11.3.2 Manipulate Trending Graphs

Whether you go to a trend graph from a card or do so from the Trending app, the user interface consists of:

- A main graph area with a preview graph underneath
- A parameter pane at the bottom
- A trend groups pane on the left-hand side

You can change the way the data shows in the main graph by directly manipulating the trend graph, or using the right-click menu.

When you zoom in on a graph, more detail is added to the graph up to a maximum level. This level depends on the configuration, particularly on whether real-time trending is enabled or not.

11.3.2.1 Manipulate Trending Graphs with the Mouse

With the mouse, you can make these changes to the way data is shown in a trend graph:

- To see the details of a point on the graph, hold the cursor over that point on the graph. The details show in the parameter pane below.
- To move the graph to the left or right, hold the right mouse button and drag the graph in either direction.
- To zoom in on a part of the graph, hold the left mouse button and drag the graph, or use the mouse scroll wheel.

You can use the bottom preview graph also. This is the small graph at the bottom of the graph window. It represents the entire trend period (week, month, etc.). The large graph at the top is an enlargement of the white part of the bottom graph.

11.3.2.2 Using the Preview Pane

With the preview pane, these changes are possible:

- Scroll through the main graph by dragging the white part of the bottom graph to the left or to the right.
- Reset the starting point or the ending point of the main graph by dragging the boundaries in the bottom graph to the left or to the right.

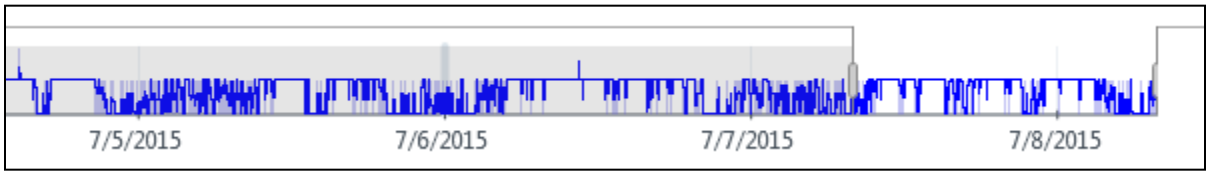


Figure 11-4. Preview Pane Example

11.3.2.3 Using the Right-Click Menu

When you right-click anywhere in the graph window, a shortcut menu opens that contains these commands:

Zoom to last hour/day/week/month/year –zooms in on a specific time frame.

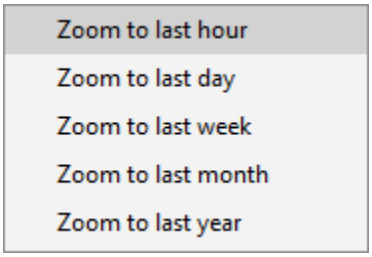


Figure 11-5. Zoom Example

Curves – you can remove a curve from a graph, or put a curve on an additional Y axis (if the units are identical).

Curves > Show Min/Max – additional option under **Curves**, enables or disables showing minimum and maximum values. When you enable this option, the minimum and maximum values show in a colored area behind the curve. By default, the option is disabled for trend graphs with multiple parameters.

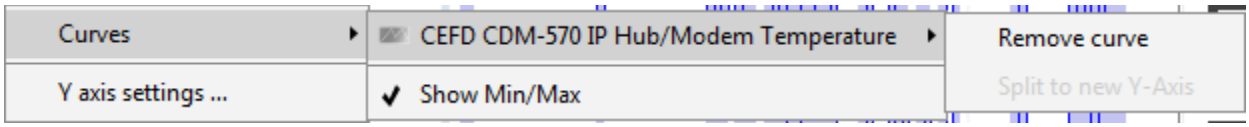


Figure 11-6. Curves Example

Y axis settings – use these settings to customize the range of the Y axis. In the **Y axis settings** window, choose one of two options:

- **Auto**, the scale is set automatically
- **Range**, you set a minimum and maximum manually, and control whether exception values are included

Print – prints the trend graph that is showing

Save image – saves the trend graph as an image file (.png or .jpg)

Copy to clipboard – copies the trend data to the Windows Clipboard. You can then paste it into third-party applications like Microsoft Word or Microsoft Excel.

Export to csv – exports trend data to a CSV file. When you select this command, the **Export trend graph to CSV file** window opens, where you can specify:

- Which curves must be exported
- Which data must be exported: all or a custom data set
- Whether to export a block graph or a line graph; a line graph is a reduced format containing only one value per time stamp.

Show most detailed data – select this option to show the most detailed data, instead of average data.

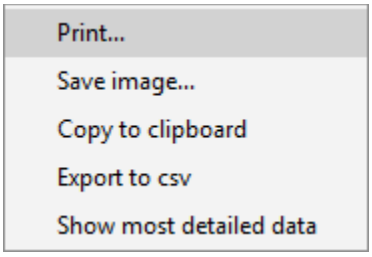


Figure 11-7. Print, Copy, Save Example

11.3.3 Trends in a Histogram

When you find parameter trend information for a parameter on a card, you can choose to see the information in a histogram instead of a trend graph. Additionally, you can see a histogram with trend information from the back of a view card.

In a histogram:

- The X axis represents the parameter value, shown in intervals
- The Y axis represents the number of times the parameter value occurred in the given time span

11.3.3.1 View Trends in a Histogram

1. Go to the trend information for a parameter on a card.
2. Above the trend graph, click **Histogram.**
3. To specify advanced options, below the histogram, click **Advanced:**
    - Next to **Start time** and **End time**, specify a custom time interval to show in the histogram.
    - Next to **Interval width**, specify a custom interval width.
    - Next to **Minimum value** and **Maximum value**, specify a different range for the histogram.
4. To change the range of data shown, you can also:
    - Zoom in on a particular section, by holding the left mouse button down while dragging, or using the mouse scroll wheel.
    - Pan the graph along the X axis, by holding the right mouse button down while dragging.

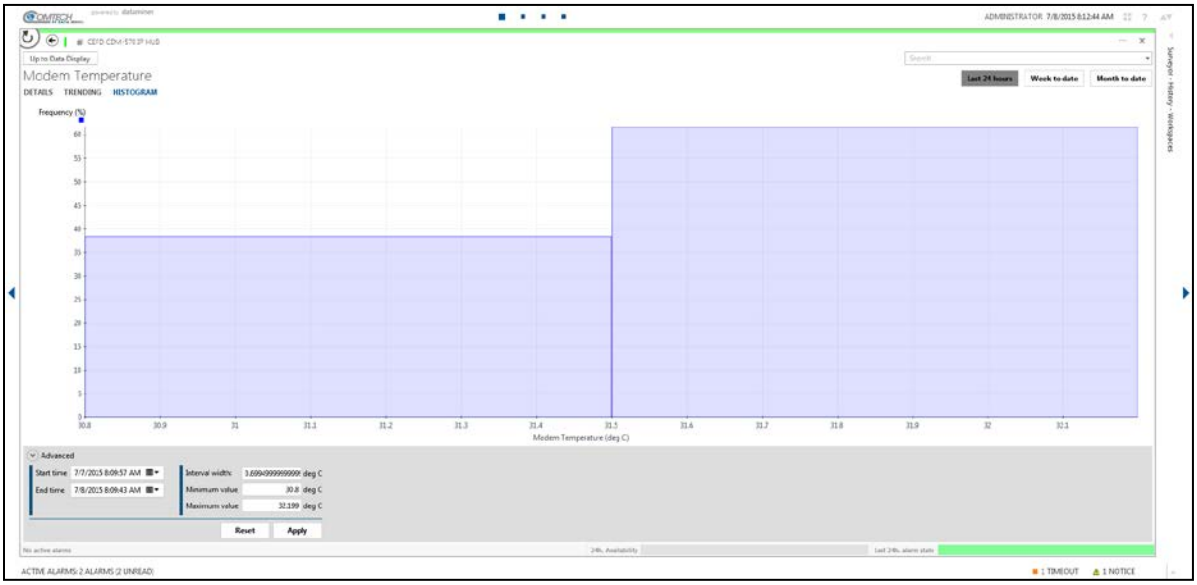


Figure 11-8. Histogram Example

11.3.3.2 View Trends in a Histogram on Back of View Card

At the back of a View card, in the histogram tab, you can select a parameter to see its trend information in a histogram. You can save and load presets for a histogram as well.

To see a parameter in a histogram, across the different elements in a view:

1. On the back of a view card, go to the **Histogram** tab.
2. Select a protocol, a protocol version and a parameter. In case of a table parameter, also specify an index.
3. Click **Load Histogram**.
4. Optionally, in the **Advanced** section, specify a custom interval width and value range (minimum and maximum values).
5. Click **Apply.**

To change the type of Y axis from the default setting of absolute values (the number of occurrences) to relative values (% of total occurrences), right-click the histogram and deselect **Use absolute frequency**.

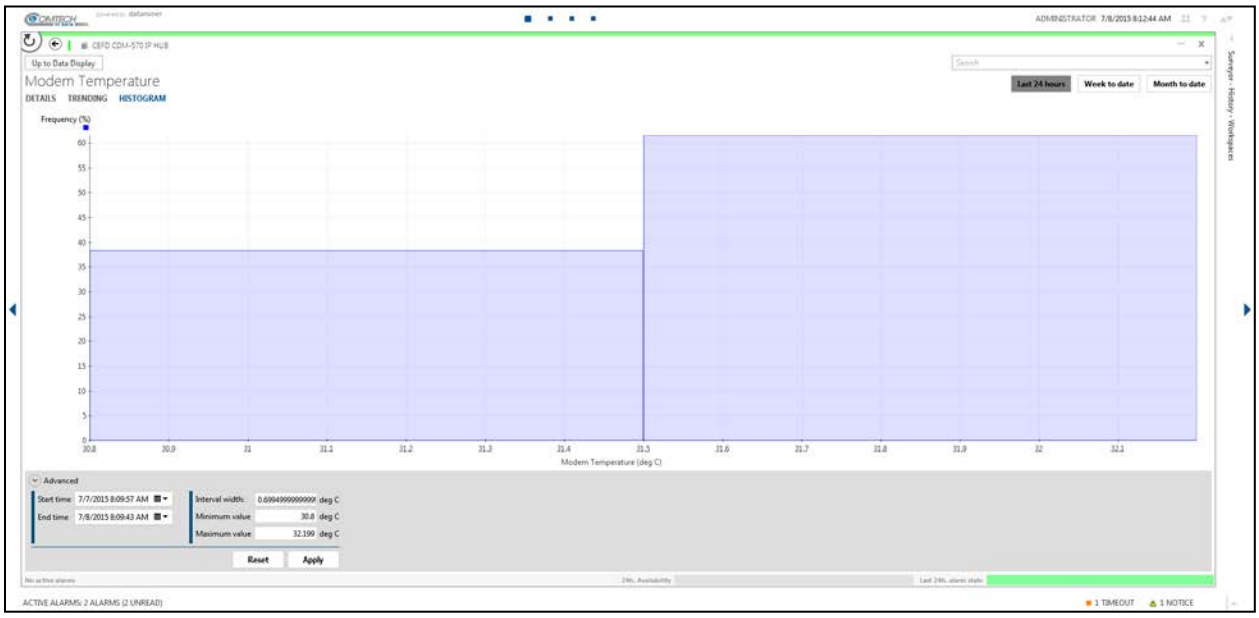


Figure 11-9. Histogram (View Card) Example

To save your selections as a preset:

1. Expand the **Presets** pane on the left side of the window.
2. Click the **Add preset** button.
3. In the **Settings** window, select the preset type: **Private, Protected** or **Public.**
4. Enter a name, and optionally a description, for the preset.
5. Click the **Save** button.

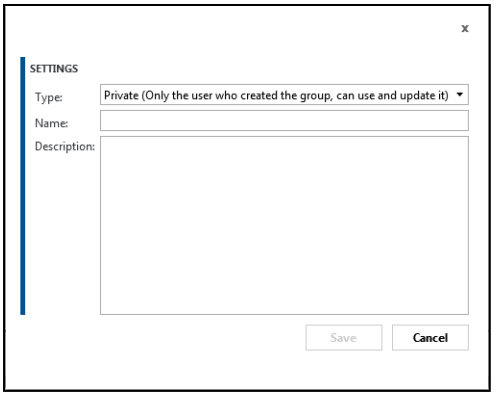


Figure 11-10. Add Preset Example

To delete a preset:

1. Select the preset in the **Presets** pane
2. Click the **Delete** button, and then click **Yes** in the confirmation window

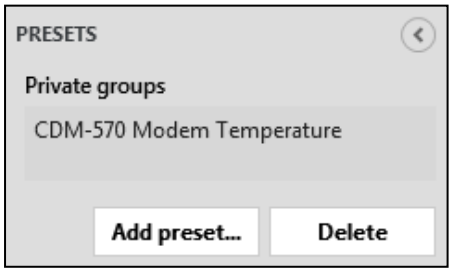


Figure 11-11. Delete Preset Example

11.3.4 Trend Groups

In the NetVue Cube, you can show trend information associated with individual parameters or with groups of parameters. The latter are called trend groups.

Create and manage trend groups with the side and bottom panes in the Trending window:

- In the trend groups pane on the left-hand side, see, add or delete trend groups.
- In the parameter pane at the bottom, add or remove parameters from a trend group.

By default, these panes are collapsed. You can expand them with the expand button.

11.3.4.1 Trend Groups Pane

In the trend group pane on the left-hand side, you can add or delete trend groups, or select trend groups to see and update them.

11.3.4.1.1 Add a Trend Group

To add a trend group:

1. Click the Add group button.
2. Specify the type of trend group:
   - Private – only you can use or update the trend group.
   - Protected – other users in the NetVue system can use the trend group, but only you can update it.
   - Public – all users in the NetVue system can use and update the trend group.
3. Specify a name for the trend group.
4. Optionally, add a short description in the Description field.

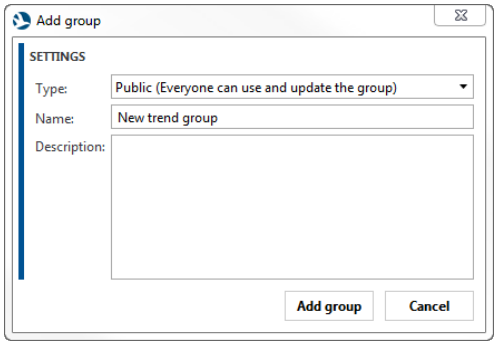


Figure 11-12. Add Trend Group Example

11.3.4.1.2 Delete a Trend Group

To delete a trend group:

- Select the trend group and click the **Delete** button.

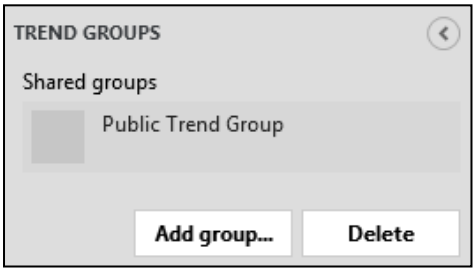


Figure 11-13. Delete Trend Group Example

11.3.4.1.3 Update a Trend Group

To update a trend group:

1. Click the trend group in the trend group name. It is then loaded in the main graph area.
2. Add or remove parameters in the parameter pane, then click the **Save** button.

11.3.4.2 Parameter Pane

In the parameter pane, you can add as many parameters as needed to create a trend group. You can duplicate or delete Parameters also.

Additionally, it functions as a graph legend for the main graph area. As you move the mouse over the graph, the timestamp of the trace dot shows, as well as the trace value of every parameter, even when the pane is collapsed. When the pane is expanded, it shows the average, minimum and maximum value of the parameter at the time.

Figure 11-14. Parameter Pane Example

To add parameters using the parameter pane:

1. Click **Add parameter** or drag an element or parameter onto the graph from the navigation pane.
2. Specify the element and parameter, if necessary. For a table parameter, you might be required to specify the index also.
3. Repeat step 1 until all necessary parameters have been added.
4. To save the trend group, click **Save as**.

These additional functions are available:

- When you add a new parameter, the parameter at the bottom of the list is duplicated by default. However, to add a parameter similar to a different parameter in the list, duplicate it using the + icon to the right of the parameter.
- To remove one of the parameters in the pane, click the x icon to the right of the parameter.
- To see the added parameters in the trend graph, click **Show trend**.
- To start over and remove all added parameters, click **Clear all.**

11.4 Trend Templates

Use Trend templates to select which parameters and what kind of trending information is logged in the trending database.

In a trend template, you define both the scope and the type of trend information stored:

- **Scope** – choose which parameters of an element are to have trending information stored. You can choose different parameters for different elements.
- **Type** – choose **Real-Time** or **Average** trending, or a combination of both.
    - **Real-time trending** – this is continuous logging of all measurements, in a sliding window of 1000 hours, maximum.
    - **Average trending** – this logs average trending per time slot. The time slot depends on the size of the window.

11.4.1 Add / Delete Trend Templates

11.4.1.1 Create a Trend Template

1. Go to **Start > Apps > Protocols & Templates**.
2. Select a protocol in the first column and a protocol version in the second column.
3. Right-click in the third column under **Trend**, and select **New.**

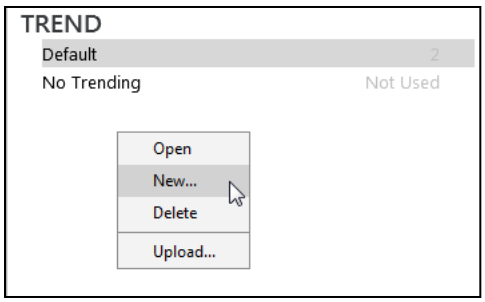


Figure 11-15. New Template Example

4. In the **New trend template** dialog box:
   a. Enter a template name.
   b. Check if the protocol and protocol version are correct; change if necessary.
   c. Click **OK.**

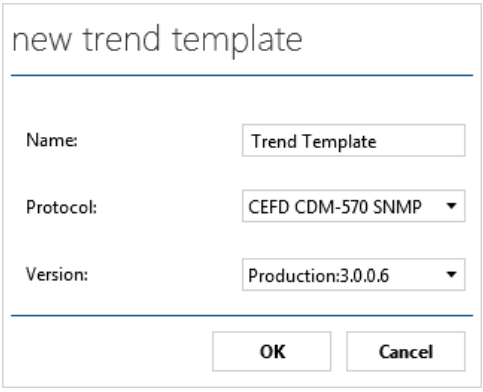


Figure 11-16. New Template Dialog Box Example

11.4.1.2 Upload a Trend Template

1. Go to **Start > Apps > Protocols & Templates.**
2. Select the protocol in the first column and the protocol version in the second column.
3. Right-click under **Trend** in the third column and select **Upload.**
4. Browse to the trend template in question and click **Open.**

11.4.1.3 Delete a Trend Template

1. Go to **Start > Apps > Protocols & Templates.**
2. Select the protocol in the first column and the protocol version in the second column.
3. Right-click under **Trend** in the third column and select **Delete.**

11.4.2 Configure Trend Templates

1. Open the template editor using either of these methods:
   a. Go to the **Protocols & Templates** app, right-click the template and select **Open.**

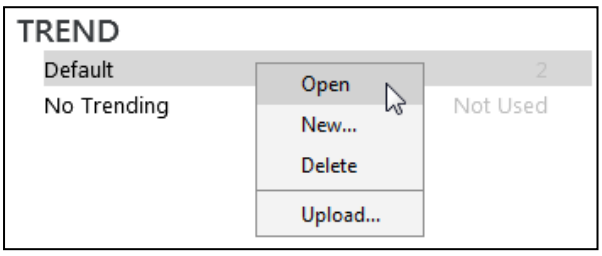


Figure 11-17. Open Template Example

- or -

b. Right-click an item in the Surveyor and select **View > Trend template.**

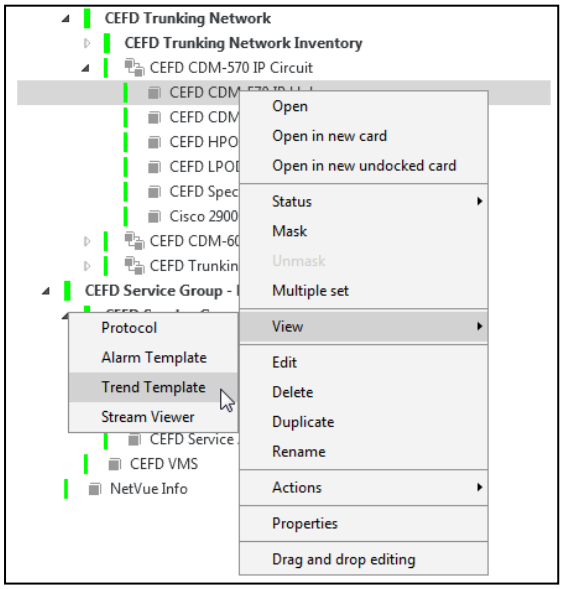


Figure 11-18. View Template Example

In the template editor, you can do any of these tasks:

- Use the filter box in the top right corner to find a parameter quickly.
- In the **General** section, click **Show details** and enter a description in the description field.
- For each parameter, to activate trending for the parameter, select the check box for **REAL**-**TIME** or **AVERAGE** trending.

When ready, click **Apply** to apply the trend template, or click **OK** to apply the trend template and exit the editor.

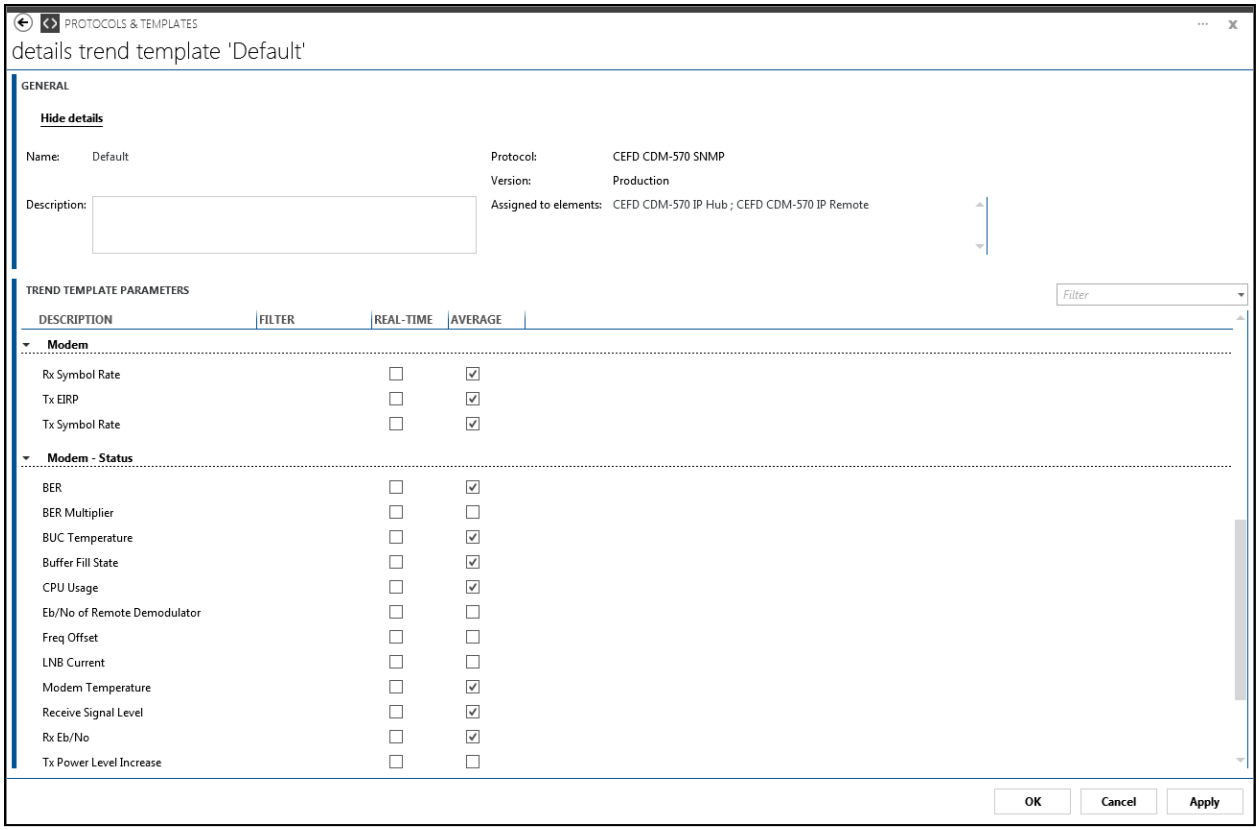


Figure 11-19. Template Editor Example

11.4.3 Assign Trend Templates

You can assign a trend template to an item with the Surveyor right-click menu, or from within the Protocols & Templates app.

In the Surveyor:

1. Right-click the item to which a trend template must be assigned, and click **Edit.**
2. In the **Edit** tab, go to **Device Details.**
3. Select the trend template in the **Trend Template** selection box.
4. Click **Apply.**

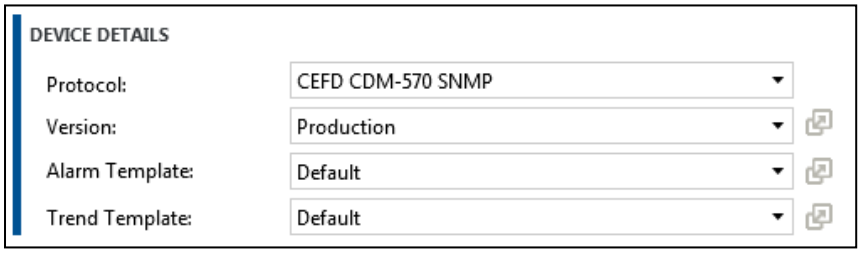


Figure 11-20. Assign Template (Surveyor) Example

In the Protocols & Templates app:

1. Select the protocol and protocol version.
2. In the **Trend** section, select the trend template.
3. Right-click in the **Elements** section.
4. Select **Assign Template.**
5. In the **Assign template** window, use **Add >>** and **Remove >>** buttons to assign the template to specific items.

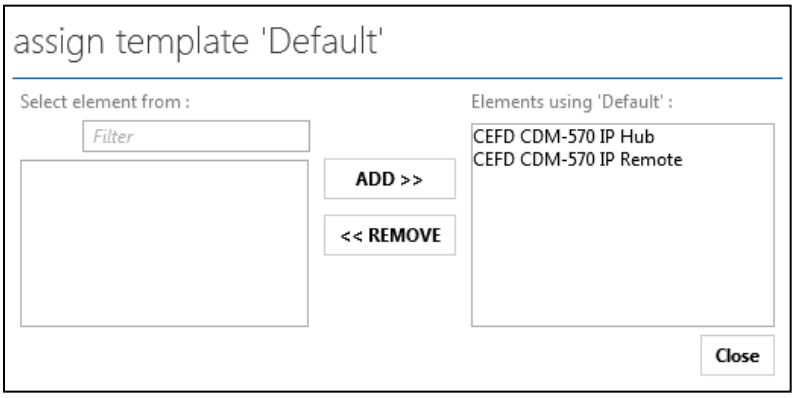


Figure 11-21. Assign Template (App) Example

Chapter 12. CORRELATION IN NETVUE CUBE

12.1 Overview

Correlation in the NetVue Cube automatically analyzes raw alarm information and real-time parameter values, and acts upon that information according to the rule sets you define in its knowledge base. It is capable of detecting single events, persistent and recurring events.

Based on the rules you set, Correlation can create correlated alarms or send notifications via SMS or email. These alarms and notifications inform operators about events.

Correlation can trigger Automation scripts as well, so that automatic countermeasures are possible in case of emergency, or preventive actions can occur in case of emerging issues.

12.2 Edit or Organize Correlation Rules

To see, edit or organize Correlation rules in NetVue Cube, open the Correlation app.

Go to ***Start > Apps > Correlation***.

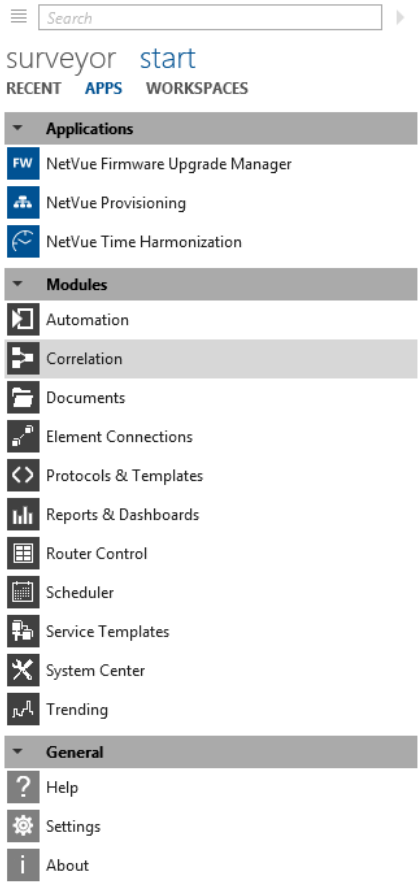


Figure 12-1. Apps Menu Example

12.3 Manage Correlation Rules in NetVue Cube

When you open the Correlation app, you see a card with a left pane and a right pane.

On the left pane, all rules show in a tree view. Use the search box at the top of the pane to find a rule quickly.

Manage Correlation rules in the left pane. Adding and deleting rules or organizing them in folders are some examples.

On the right pane, rule details show. Here, you can see and edit rules.

You can see the rule details in a separate card as well. To do this, right-click the rule and select **Open in new card** or **Open in new undocked card**.

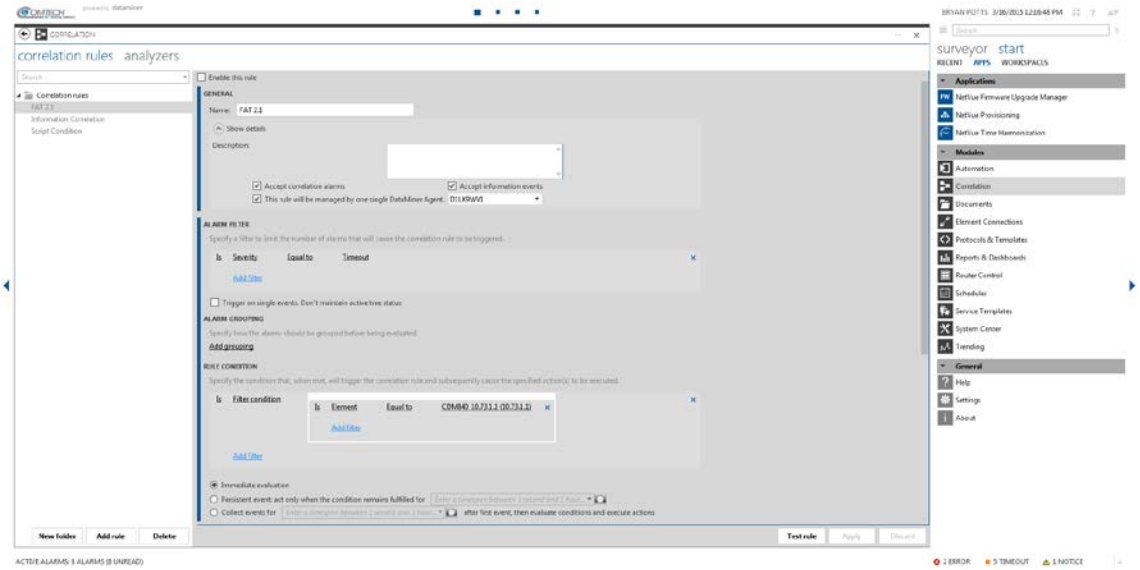


Figure 12-2. Correlation Rules Example

12.3.1 Collapse and Expand Folders

You can collapse or expand folders in the tree view. If you select **Collapse all**, the root folder does not collapse. To collapse or expand folders:

Click the triangle in the front of the folder;

- or -

Right-click the tree view and select **Collapse all** or **Expand all.**

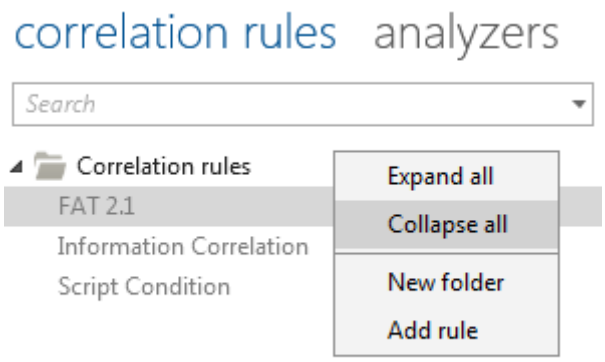


Figure 12-3. Correlation Rules Folder Options

12.3.2 Add a New Folder

When you create a new folder, it is saved only if a rule is added to it. Empty folders are deleted automatically when you close the Correlation app.

To add a new folder:

Click the **New Folder** button at the bottom of the pane;

- or –

Right-click a folder where a new folder must be added, then select **New folder.**

12.3.3 Move Rules or Folders

To move rules or folders in the Correlation tree view, drag the rule or folder and drop it in the new location in the tree view.

12.3.4 Delete a Rule or Folder

To delete a Rule or Folder:

Select the rule or folder, and then select the **Delete** button at the bottom of the pane;

- or -

Right-click the rule or folder, and then select **Delete** in the right-click menu.

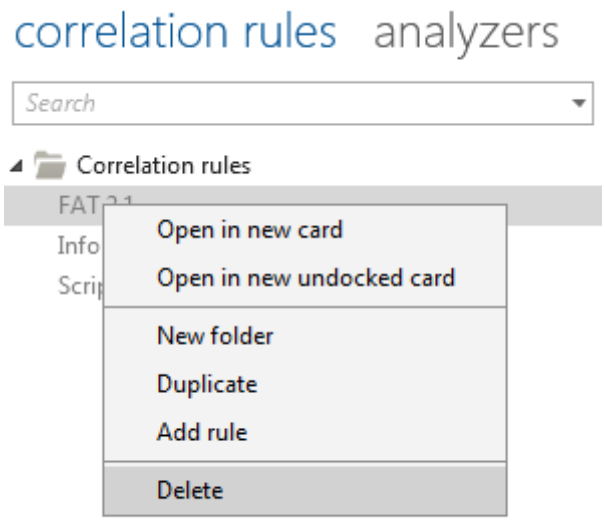


Figure 12-4. Delete a Correlation Rule or Folder

12.3.5 Rename a Folder

To change the name of a folder:

Right-click the folder, and select **Rename;**

- or -

Select the folder, and press ***F2.***

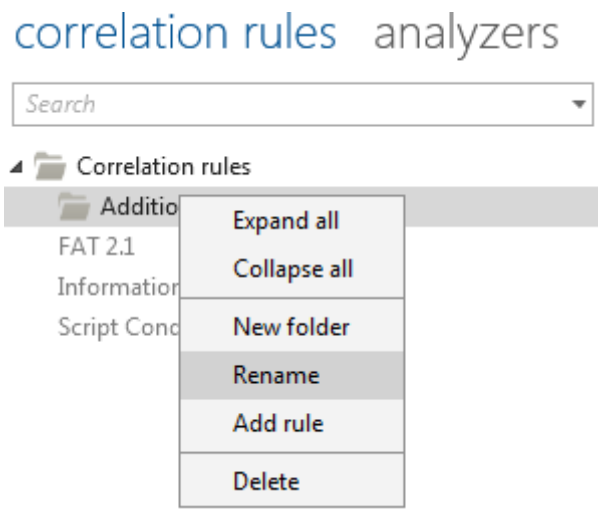


Figure 12-5. Rename a Folder

12.3.6 Add a New Correlation Rule

To add a new rule:

Select the folder where you want to add the rule, and click the **Add** button at the bottom of the pane;

- or -

Right-click the folder where you want a new rule and select **Add Rule;**

- or –

Right-click an existing rule and select **Duplicate**. Change the new duplicate rule as necessary.

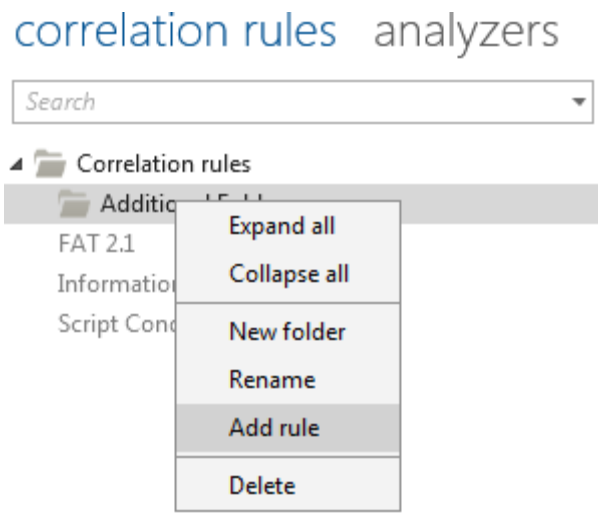


Figure 12-6. Add a Correlation Rule

To create a functional new rule, you must do these tasks as well:

- Give the rule a name and configure general options. See **General configuration of Correlation rules**.
- Optionally, filter out alarms that can trigger the rule. See **Filtering and grouping base alarms for Correlation rules.**
- Add rule conditions that can activate the rule. See **Adding rule conditions in Correlation rules.**
- Add rule actions that occur when the rule is activated. See **Adding rule actions in Correlation rules.**

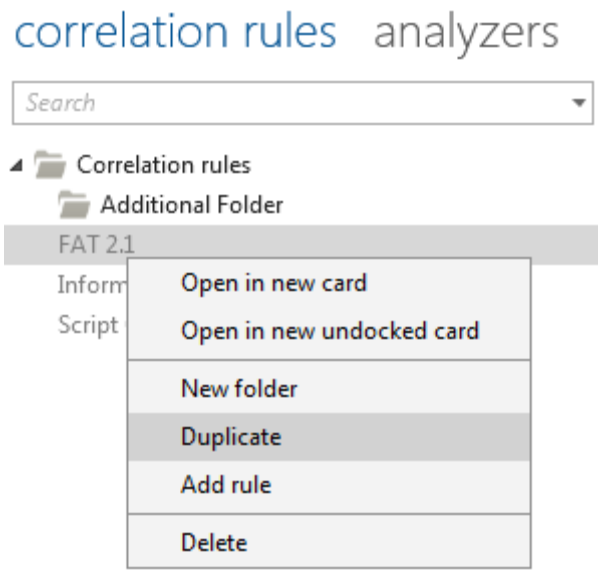


Figure 12-7 Duplicate a Correlation rule

12.3.7 Test a Correlation Rule

1. Open the Correlation app.
2. Select the rule in the tree view.
3. In the details pane, click the **Test rule** button

If the rule has errors, the button is disabled.

4. Specify the time range for the historical alarms against which the rule is to be tested.
5. Click **Test.**

   The results show in the test results window. Results include the correlated alarms and the corresponding base alarms.

12.3.8 General Configuration of Correlation Rules

In the Correlation app, select a rule in the tree view pane on the left so that you can configure it in the details pane on the right.

In the top left corner of the pane, select **Enable this rule** to enable a Correlation rule. By default, new rules are disabled.

In the **General** section, next to **Name**, enter a new name for the Correlation rule. By default, new rules are named **Correlation rule**.

In the **General** section, click **Show details** to specify the general properties of a Correlation rule.

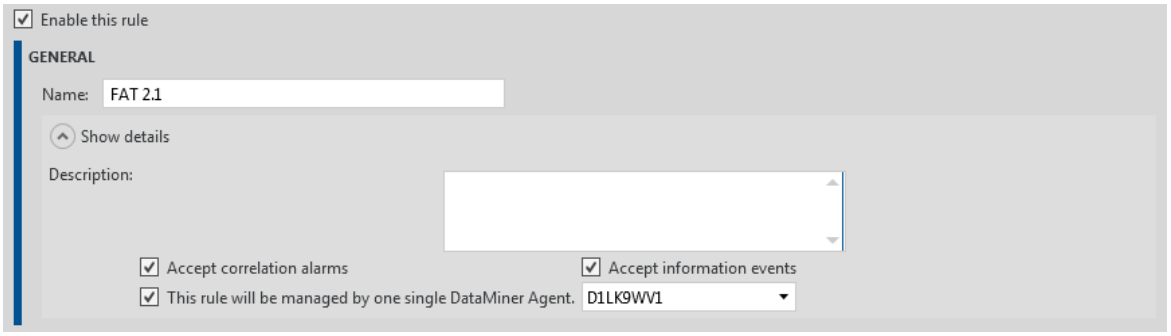


Figure 12-8. Show Details Example

Description

A short text that describes the Correlation rule.

Accept correlation alarms

Select this option to cause Correlation alarms to activate the Correlation rule.

Be careful when using this option. Depending on alarm filter settings and rule conditions, it could cause an endless loop, where the correlation rule is triggered and generates a correlated alarm, which triggers the rule again, etc.

Accept information events

Select this option to cause information events to activate the Correlation rule.

Be careful when using this option. Make sure there are no information events generated by the correlation rule that can trigger the rule again, causing an endless loop.

This rule will be managed by one single DataMiner Agent

By default, every DMA in the NetVue System checks the enabled Correlation rules against the alarms associated with locally managed elements.

If you select this option and you select a DMA in the selection box on the right, then only the selected DMA can evaluate the Correlation rule you are creating. The selected DMA must check the rule against all alarms generated in the NetVue System.

To cause a new correlation alarm to be created for every change to an alarm:

In the **ALARM FILTER** screen section, select **Trigger on single events. Don't maintain active tree status.**

If you do not select this option, the same Correlation alarm is updated for every new status.

This setting is important for Correlation rules that use a number of separate alarm events as the trigger. If the option is not selected, recurring alarms contained within the same alarm tree are not considered separate events.

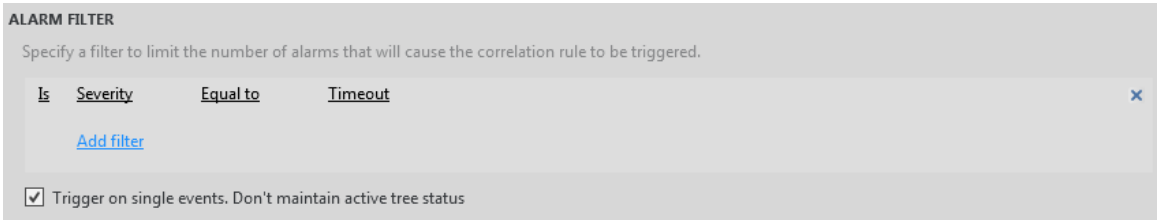


Figure 12-9. Alarm Filter Example

12.3.9 Filter and Group Base Alarms for Correlation Rules

In the Correlation app, select a rule in the tree view pane on the left to configure filters or groupings in the details pane on the right.

12.3.10 Add Alarm Filters to Correlation Rules

If no alarm filtering is used, the conditions are evaluated for all alarms. It is best to use alarm filtering whenever possible, to reduce the load on the system.

In the **Alarm Filter** section of the details pane, you can create a filter to limit the alarms that the Correlation rule evaluates.

1. Click ***Select a Filter.***
2. Select one of the listed properties and create an alarm filter;

   - or -

   Select ***Saved filters*** and select an existing alarm filter.
3. To add another condition to the filter, click ***Add a Filter,*** *then* repeat step 2.
4. To delete one of the filter conditions, click the X to the right of the filter.

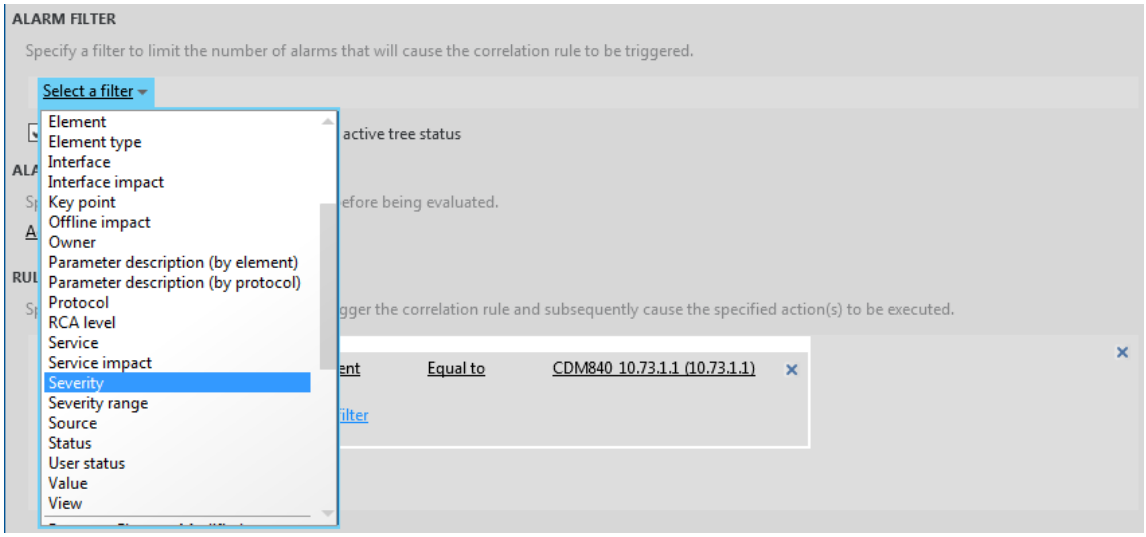


Figure 12-10. Select a Filter

12.3.11 Limit the Base Alarms

You can limit the base alarms for a correlation rule, as an alternative to, or in addition to, adding alarm filters.

1. In the **Actions** section, click **Add Option**.
2. Select **Limit the base alarms**.
3. Click **Select a filter**.
4. Select one of the listed properties.
5. Create a filter condition;

   - or -

   Select **Saved filters** and select an existing filter.
6. If necessary, select the option **Include all Alarms generated … before and after the moment this rule was triggered.**

   a. Specify a time span.

When you select this option, any alarms that match the filter and occur within the specified time span are included in the same correlation alarm.

You can select this option without specifying a filter. In this case, any alarm events that match the rule detected during the indicated time span are included as base alarm events.

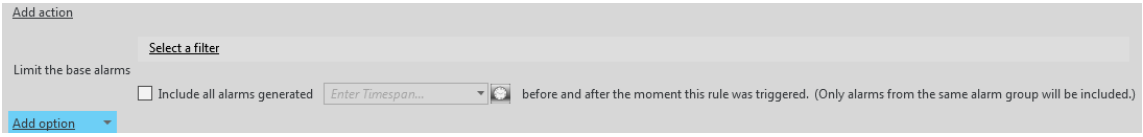


Figure 12-11. Add Action Example

12.3.12 Group Alarms in Correlation Rules

With the NetVue Cube Correlation engine, you can group alarms matching the same criteria into separate correlated alarms. For example, you can group all alarms from various services into one correlated alarm per service.

In the **Alarm Grouping** section of the details pane, specify the manner in which the alarms must be grouped before they are evaluated.

1. Click ***Add grouping***
2. Select one of the listed grouping options:

by alarm	by component info	by DataMiner	by element	by key point
by service	by parameter	by property value	by table index	by view

   If you have alarms grouped by view, and an alarm event occurs on an element that is in more than one view, the alarm is added for each of these views. However, only elements directly under a view are grouped. Elements from sub-views are not part of the same group.

3. To select an additional grouping method, go back to Step 1.
4. To move one of the grouping methods up or down in the list, hold the mouse cursor over the method and click an up or down triangle.
5. To delete one of the grouping methods, hold the mouse cursor over the method and click the ***X***.

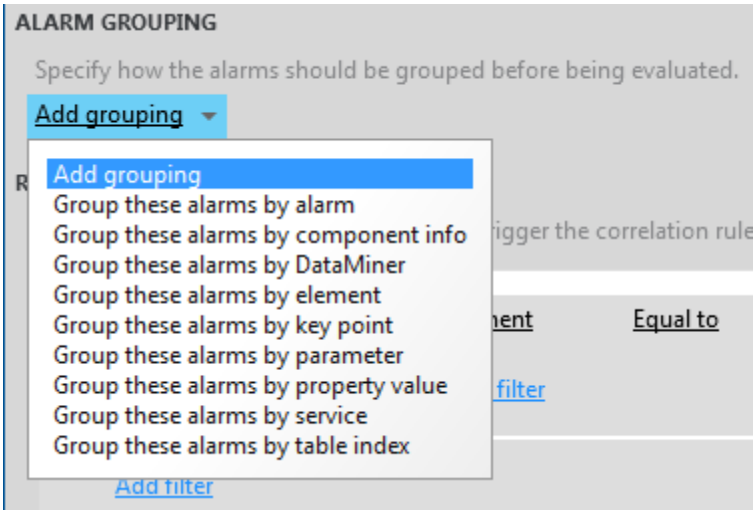


Figure 12-12. Add Grouping Example

12.3.13 Add Rule Conditions in Correlation Rules

In the Correlation app, select a rule in the tree view pane on the left, then add rule conditions to it in the details pane on the right.

In the **Rule condition** section of the details pane, specify one or more conditions that activate the Correlation rule. You can select and combine Script conditions and Fir conditions, and specify one of different activation mechanisms. In the **Sliding window** section, you can select an additional activation mechanism.

1. Click ***Select a Condition***.
2. Select either ***Script condition*** or ***Filter condition.***
3. If you selected ***Script condition***, enter the script in the large text box.

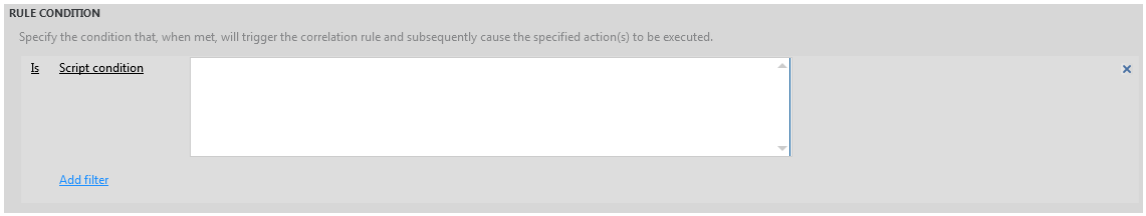


Figure 12-13. Script Condition Example

4. If you selected **Filter condition**, do these steps:
   a. Click ***Select a filter.***
   b. Select one of the listed properties and create a filter condition;

      or -

      Select Saved filters and select an existing alarm filter.

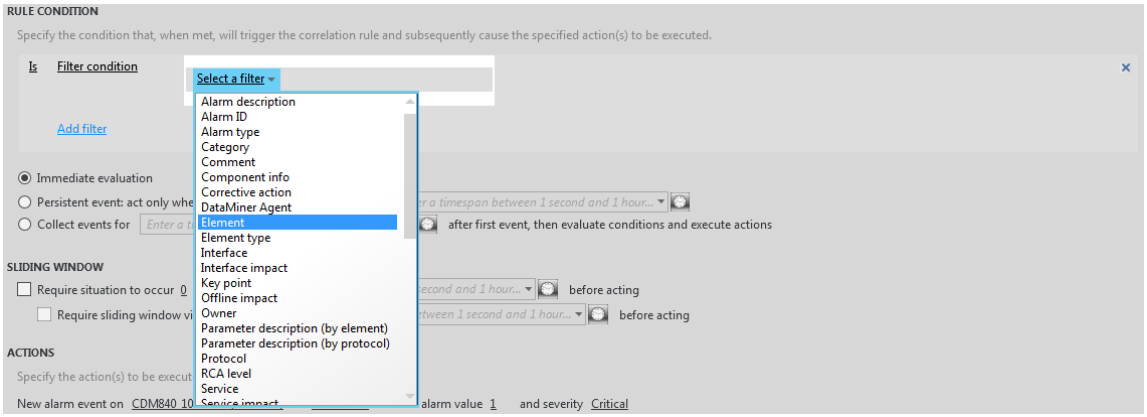


Figure 12-14. Select a Filter Example

5. If this is the first (or only) rule condition, select ***Is*** or ***Is Not*** to specify whether the condition must be true or false.

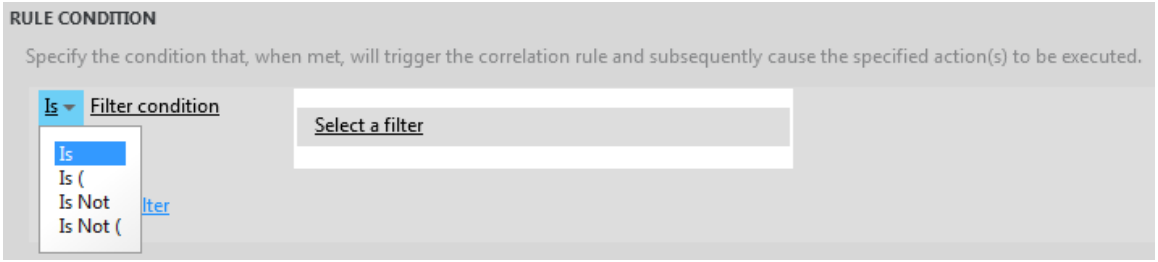


Figure 12-15. Condition True or False Options

6. If this is not the first (or only) rule condition, select the operator linking it to the previous condition: **and**, **and not**, **or**, **or not**

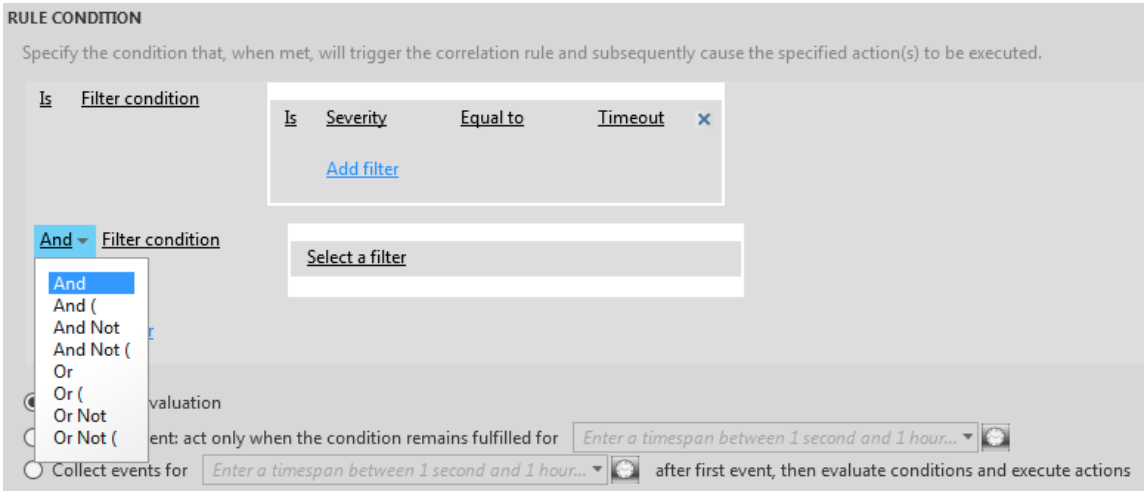


Figure 12-16. Filter Condition Operators

7. To add another rule condition, click **Add Filter** and go back to step 1
8. To delete one of the rule conditions, click the ***X*** to the right of that condition
9. To set the activation mechanism, select one of these options:

   Immediate evaluation

   If you select this option, the rule action(s) occur as soon as there is a match with the rule conditions.

   Use this option if you want to use a sliding window, see Step 10.

   Persistent event: act only when the condition remains fulfilled for…

   If you select this option and specify a time span, the rule action(s) occur when there is a match with the rule conditions that lasts for duration of the specified time span.

Collect events for … after first event, then evaluate condition(s) and execute actions

If you select this option, specify a time span. As soon as an alarm matches the alarm filter(s), the correlation rule starts collecting all alarm events matching the same alarm filter(s). After the specified time span, the rule conditions are checked for the collected alarm events. If there is a match, the action(s) occur.

You can use this option to activate the rule action(s) only if the average value of the alarms matching the filter during the time span is higher than a value defined in the rule.

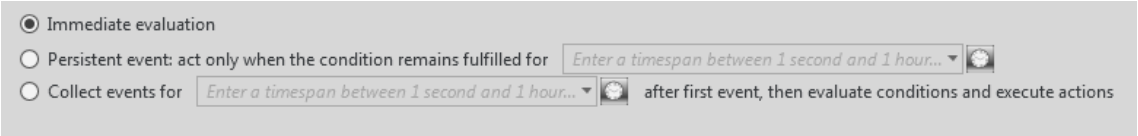


Figure 12-17. Activation Mechanism Options

10. In the **Sliding window** section, you can set an additional activation mechanism in a sliding window.
    - To activate the Correlation rule if a situation occurs a specified number of times in a given time span, select **Require situation to occur … times in … before acting**
    - Specify the number of times and the time span.
    - When you select this option, and there is a match with the rules conditions, the occurrence is registered. As soon as there are enough occurrences in the interval, the rule is activated.
    - To create a rule that is activated if a certain number of alarms occur within a sliding window, you must also select the option **Trigger on single events. Don't maintain active tree status** in the **Alarm filter** section. Only the base alarms are counted; therefore, if you do not select this option, and there are changes in an alarm tree, these are not counted as separate events.
    - To activate the Correlation rule only if this situation persists during a given time span, also select the option **Require sliding window violation to persist for … before acting**, and specify the time span.

Figure 12-18. Sliding Window Example

12.3.14 Add Rule Actions in Correlation Rules

In the Correlation app, select a rule in the tree view pane on the left, then add rule actions to it in the details pane on the right.

In the **Actions** section of the details pane, specify the actions that must occur when the Correlation rule is activated.

There are three types of actions:

- A new, correlated alarm.
- Running an Automation script.
- A parameter set.

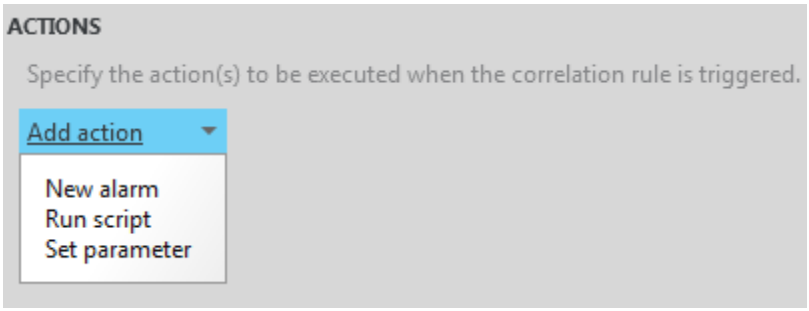


Figure 12-19. Add Action Options

You can combine these actions so that they are activated in a specific order. To change the order of the actions:

1. Hold the mouse cursor over the actions.
2. Use the up or down triangles to move them up or down in the list.

To delete an action:

1. Hold the mouse cursor over the action.
2. Click the ***X.***

12.3.15 Trigger a Correlated Alarm

To trigger a correlated alarm:

1. Click Add Action.
2. Select New Alar.
3. Click the first underlined field.
    - Select an element from the list.
4. Click the second underlined field.
    - Select a parameter from the list.
5. If you select a dynamic table parameter, click **<empty>** to right of the parameter.

6. Select the row index.

You can leave the element and parameter empty in the New Alarm action. This generates a correlated alarm on the same element and parameter as the base alarm.

7. Click the underlined field to the right of ***with alarm value***
8. Specify a parameter value

Instead of a value, you can enter a placeholder. For more information, see Correlation rule syntax.

9. Click the underlined field to the right of ***and severity***
10. Select an alarm severity
11. If necessary, select one or more of these options:

Auto clear

Select this option to cause the Correlated Alarm to clear automatically as soon as the conditions specified in the Correlation rule are no longer met.

Include name in alarm value

Select this option to cause the name of the Correlation rule to show in the alarm value.

Update base alarms

Select this option to update the list of base alarms automatically after a correlated alarm is generated.

Evaluate value

Select this option if the alarm value of the correlated alarm to be generated contains functions that must be evaluated. These functions are enclosed in square brackets; Avg value is shown as [AVG(FIELD(VALUE))]. For more information on Correlation functions, see **Correlation rule syntax**.

Root time of base alarm

Select this option to cause the root time of the Correlation alarm to be the same as the base alarm that activated its creation.

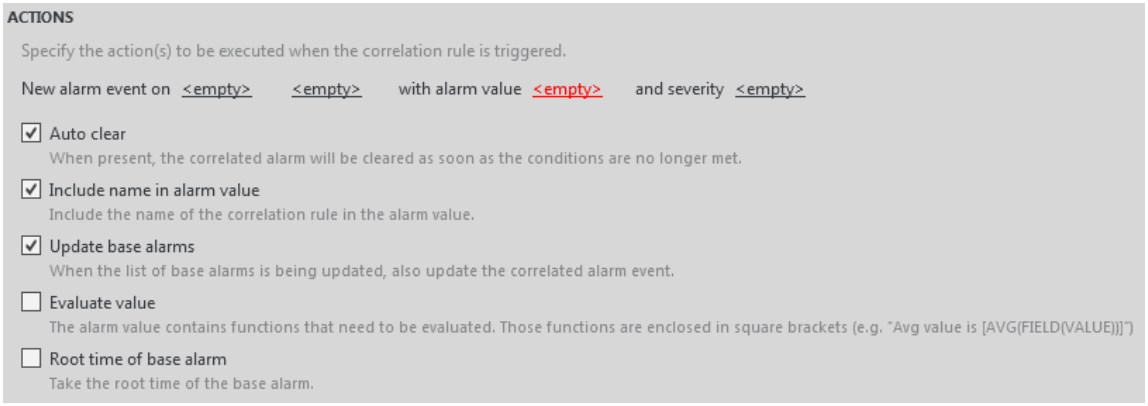


Figure 12-20. Actions Options Example 1

12.3.16 Run an Automation Script from a Correlation Rule

1. Click Add Action
2. Select Run script
3. Click the first underlined field
   - Select an element from the list
4. Click the second underlined field
   - Select a parameter from the list
5. Click the underlined field to the right of **with value**
6. Enter the value for the parameter
7. If necessary, select one or more of these options:

   Execute on clear

   This option sets the parameter when the conditions activating the rule are no longer true.

   Execute on base alarm updates

   This option sets the parameter when the base alarms change.

   Evaluate value

   This option allows placeholders in the parameter value. For more information, see Correlation rule syntax.

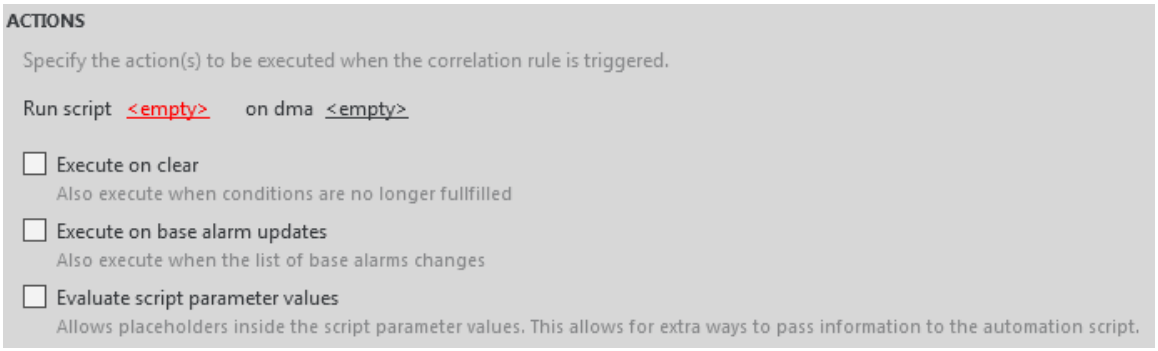


Figure 12-21. Actions Options Example 2

12.3.17 Correlation Rule Syntax

When you specify a condition in the NetVue Cube Correlation module, you can use a special syntax to construct a script condition.

12.3.18 Condition Format

<value> <operator> <value>

Examples:

count(*) > 5
field(pid)==123
field(value) == “Connected”
parameter(7,56,110,”SLDataMiner”) > 55.2
round(avg(field(value)),3) == “12.555”
field(value) == “Status: \”OK\””

Available operators

Numeric comparison (values parsed into double, using invariant culture)

<
>
<=
>=

String comparison (case insensitive, invariant culture)

!=
==

Values

String values can be enclosed in double quotes:

“Connected”

Double quotes in a quoted string can be encoded by adding a backslash in front:

“string with a \” in it”

When not enclosed in double quotes, values can contain the following characters:

a-z
A-Z
0-9
_ (underscore)
– (dash)
. (dot)
* (asterisk)

Remarks

Any white space characters in between values, function names, function arguments, etc., are ignored. White space characters include space, tab, form feed, etc.

When script conditions use functions, fields or properties outside of the min/max/avg aggregated functions context, values are retrieved from one of the alarms in the bucket only. Typically, this is the triggering alarm or the most recent one in the rule bucket.

Within a single script condition, it is not possible to combine multiple conditions using **and** or **or**.

12.3.19 Correlation Rule Functions

Functions you can use in a script condition are listed in this section. Examples follow each function.

You can use these functions as placeholders, such as in parameters in Correlation rules. In this case, enclose them in brackets: [field(elementname)].

12.3.19.1 Field

Retrieves one of these fields from a base alarm:

Field	Description
rawvalue	Raw alarm value
value	
dmaid	DataMiner ID
eid	Element ID
pid	Parameter ID
idx	Display key of table row
pk	Primary key of table row
severity	(as ID)
severityrange	(as ID)
status	(as ID)
type	(as ID)
source	(as ID)
elementrca	
parameterrca	
servicerca	
rootkey	Root alarm ID
id	Alarm ID
userstatus	(as ID)
owner	
elementname	
parametername	
previous	ID of previous alarm in tree
category	
keypoint	
componentinfo	
hostingdmai	
viewname	Name of the view containing the element that generated the alarm If the element can be found in more than one view, then a random name is used.

12.3.19.2 Property

Retrieves a property of a base alarm.

When used outside of the min/max/avg aggregated functions context, the value is retrieved from one of the alarms in the bucket only. Typically, this is the triggering alarm or the most recent one in the rule bucket.

Syntax:

property([dataype].[property name])

[datatype] can have one of the following values:

view
element
service
alarm

Example:

property(view.location)

12.3.19.3 Parameter

Retrieves a parameter value.

Examples:

Parameter(DMAID, elementID, parameterID)
parameter(7,59,250)
Parameter(DMAID, elementID, parameterID, rowindex)
parameter(7,56,110,SLDataMiner)

12.3.19.4 Base Alarm Count

Count: Returns the number of base alarms.

Example:

count(*)

12.3.19.5 Set the Minimum Value

Min: Sets the minimum value among all alarm events in the rule bucket.

Example:

min(field(value))

12.3.19.6 Set the Maximum Value

Max: Sets the maximum value among all alarm events in the rule bucket.

Example:

max(field(value))

12.3.19.7 Set the Average Value

Avg; Sets the average value among all alarm events in the rule bucket

Example:

avg(field(value))

12.3.19.8 Round the Value

Round: Rounds the value to a specific amount of digits after the comma

Example:

round(avg(field(value)),3)

12.3.20 Script Condition Examples

avg(field(value)),3) < 1.3

means: If the calculated average value is less than 1.3, …

count(*) > 5

means: If there are more than 5 base alarms, …

max(property(Alarm.ImpactedClients)) >= 3

means: If, after comparing the ImpactedClients Properties of all base alarms, the highest value found is at least equal to 3, …

parameter(7,59,350) > 10

means: If parameter 350 of element 59 of DMA 7 contains a value higher than 10, …

parameter(field(dmaid), field(eid), 350) > 10

means: If there is a base alarm of which parameter 350 of the associated element contains a value higher than 10,

12.3.21 Use Correlation Analyzers

NetVue can analyze the alarms occurring over time, and then suggest a correlation rule based on this analysis.

The analyzers used for this purpose are found in a second tab in the Correlation app: the **Analyzers** tab.

12.3.22 Create an Analyzer

Use one of these two methods to create a Correlation analyzer:

In the **Analyzers** tab of the Correlation app, click the **Add analyzer** button;

- or -

In the Surveyor, right-click an element or view for which you must create an analyzer, and select **Actions > Analyze**.

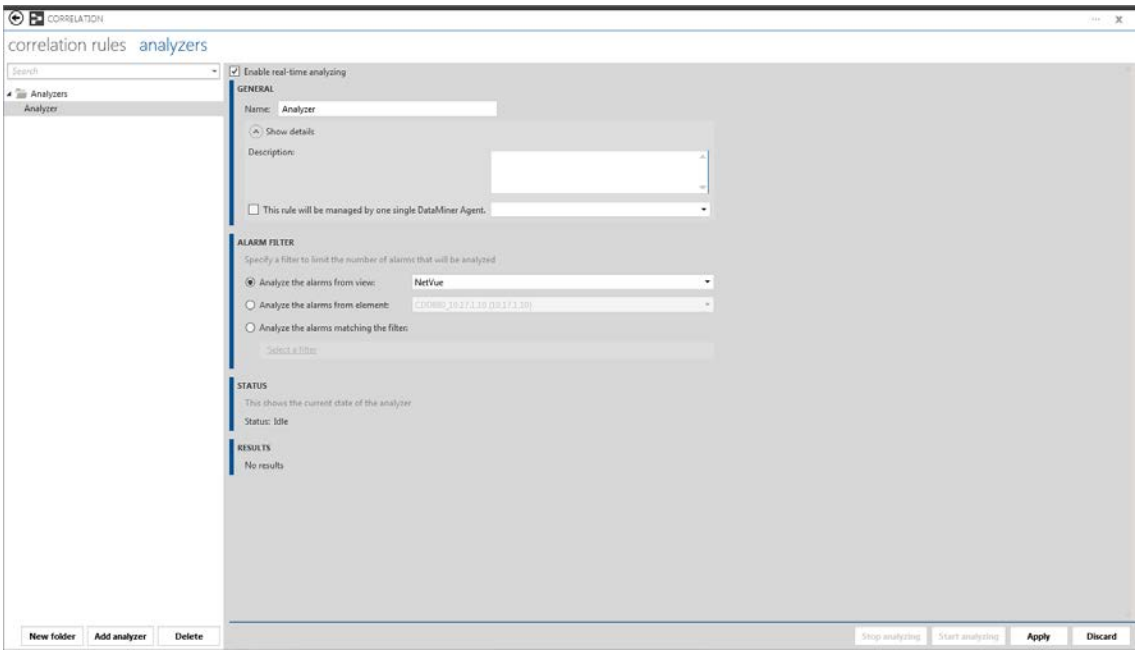


Figure 12-22. Analyzers Example

12.3.23 Configure an Analyzer

To configure an analyzer, select it in the tree view. Change the configuration in the details pane:

1. Enter a name for the analyzer in the **Name** field

   A new analyzer is named ***Analyzer*** by default. You cannot have two analyzers with the same name in the same folder. However, using the same name in different folders is acceptable.

2. Optionally, expand **Show details** and add a description in the **Description** field
3. If the analyzer must always be managed by NetVue:
   - Expand ***Show details***
   - Select ***This rule will be managed by one single DataMiner Agent***
   - Select the NetVue server in the drop-down list

Figure 12-23. General Analyzer Example

4. In the **Alarm filter** section, select what must be analyzed.
   a. To analyze a view, select **Analyze the alarms from view** and select the view in the drop-down list.
   b. To analyze an element, select **Analyze the alarms from element** and select the element in the drop-down list.
   c. To analyze based on an alarm filter, select **Analyze the alarms matching the filter** and create a filter:
      i. Click Select a filter.
      ii. Select a parameter to filter by.
      iii. If this is the first (or only) filter condition, select Is or Is Not to set whether the condition has to be true or false, otherwise;
      iv. Select the operator linking it to the previous filter condition (***and***, ***and not***, ***or***, ***or not***).
      v. Specify whether the parameter must match, or not match, a regular expression or wildcard expression.
      vi. Specify the applicable expression.

5. To use the analyzer to analyze real-time alarms, select **Enable real-time analyzing** at the top of the details page.
6. To delete one of the filter conditions, click the ***X*** to the right of the filter.

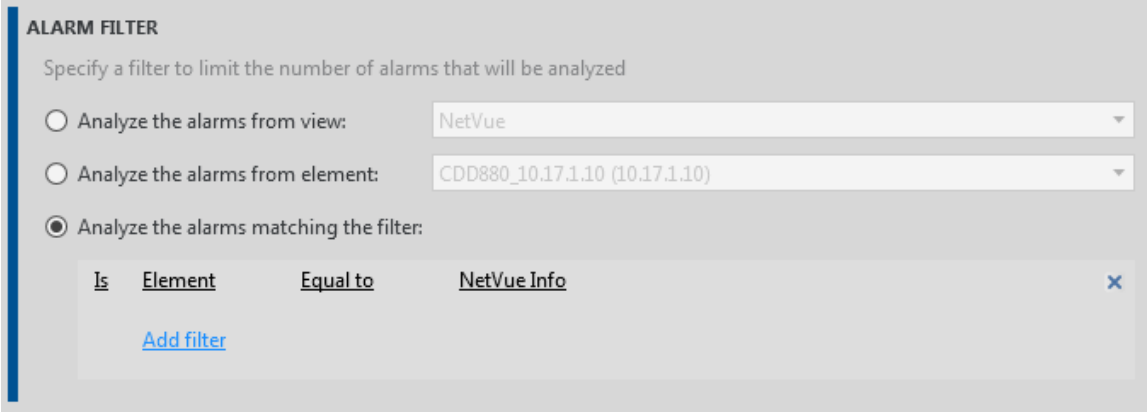


Figure 12-24. Alarm Filter Example

7. To add another condition to the filter, click ***Add a filter*** and go back to Step 4.
8. If this option is not selected, you must specify a time range for history alarms when the analyzer is used.
9. Click the **Apply** button at the bottom of the details pane to save the configuration changes.

12.3.24 Run an Analyzer

To run a Correlation analyzer:

1. Select the analyzer in the tree view of the **analyzers** pane.
2. Click the **Start analyzing** button at the bottom of the details pane.
3. If the option **Enable real-time analyzing** is not selected, set a time range for the history alarms you want to analyze, and click **Apply.**
4. While the analyzer is working, its status changes from **Idle** to **Collecting.**
    - To stop real-time analyzing, click **Stop analyzing**. Analysis of history alarms stops automatically as soon as the analyzer is ready.
5. The analyzer status returns to **Idle**, and a Correlation rule is proposed under **Results**.
6. To see the proposed Correlation rule:
    a. Right-click the result.
    b. Select Add to correlation.

The new Correlation rule is not enabled or saved automatically.

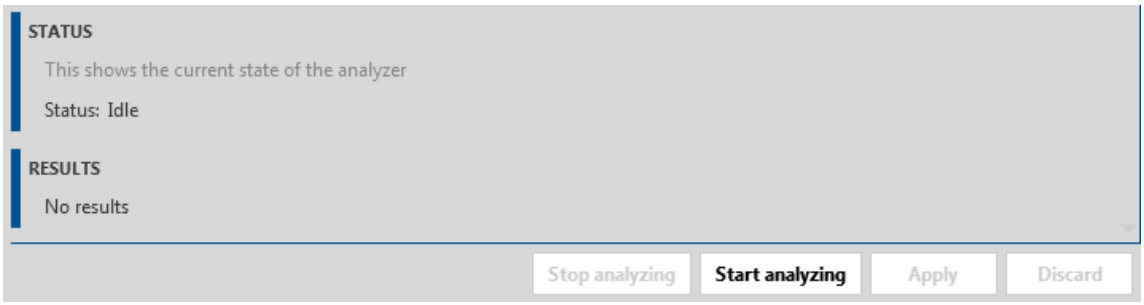


Figure 12-25. Analyzer Status Example

12.3.25 Manage Analyzers

Like the main Correlation app, the **Analyzers** tab has a tree structure on the left, and a detailed view on the right. The management of the available analyzers is very similar to the management of Correlation rules in the **Correlation** tab.

- To add or delete folders and analyzers, use the buttons at the bottom of the tree view pane, or use the right-click menu.
- To duplicate an analyzer, right-click it and select **Duplicate**.

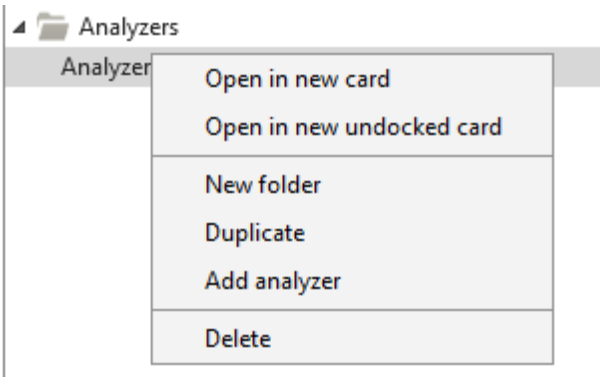


Figure 12-26. Duplicate Analyzer Example

- Drag and drop analyzers to move them to and from folders in the tree view.
- In the tree view, right-click a folder and select **Collapse all,** or **Expand all,** to collapse or expand all folders in the tree view.

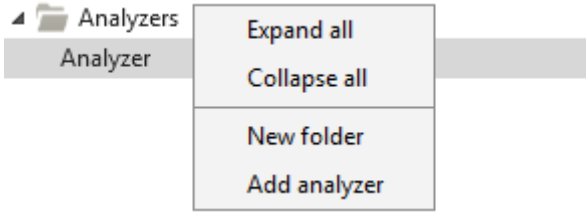


Figure 12-27. Expand or Collapse All Analyzer Tree View

Chapter 13. AUTOMATION

13.1 NetVue Automation

NetVue Automation allows you to create scripts that can execute backup routines, system configuration, channel selection, report generation, notification via email or SMS, etc., all automatically.

Using an intuitive, feature-rich graphical interface, you can build intricate, nested scripts. Set schedules for these scripts for one time or repeated execution. Additionally, link the scripts to objects shown in Microsoft Visio drawings, so that operators can run them with the click of a button.

13.2 Automation Scripts

To create, view, edit or organize Automation scripts in the NetVue Cube, open the Automation app by going to **Start > Apps > Automation**.

13.2.1 Manage Automation Scripts

When you open the Automation app, it shows a card that has two panes:

- The left pane shows all scripts in a tree view. Use the search box at the top of the pane to find a particular script quickly.
- The right pane shows script details. Use it to see and edit scripts.
- Manage automation scripts in the left pane.

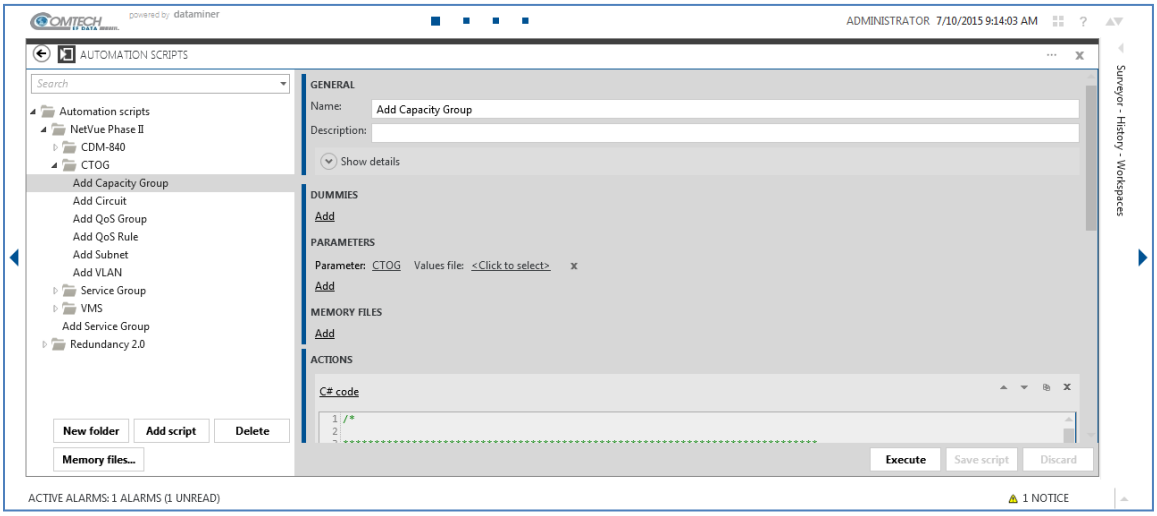


Figure 13-1. Automation Scripts Application Example

13.2.1.1 Collapse and Expand Folders

You can collapse or expand folders in the tree view. If you select **Collapse all**, the root folder does not collapse.

1. Click the triangle in front of the folder.
2. Right-click the tree view and select **Collapse all** or **Expand all.**

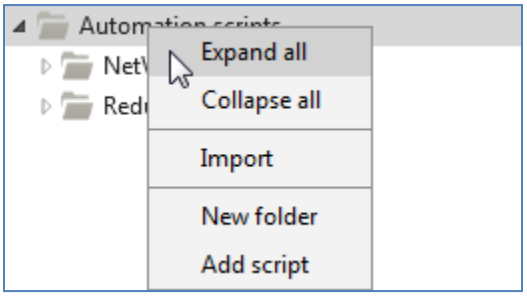


Figure 13-2. Collapse/Expand Folders Example

13.2.1.2 Add a New Automation Script

To add a new script:

1. Select the folder where you want to add the script.
2. Click the **Add script** button at the bottom of the pane;

   - or -

   Right-click the folder where you want to add a new script.
3. Select **Add script**.

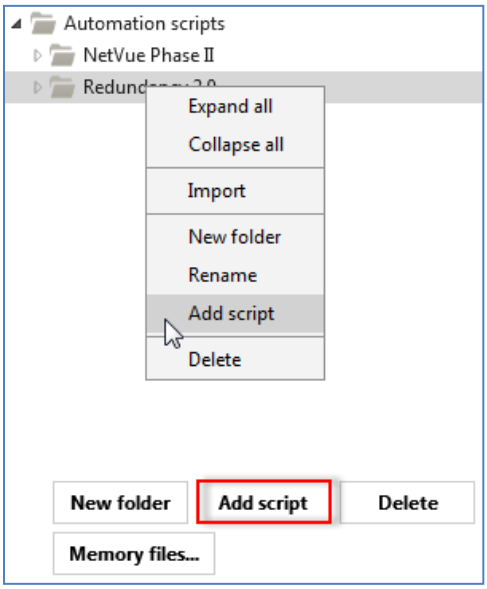


Figure 13-3. Add Script Example

Additionally, you can add a new script by duplicating an existing script, and then changing this duplicate as necessary. You cannot create two Automation scripts with the same name.

1. To duplicate a script, right-click the script.
2. Select **Duplicate**.

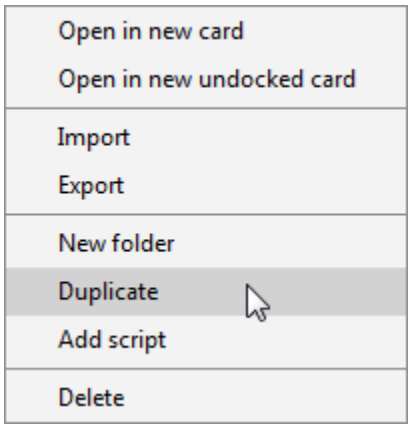


Figure 13-4. Duplicate Example

13.2.1.3 Add a New Folder

To be saved, a new folder must have at least one script. Otherwise, empty folders are deleted automatically when you close the Automation app.

To add a new folder:

1. Click the **New Folder** button at the bottom of the pane;

   - or -

   Right-click the folder where you want a new folder.

2. Select **New folder.**

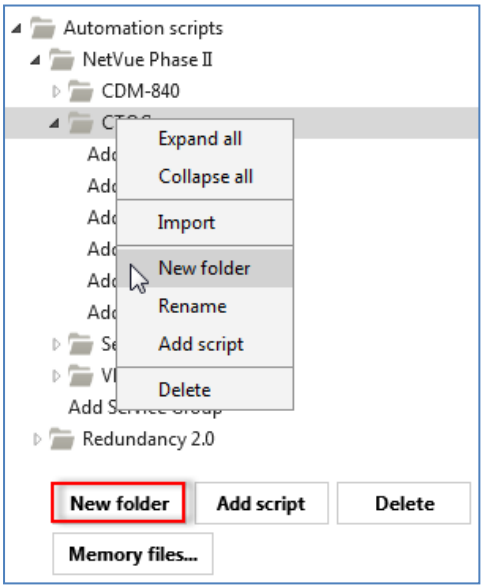


Figure 13-5. New Folder Example

13.2.1.4 Move a Script or Folder

To move a script or folder in the Automation tree view, drag the script or folder and drop it in the new location in the tree view.

13.2.1.5 Delete a Script or Folder

When you delete a folder, all scripts in that folder are deleted also.

To delete a script or folder:

1. Select the script or folder.
2. Select the **Delete** button at the bottom of the pane;

   - or -

   Right-click the script or folder.
3. Select **Delete** in the right-click menu.

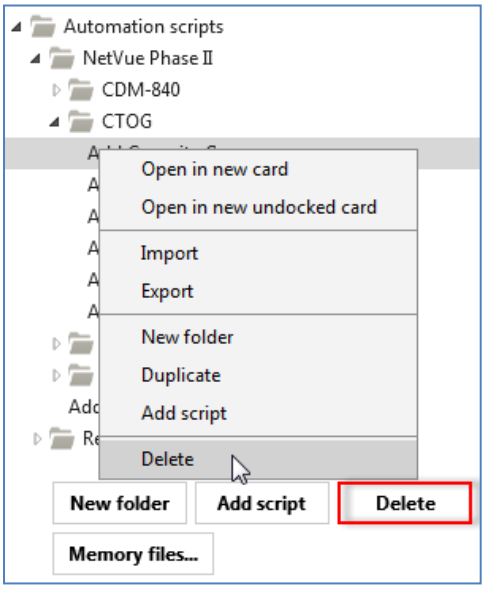


Figure 13-6. Delete Example

13.2.1.6 Rename a Folder

To change the name of a folder:

1. Right-click the folder.
2. Select **Rename;**

   - or -

   Select the folder.
3. Press F2.

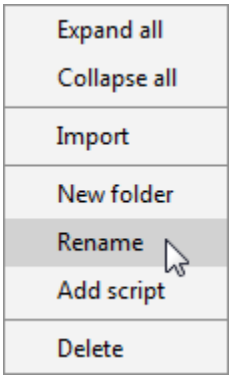


Figure 13-7. Rename Folder Example

13.2.1.7 Import or Export Scripts

To import is to upload a locally stored XML file containing a script and add it to a folder.

1. Right-click the folder.
2. Select **Import.**

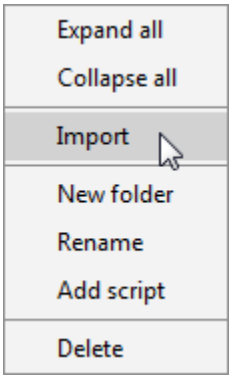


Figure 13-8. Import Script Example

To export is to download a script as an XML file.

1. Right-click the script.
2. Select **Export.**

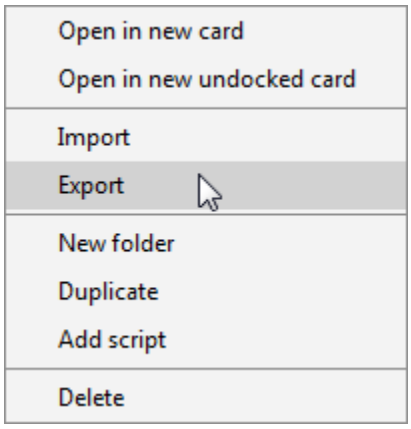


Figure 13-9. Export Script Example

13.2.2 Design Automation Scripts

In the Automation app, select a script in the left tree view pane. Configure the script in the details pane on the right.

To design a script, specify the general configuration, add script actions and specify variables when necessary.

Click **Save script** to save changes any time while working on the script. You cannot make more changes until the script has finished saving. A dialog box opens and prompts you to save changes if you try to go to a different script, or if you try to run a script that has unsaved changes.

If a script has errors, a red warning message shows at the bottom of the editor pane, and the **Save script** button is disabled temporarily.

13.2.2.1 General Script Configuration

In the **General** section of the details pane, you can configure general information and options for a script. To see the options, click the down arrow next to **Show details**.

To configure a script:

1. In the text box next to **Name**, enter a new name for the script.
2. In the text box next to **Description**, optionally enter extra information about the script.
3. Expand the details section and select or deselect these options as required:
    a. Select **Support back/forward buttons in interactive mode** to add back and forward buttons in a dialog box that requests a user response.
    b. Select **Do not fail when elements are not active or in timeout** to keep a script from failing when it finds an element that is not active or are in timeout.
    c. Select **Write comments to log file** to write any comments in the script to the Automation log file.
    d. Select **C#: Return NULL instead of an exception upon a GetParameter of a non-initialized parameter** to make sure no exception occurs when an undefined or empty parameter is found in C# code. Null is returned instead.

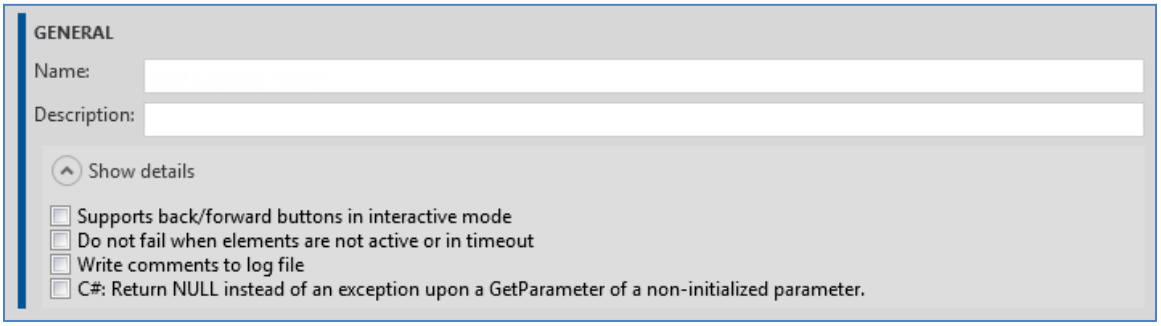


Figure 13-10. General Configuration Example

13.2.2.2 Variables

For most script actions, variables are required. There are three kinds of variables:

- **Dummies**: required for every different element in the script; when the script is run, an actual element is linked to each dummy.
- **Parameters:** typically used to get input from the outside world, e.g., from an operator.
- **Memory files:** containers of values, typically provided by the script itself.

When you add a script action that contains a variable, a line is added to the applicable section automatically.

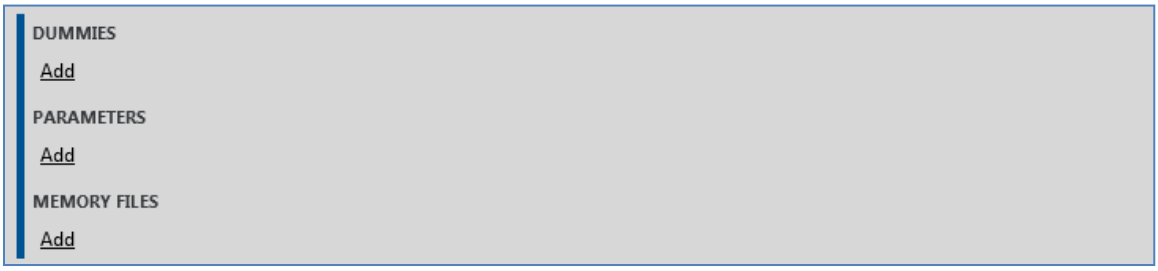


Figure 13-11. Variables Example

13.2.2.2.1 Create a Dummy

To create a new line in the **dummy** section:

1. Click **Add** in the **dummy** section;

   - or -

   In a script action that requires a dummy, click the field where the dummy must be filled in.

2. Select **Create new dummy.**

To specify the dummy properties:

1. To change the name of the dummy:
   a. Click the leftmost underlined field.
   b. Enter a new name.
2. To change the protocol for a dummy:
   a. Click the underlined field next to **Protocol**.
   b. Select a new protocol and protocol version.
3. Optionally, to link a default element to a dummy:
   a. Select an element in the underlined field next to **Configuration Element** for this dummy.

      This is useful when a table parameter column is selected, because you can then select an index from the available indices of the table of that default element.

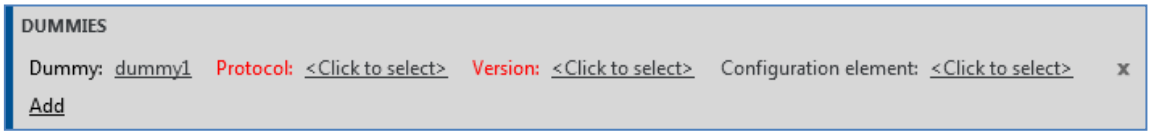


Figure 13-12. Dummies Example

13.2.2.2.2 Create a Parameter

To create a new line in the **parameter** section:

Click **Add** in the **parameter** section;

- or -

In a script action that requires a parameter, click the field where the parameter must be filled in, and select **Create script input.**

To specify the parameter properties:

1. To change the name of the parameter:
    a. Click the leftmost underlined field.
    b. Enter a new name.
2. Optionally, link a memory file to the parameter to suggest possible values to the user who runs the script:
    a. Click the underlined **<Click to select>** next to **Values file.**
    b. Select the file.

Figure 13-13. Parameters Example

13.2.2.2.3 Create a Memory File

You can create a memory file using any of these methods:

Use the script editor:

Click **Add** in the **parameter** section;

- or -

In a script action that requires a memory file, click the field where the memory file must be filled in and select **Create new memory file.**

Click the **Memory files** button in the bottom left corner of the Automation card.

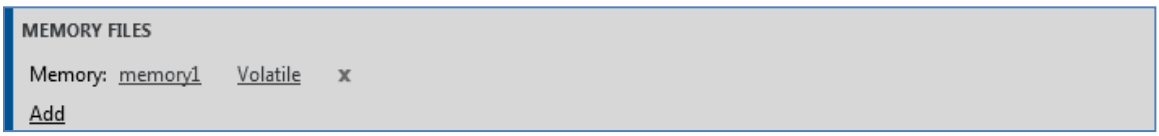


Figure 13-14. Memory Files Example

13.2.2.2.4 Configure a Memory File

While in the script editor, you can configure a memory file.

1. To change the name of the memory file:
    a. Click the leftmost underlined field.
    b. Enter a new name.
2. To set the memory file as either volatile or persistent:
    a. Click the second underlined field.
    b. Select either **Volatile** or **Persistent.**

13.2.2.3 Script Actions

A script is a series of script actions (lines). These show in the **Script** section of the right pane. You can add or modify script actions any time during script configuration.

To create a script action under any previously added script actions:

1. In the **Actions** section, click **Add.**
2. Select the script action.

To create a script action between existing script actions:

1. Right-click the location where you want to add the script.
2. Click **Insert.**
3. Select the action.

Figure 13-15. Add Actions Example

For all script actions, these options are available using the buttons to the right of the action:

To move an action within the list:

Click the up or down triangle to move the script action one position up or down in the list;

- or -

Drag a script action to a different position in the script.

To add a duplicate script action, click the duplicate icon. The duplicated script action is added immediately below the original script action.

To delete an action, click the **x**.

Additional configuration options depend on the type of script actions you added.

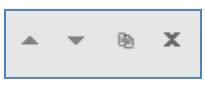


Figure 13-16. Action Options Example

13.2.3 Automation Script Actions

With the **Add action** drop-down list, you can choose different actions to add to a script. To configure these actions, click the underlined sections of text.

13.2.3.1 Assign Dummy

To assign an Automation script's dummy to a specific element by using a variable or a value:

1. Click the left-most underlined field to select or create a dummy element.
2. Select how the new element is determined:
    a. For a pre-determined element, select **value** to select a specific element, and enter the element name or ID.
    b. For an element determined by a script variable, select **variable** and select a variable.

Figure 13-17. Assign Dummy Example

13.2.3.2 Assign Template

To assign an alarm or trend template to a dummy:

1. To assign a trend template, click the default **Alarm Template** option, and select **Trend Template**.
2. Next to **for**, click the underlined field to either add an existing dummy element, or create a new dummy element.
3. To select a variable, click the default **value** option, and select **variable**.
4. Click the final underlined field and select a script variable; or, if you chose **value**, an existing template.

Figure 13-18. Assign Template Example

13.2.3.3 C# Code

To include a C# code block in an automation script:

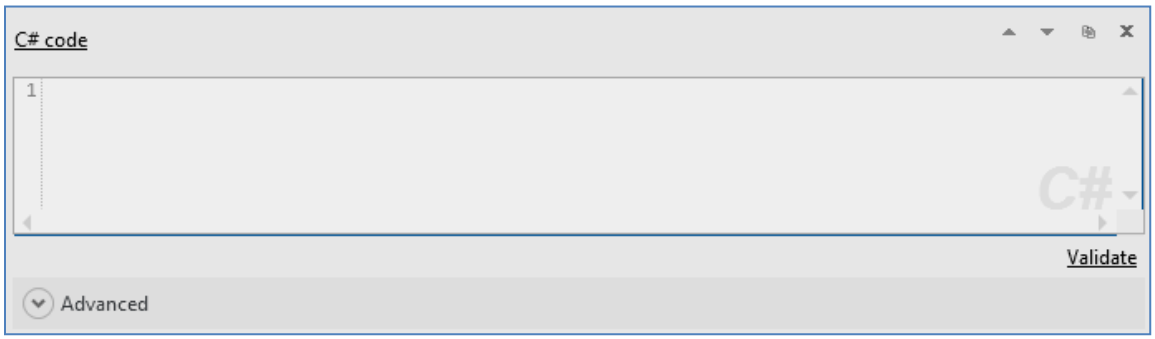


Figure 13-19. C# Code Example

13.2.3.4 Clear Memory

To clear the contents of an Automation script's memory file:

Click the underlined field next to **file** to select the memory file to be cleared.

Figure 13-20. Clear Memory Example

13.2.3.5 Comment

To add extra comments to the script:

Click **Text of the comment** and fill in the comment.

Note these special comments:

- If you add a comment line containing **debug=true**, the debug mode is enabled. During script execution, all comments appear as information events. They are added to the SLAutomation.txt log file. A comment line containing **debug=false** disabled the debug mode.
- If you add a comment line containing **skipElementChecks=true**, the script will not verify the current state of the element. This way, scripts can be executed even if included elements are in a timeout state or not active.
- If you add a comment line containing **skipInformationEvents=true**, you will prevent information events from being generated by the SET statements in the script.

Figure 13-21. Comment Example

13.2.3.6 Email

To send a notification via email:

1. Enter the recipients in the **To, CC** and **BCC** fields.
2. Enter the message **Subject.**
3. Enter the email message in the **Message** field.
4. To send a plain text email, select **Send as plain text.**
5. To include a report in the email, select **Include Report.**
6. Select an existing report template and add any required elements, parameters, etc.

Figure 13-22. Email Example

13.2.3.7 Exit

To terminate an Automation script immediately:

1. Next to **Exit script with**, select **Success** or **Failure** in the drop-down list:
   a. Success: after termination by this action, the script execution is considered successful.
   b. Failure: after termination by this action, the script execution is considered a failure. In this case, the Alarm Console generates a Fail message.
2. Click **Reason** and enter a message that shows in the Automation logging and, in case of failure, in the Alarm Console.

Figure 13-23. Exit Example

13.2.3.8 Find Interactive Client

Use this action to ask an interactive user to attach to the script. A message box asks you to select from two options:

- **Attach**: the script starts in a popup window
- **Ignore**: the message box is closed

Either selection generates an information event.

To configure the action:

1. Next to **Show message**, click the underlined field to add the message that shows in the message box.
2. Next to **Timeout**, add the number of seconds that the script waits for the user to respond. When this timeout expires, the script continues and the *Find Interactive Client* method returns False.

Figure 13-24. Find Interactive Client Example

13.2.3.9 Get Parameter or Memory Value

For this script action, choose what is to be retrieved: a parameter or a memory value. Subsequent configuration options depend on this first choice.

13.2.3.9.1 For a Parameter Get

1. In the first underlined field, keep **Parameter** selected.
2. Click the next underlined field to add an existing dummy element, or to create a new dummy element.
3. Select the parameter to be retrieved.
4. For a dynamic table parameter, also specify the index.
5. Specify the destination value.

Figure 13-25. Parameter Get Example

13.2.3.9.2 For a Memory Get

1. In the first underlined field, select **Memory value.**
2. Click the next underlined field.
3. Add an existing memory file, or create a new memory file.
4. Click the last underlined field.
5. Specify an existing script parameter, or create a new one.

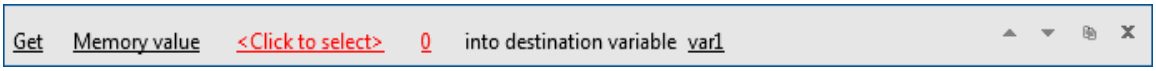


Figure 13-26. Memory Get Example

13.2.3.10 GoTo and Label

These two script actions are linked:

- Use **Label** to add a label text, which adds a label in a script.

Figure 13-27. Label Example

- Use **GoTo** and enter a label text to go to a particular label in the script.

Figure 13-28. GoTo Example

13.2.3.11 If Condition

Add an **If** condition to make specific actions in the script depend on one or more conditions.

When you add an **If** condition, a block is added that consists of three sections:

- **If**: contains one or more conditions, combine with 'and' or 'or'.
- **Then**: contains actions that will be executed only if the If condition is true.
- **Else**: contains actions that will be executed only if the If condition is false.

To add a condition:

1. Click **Add condition.**
2. Select **Parameter** or **Variable.**
3. If a condition exists already:
    a. If both conditions are applicable at the same time, leave the default field **and** as it is.
    b. If either of the conditions are applicable, change the field to **or**.
4. If the condition is based on a variable, specify the variable. The value of the variable can depend on user input, or it can be a value returned elsewhere in the script;

    - or -

    If the condition is based on a parameter, add a dummy element, or choose an existing dummy element.
5. Select the applicable parameter.
6. Specify whether the variable or parameter should be **less than**, **equal to**, or **greater than** a particular value or variable to which it is compared. A combination of these is possible also.
7. Specify whether to compare to a **value** or a **variable.**
8. Enter the comparison value, or select the comparison variable.
9. Optionally, select **Wait for positive result …** and enter a time span. The script waits during this specified time span before it evaluates the **If** condition.

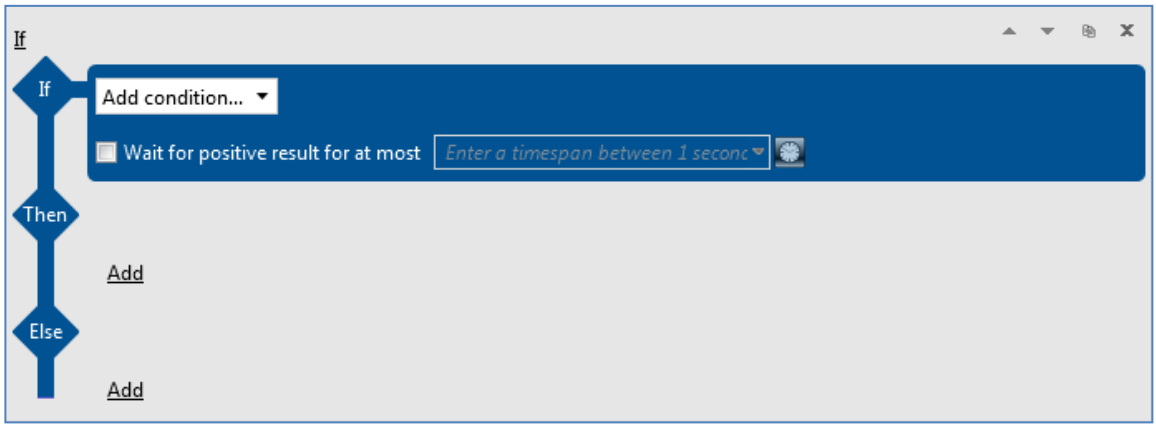


Figure 13-29. If Condition Example

13.2.3.12 Information

Use this action to generate an information event in the Alarm Console:

- In the **Message** field, enter the message that should appear in the Alarm Console.

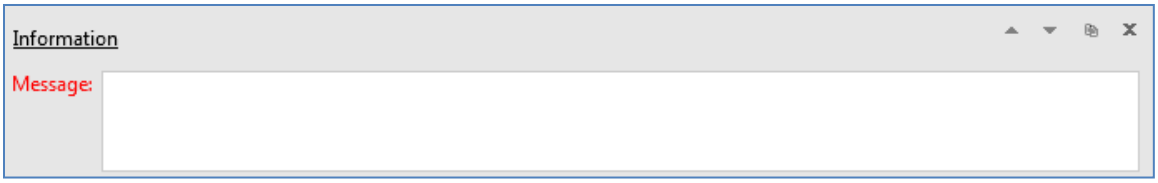


Figure 13-30. Information Example

13.2.3.13 Log

Use this action to have a script create a log message and save it in the SLAutomation.txt log file. It can be a fixed message, or a message that depends on a variable:

1. To have a fixed message logged:
    a. Change the default **variable** field to **message.**
    b. Type a message in the next underlined field.
2. To have a message logged based on a variable:
    a. Make sure **variable** is selected.
    b. Click the next underlined field to select a variable.

Figure 13-31. Log Example

13.2.3.14 Execute Subscript

Use this action to run another Automation script from within the current script.

1. In the underlined field, select one of the available scripts.
2. If necessary, link the dummies in the selected script to the dummies in the current script, or to variables.
3. If necessary, enter a value for each of the parameters used in the selected script, or link them to variables in the current script.
4. If necessary, link the memory files in the selected script to the memory files in the current script.
5. Specify more options for the way the subscript will be run.

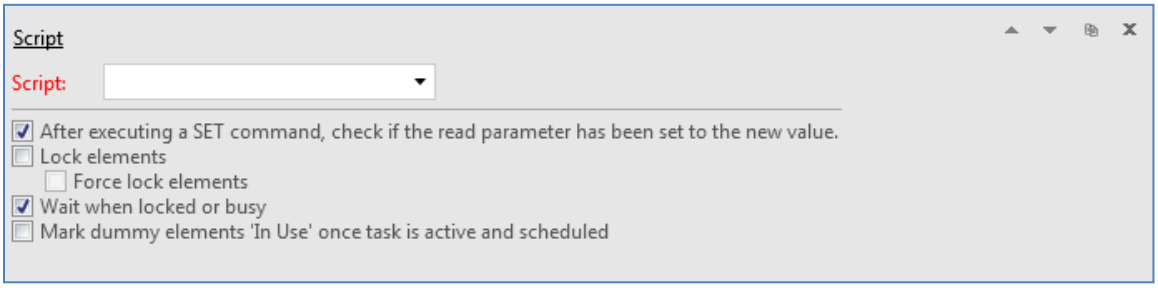


Figure 13-32. Execute Subscript Example

13.2.3.15 Set Parameter, Memory Position, or Variable

For this script action, choose what is to be set: parameter, memory position or variable. Subsequent configuration options depend on this first choice.

13.2.3.15.1 For a Parameter Set

1. In the first underlined field, make sure **parameter** is selected.
2. Next to **parameter**, click the next underlined field to add an existing dummy element or to create a new dummy element.
3. Click the next underlined field to select a parameter.
4. For the next underlined field:
   a. Make sure **value** is selected, and specify the value;

      - or -

   b. Change the **value** field to **variable**, and select the variable.
5. Optionally, if the parameter is a number, click the underlined field next to **Offset** and specify an offset value.

Figure 13-33. Parameter Set Example

13.2.3.15.2 For a Memory Position Set

Change the default **parameter** field to **memory position**:

1. Click the next underlined field and add an existing memory file, or create a new memory file.
2. For the next underlined field:
    a. Make sure **value** is selected, and specify the value.
    - or -
    b. Change the **value** field to **variable**, and select the variable.
3. Optionally, click the underlined field next to **Offset** and specify an offset value.

Figure 13-34. Memory Position Set Example

13.2.3.15.3 For a Variable Set

Change the default parameter field to **variable**:

1. In the next underlined field, specify an existing script parameter, or create a new one.
2. For the next underlined field:
    a. Make sure **value** is selected, and specify the value.
    - or -
    b. Change the **value** field to **variable**, and select the variable.
3. Optionally, click the underlined field next to **Offset** and specify an offset value.

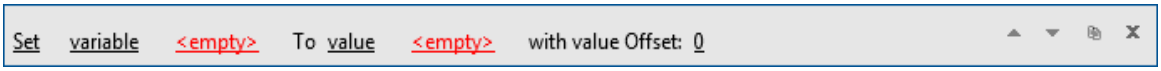


Figure 13-35. Variable Set Example

13.2.3.16 Set Element State

Use this action to set the state of a dummy in an Automation script:

1. Click **Restart**.
2. Select the element state: **start**, **stop**, **restart**, **pause**, **mask** or **unmask**.
3. Click the last underlined field to add an existing dummy element, or to create a new dummy element.

Figure 13-36. Set Element State Example

13.2.3.17 Sleep

Use this action to stop an Automation script for a specified period of time before it is allowed to continue.

To specify how long the script must sleep:

1. Click the underlined field.
2. Enter a number of milliseconds. The default sleep time is 1000 ms.

Figure 13-37. Sleep Example

13.2.3.18 SMS

Use this action to send a text message notification to a user:

1. In the **To** field, enter the recipient's telephone number.
2. In the **Message** field, enter the text message.

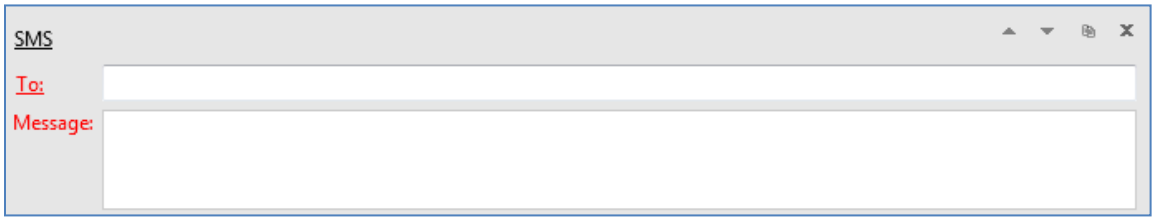


Figure 13-38. SMS Example

13.2.3.19 Upload Report to FTP

Use this action to upload a report to an FTP server:

1. In the **IP address/host** field, enter the host name or IP address of the FTP server.
2. Optionally, enter the port in the **Port** field.
3. In the **Folder path** field, enter the path of the folder where the report must be uploaded.
4. In the **User name** and **Password** fields, enter the credentials to connect to the FTP server.
5. To upload the report in PDF format, instead of the default MHT format, next to **Format,** select **PDF.**
6. Optionally, in the **Report name prefix** field, specify a prefix for the report name. Examples include the name of the NetVue agent, or the location where a problem occurred.
7. Click the field next to **Report** and select a report template.
8. Specify any elements or other input required for the report.

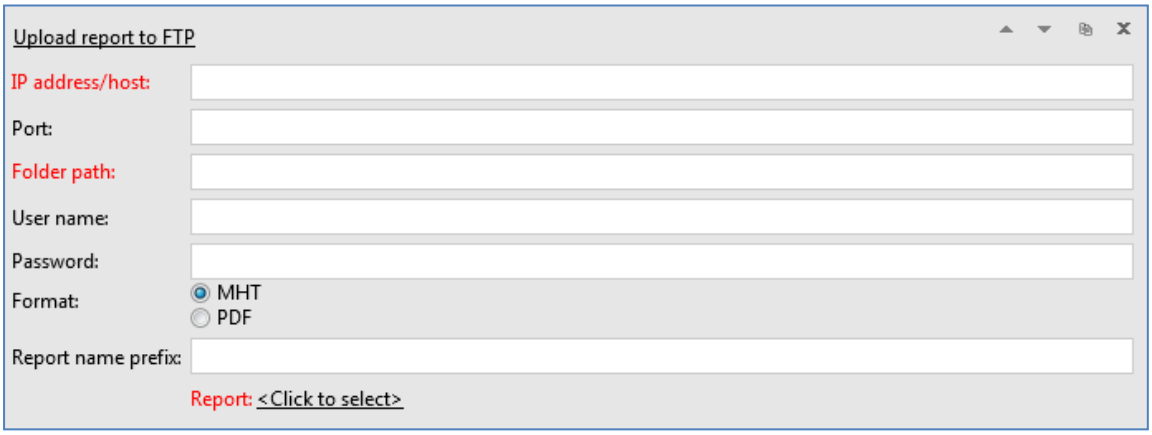


Figure 13-39. Upload Report to FTP Example

13.2.3.20 Upload Report to Shared Folder

Use this action to upload a report to a shared network folder:

1. In the **IP address/host** field, enter the host name or IP address of the server.
2. In the **Folder path** field, enter the path of the folder where the report must be uploaded.
3. In the **Domain/User name** and **Password** fields, enter the credentials to connect to the server.
4. To upload the report in PDF format, instead of the default MHT format, next to **Format**, select **PDF.**
5. Optionally, in the **Report name prefix** field, specify a prefix for the report name. Examples include the name of the DMA agent, or the location where an issue occurred.
6. Click the field next to **Report** and select a report template.
7. Specify any elements or other input required for the report.

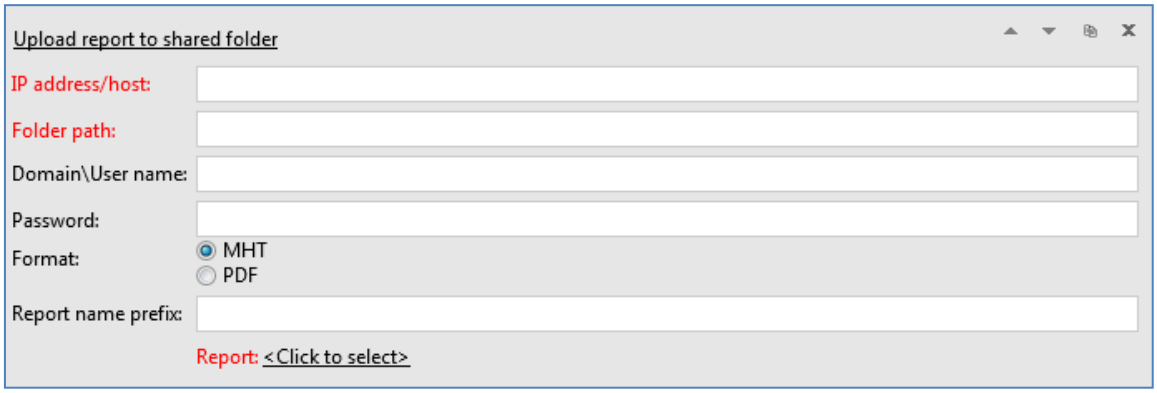


Figure 13-40. Upload Report to Shared Folder Example

13.2.3.21 User Interaction

This action lets you configure a dialog box to request a user response. The dialog box is a pop-up window that has different parts, and a default margin of 5 pixels.

To configure the dialog box, select parts in the **Add part** box on the right, and look at the result in the preview on the left:

To enter a fixed piece of text:

1. Select **Text**.
2. Type or paste the text in the **Text** field.

To show the contents of a variable in the dialog box:

1. Select **Variable Contents**.
2. Click the underlined field to select the variable.

To create a text box where the user enters a value:

1. Select **Text box**.
2. Click the underlined field to select a destination variable.

To add a drop-down list:

1. Select **Drop down**.
2. Click the underlined field to select a destination variable.
3. Add options for the drop-down list with the **Add new option** button.

To add a button:

1. Select **Button**.
2. Enter the text that must show on the button.
3. Select a destination variable for the button.

To change the order of the parts, use the up and down buttons at the right of the parts.

To delete a part, click the **X** next to the applicable part.

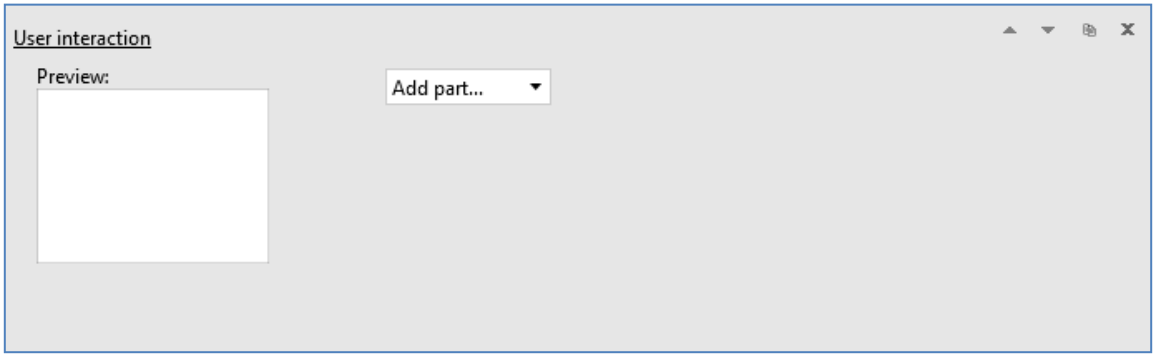


Figure 13-41. User Interaction Example

13.3 Run Automation Scripts

There are several ways to run a script:

- Manually: a one-time run from the NetVue Cube, done from a visual overview, or from the Automation app or page
- NetVue Scheduler: run scripts automatically at specified times.
- NetVue Correlation: scripts run scripts automatically whenever user-defined events occur.

13.3.1 Run a Script Manually

To run an Automation script manually:

1. Go to **Start > Apps > Automation.**
2. In the list on the left side of the **Automation** Card, select the script to run.
3. Click the **Execute** button at the bottom of the right pane.
4. Specify the required dummies, parameters and memory files.
5. Select or deselect the available options, if necessary.
6. Click **Execute now** to run the script.

Figure 13-42. Execute Script Example

13.3.2 Script Execution Options

- **Synchronous run behavior** (On by default) – by default, an Automation script runs synchronously. You must wait for the script to finish before you can continue. If you want a script to be run asynchronously, clear this option.
- **Perform a check on SET statements in the Script** (On by default) – by default, every time a script does a parameter update, it waits for a return value that indicates whether or not the update was successful. If you do not want a script to wait for return values after parameter updates, clear this option.
- **Lock Elements** (Off by default) – by default, an Automation script will never lock elements. If you want a script to do so, select this option.
- **Force Lock Elements** (Off by default) – by default, an Automation script will never lock elements. If you want a script to do so, even when elements are locked by another process, select this option.
- **Wait when Locked or Busy** (On by default) – by default, when an Automation script must access an element that is locked by another process, it waits until that element is unlocked. If you do not want a script to wait when it encounters a locked element, clear this option.

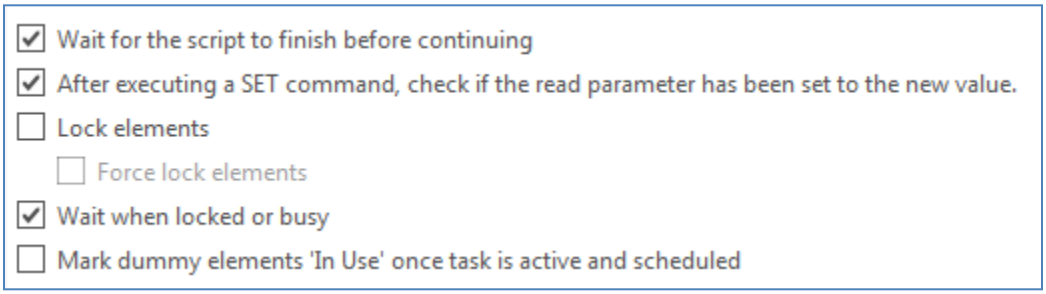


Figure 13-43. Script Execution Options Example

Chapter 14. NetVue Cube Scheduler

14.1 NetVue Cube Scheduler App

To open the Scheduler app in NetVue Cube, go to **Start > Apps > Scheduler**.

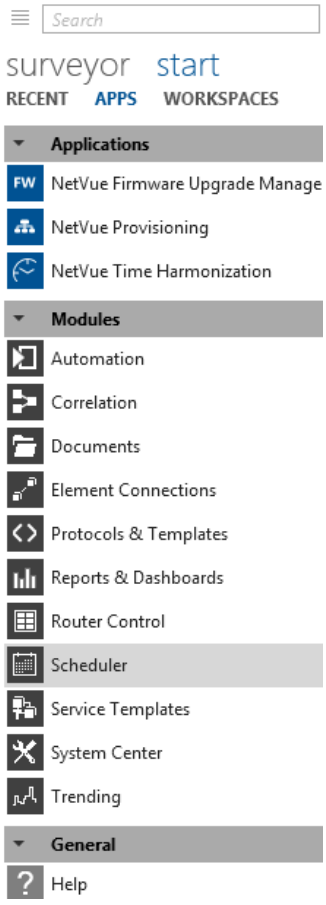


Figure 14-1. Apps Menu Example

Using the Scheduler app in NetVue Cube, you can schedule events two ways:

1. Drag events, based on Scheduler templates, onto a timeline in the **timeline > EVENTS** tab.
2. Add a task to the list of scheduled tasks, in the **list** tab.

14.1.1 View Scheduled Tasks in Cube

In the **timeline** tab, two different subtabs give a different view on the scheduled tasks:

Under **TASKS** you can see all scheduled tasks, including events based on Scheduler templates. For the latter, two tasks show, a **START** and a **STOP** task. The tasks show as dots on the timeline.

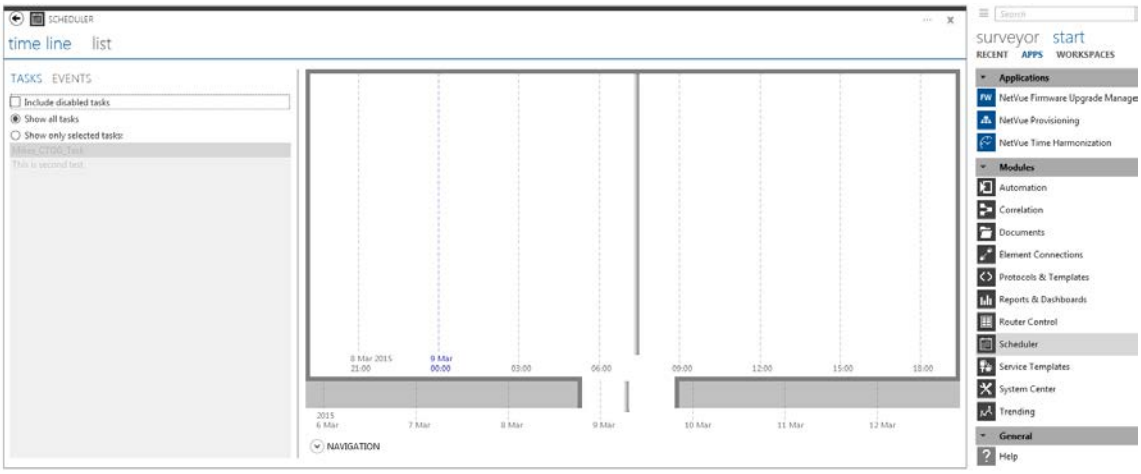


Figure 14-2. Scheduler Time Line, Tasks Example

Under **EVENTS** you can see only events based on Scheduler templates. These show as colored rectangles. Completed tasks show as gray rectangles. Tasks in progress show as green rectangles. Future tasks show as blue rectangles.

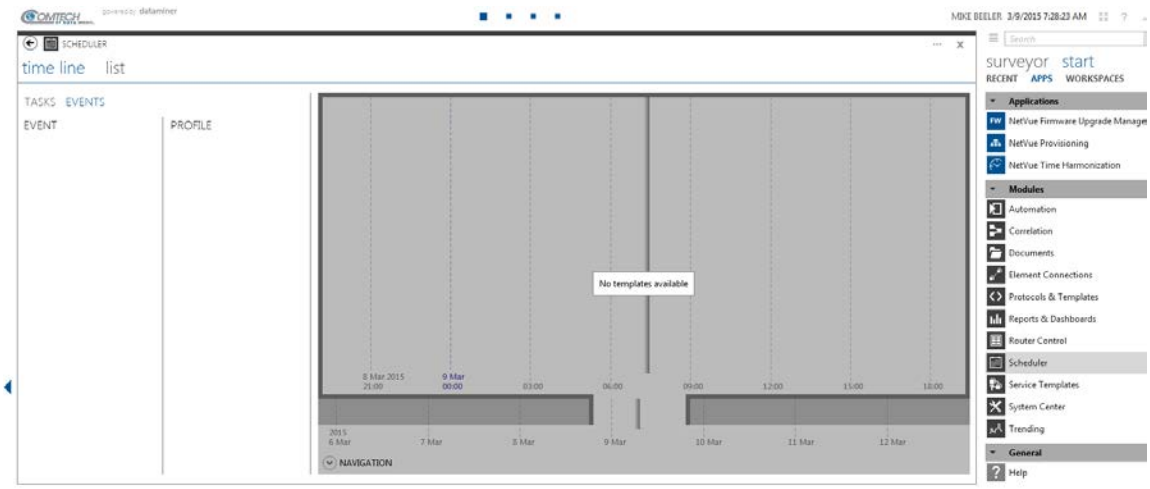


Figure 14-3. Scheduler Time Line, Events Example

In each of the subtabs, the large pane on the right shows the Scheduler timeline, where you can see the scheduled tasks.

The timeline has a preview pane at the bottom. The main timeline is an enlargement of the white section of the preview pane.

To zoom in or out, scroll in the timeline pane or drag the mouse right or left in the preview pane.

To zoom to a particular time, e.g., the next hour, or the past month, right-click the timeline, and select **Zoom to [time]**.

Open the **Navigation** section at the bottom for more options:

Click a button with a particular time to zoom to this time on the timeline, e.g., Today, Last week, Next month, etc.

To make the timeline move along with the current time, in the bottom left corner, select **Follow mode**.

To change the time zone for the timeline pane, in the bottom right corner, select a different **Time zone**.

To see disabled tasks also, in the **TASKS** tab, select **Include disabled tasks**.

To see only specific tasks on the timeline, in the **TASKS** tab, select **Show only selected tasks** and select the tasks in the list.

Within the tasks list, you can execute any of the existing tasks immediately, regardless of the interval and timing set for them. To do this, select the task and click the Execute button.

14.1.2 Manually Add a Scheduled Task

To add a new scheduled task, without a Scheduler template:

1. In the **Scheduler** app, go to the **list** tab.
2. Click the **Add** button.

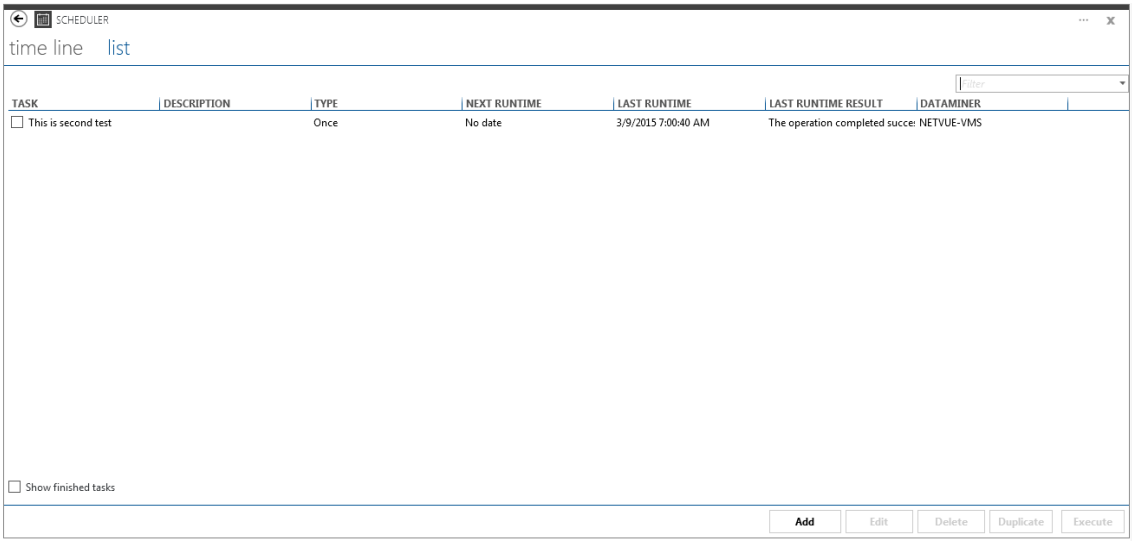


Figure 14-4. Add a Task

If you want to make a task that is very similar to an existing task, you can select the existing task and click the **Duplicate** button. In the same manner, you can edit existing tasks with the **Edit** button, or delete them with the **Delete** button.

1. In the **General** tab, enter a name and a description.
2. To enable the task immediately, make sure the **Enabled** check box is selected.
3. Click **Next** to go to the **Schedule** tab.

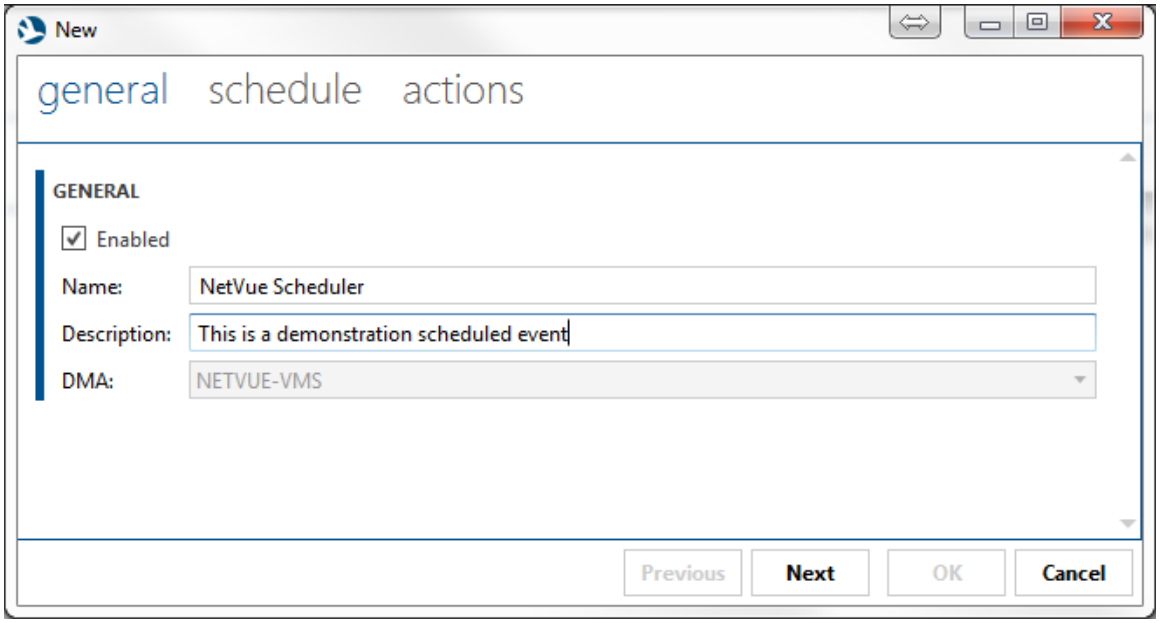


Figure 14-5. Enable a Task

4. Under **Schedule**, select the interval for task execution: once, daily, weekly or monthly.
5. Under **Time of execution**, select the time for task execution. Depending on the interval, different options are available.
6. Click **Next** to go to the **actions** tab.

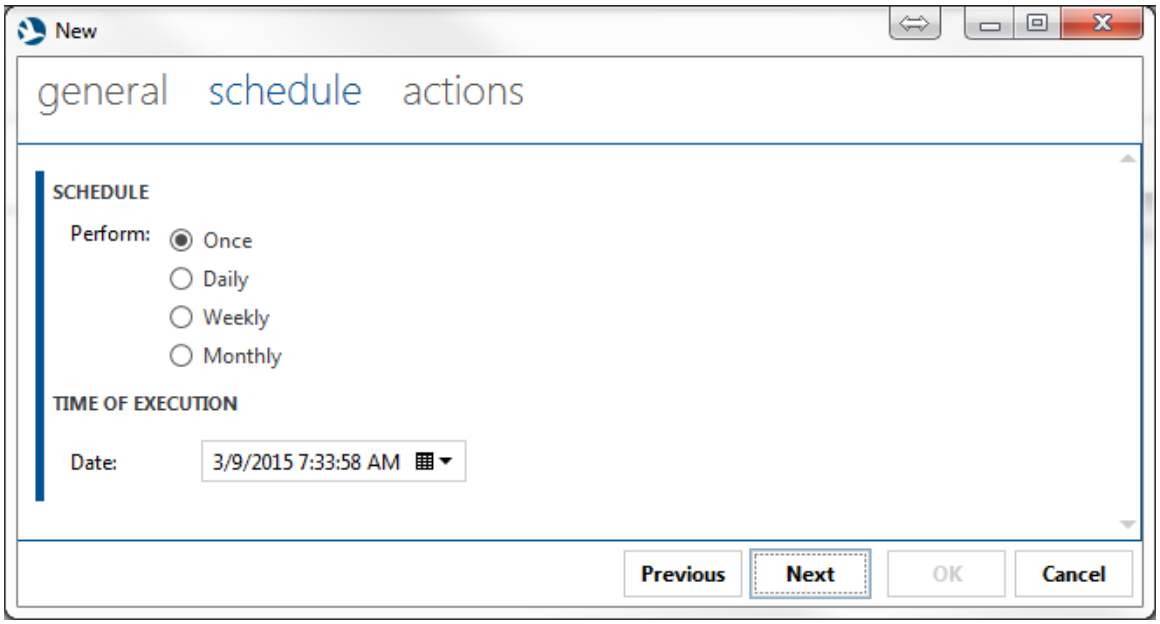


Figure 14-6. Schedule a Task

Actions include:

- **Information -** Specify a message that shows as an information event at the scheduled time.
- **SMS -** Specify a text message that is sent to the cellphone of a contact person.
- **Email -** Compose an email message, optionally including a report.
- **Upload report to FTP -** Specify an FTP server, and a report to upload to it.
- **Upload report to shared folder -** Specify a shared folder, and a report to upload to it.
- **Script -** Select an existing automation script to execute at the scheduled time. For more information on script execution options, see **Script execution options**.

Under the Actions tab:

1. Click **Add** and select the action.
    a. To add more actions, repeat the previous step until all actions have been added.
    b. To add actions that execute when the task is removed, select the option **Execute final actions when the task is removed**, and add the necessary actions below it.
2. When all the necessary actions have been added, click **OK**. The task then shows in the task list.
3. To see tasks that have already executed, select the **Show finished tasks** option in the bottom left corner.
4. To find a specific task in the list, use the filter box in the top right corner.

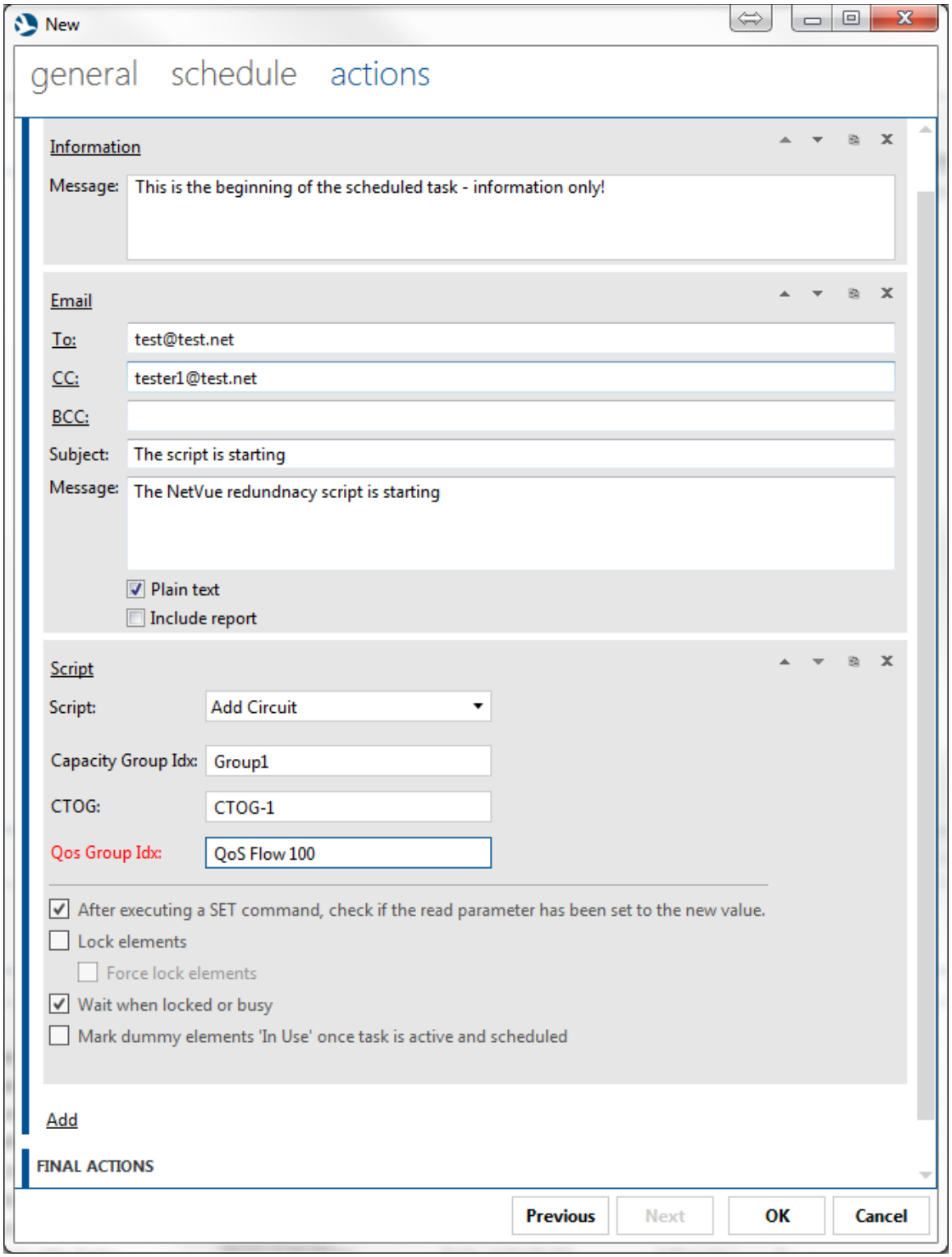


Figure 14-7. Actions Example

14.1.3 Schedule an Event Based on a Scheduler Template

Scheduled events are a combination of a START and STOP task, based on a special type of Automation script called a “Scheduler template”.

To schedule events in the **timeline > EVENTS** tab, first create a Scheduler template in NETVUE (NetVue) Automation. See **Creating a Scheduler template**.

Each of the events in the **EVENT** column represents an action or a sequence of actions set in the Scheduler template script.

The profiles in the **PROFILE** column are collections of preset dummies and/or parameter values for specific events.

On the timeline, the events show as rectangles, with the left and right edges of the rectangle representing the START and STOP task.

14.1.3.1 Schedule an Event

The starting time of any new event must be at least one minute in the future. You can change the time only for events that have not ended. If an event has already started, you can edit the end time only.

1. Drag an event or profile onto the timeline.
2. In the **Task** window, specify any dummies or parameters, if necessary.
3. Click **OK**.
4. To adjust the timing, drag the edges of the rectangle to a different point on the timeline. While you are dragging, the exact time shows under the rectangle.

If an event has not started, you can right-click the event’s rectangle on the timeline, and:

1. Select **Edit** to change the input dummies or parameters.
2. Select **Delete** to remove the event.

14.1.3.2 Schedule a Recurring Event

You can make a scheduled event into a recurring event. Make sure both tasks recur at the same interval, both daily or both weekly, but not one daily and the other weekly. Make sure recurrence does not make the tasks overlap.

You cannot edit an existing recurring event directly in the timeline. Use the **list** tab instead.

1. Go to the **list** tab.
2. Do this for both the START and the STOP tasks of the event:
    a. Select the task and click the **Edit** button.
    b. In the **schedule** tab of the **Edit** window, select the interval at which the tasks should recur.
3. Click **OK.**

14.1.4 Manually Start and Stop a Scheduled Event

You can start or stop a scheduled event any time.

1. In the **Scheduler** app, go to the **timeline > EVENTS** tab.
2. On the timeline, right-click the task's colored rectangle.
    a. To start a task immediately, select **Manual start**.
    b. To stop a running task immediately, select **Manual stop**.

14.1.5 Create a Scheduler Template

To create scheduler templates that show up in the **EVENT** list in **Scheduler**, use the **Automation** module in **System Display**:

1. In the System Display main menu, choose **Advanced > Automation**.
2. In the folder pane on the left, look for a script folder named **Scheduler Templates**.
3. Create the Scheduler Templates script folder if step 2 (above) did not produce the folder. NetVue Scheduler detects any scripts in this specific folder as possible events.
4. Select the Scheduler Templates folder.
5. Click the **Add** button to add a script.
6. Configure the script as described in the section **Working with Automation scripts in System Display**. However, to make the script usable as a Scheduler template, add a parameter named **Action**.

While the scheduled task runs, the value of the Action parameter is set to **START** or **STOP** automatically. The values are set to be the same as the start and stop times linked to the left and right border of the task rectangle in Scheduler.

Add comments to the top of the script for additional configuration of the scheduler event:

1. For each profile you want to create for the event, add a comment similar to this:
   `Preset="ProfileName" [Parameter name]="value"[Dummy name]="[DMA ID]/[Element ID]"`

   Example: To define an Event Profile named **MyPresets** that contains a preset value for two parameters named **From** and **To,** and one dummy named **MyDummy**, add this comment:

   `Preset="MyPresets" From="a" To="b" MyDummy="34/2"`

   In this example, the dummy value is 34/2, meaning Element ID 2 of DMA ID 34.
2. To show text on the task rectangle for an event, add a comment similar to this:
   `Display="Text to be displayed"`

   You can have script dummies or script parameters shown this way, by using syntax similar to this:
   - For a dummy: `Display="{d:MyDummy}"`
   - For a parameter: `Display="{p:MyParameter}"`
3. To show a custom tooltip over the task rectangle for an event, add a comment similar to this:
   `ToolTip="Tooltip text"`

If you do not define a custom tooltip, the default tooltip shows the value of every parameter and dummy.

Chapter 15. SPECTRUM ANALYSIS

15.1 Introduction to the NetVue™ SpectrumVue-8

The NetVue™ SpectrumVue-8 is an integrated spectrum analyzer that operates with the Comtech EF Data NetVue product. Because the SpectrumVue-8 is integrated with and controlled by the NetVue NMS, you use the native NetVue Cube interface to operate the SpectrumVue-8.

The SpectrumVue-8 has eight input ports. Connect it to as many as eight input feeds through either SMA (50Ω) or F-type (75Ω) input connectors.

The SpectrumVue-8 views one spectrum (single carrier frequency) at a time. However, using "move and dwell," the SpectrumVue-8 takes snapshots from various frequencies and inputs.

The SpectrumVue-8 does two types of spectral monitoring:

- Continuous spectral monitoring for dedicated troubleshooting (dedicated to a single port), or;
- "Move and dwell" monitoring of up to eight input feeds, by dwelling long enough to record the spectrum on an input or frequency, and then moving to another frequency or input.

A network may have one or multiple SpectrumVue-8 devices. The SpectrumVue-8 supports IF and L-Band operation that may be installed in racks in a common area. No dedicated spectrum analyzer is required if the SpectrumVue-8 is installed.

The SpectrumVue-8 works well for teleports (local and remote) and distributed sites with multiple feeds, where multiple spectrums must be monitored.

The SpectrumVue-8 is an option that can be purchased with the standard NetVue™ product. For more details on the SpectrumVue-8, see the datasheet at www.comtechefdata.com.

Figure 15-1. SpectrumVue-8 Front Panel

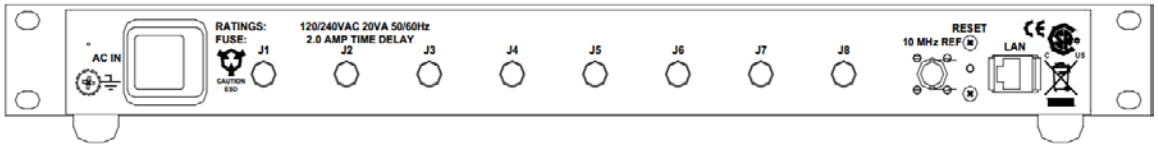


Figure 15-2. SpectrumVue-8 Rear Panel

15.2 Get Started with the SpectrumVue-8

Before using the SpectrumVue-8, make sure the SpectrumVue-8 protocol is loaded in the NetVue. See Chapter 4 Protocols in this guide for instructions.

There are two operating modes for the SpectrumVue-8:

- **Integrated** carrier view that is embedded in the templates.
- **Single seat** carrier monitoring and view.

15.2.1 Integrated Operation for SpectrumVue-8

Figure 15-3. Integrated operation shows the spectrum views in the user templates. One SpectrumVue-8 can be shared among many templates. The views are acquired by the SpectrumVue-8's eight (8) input ports.

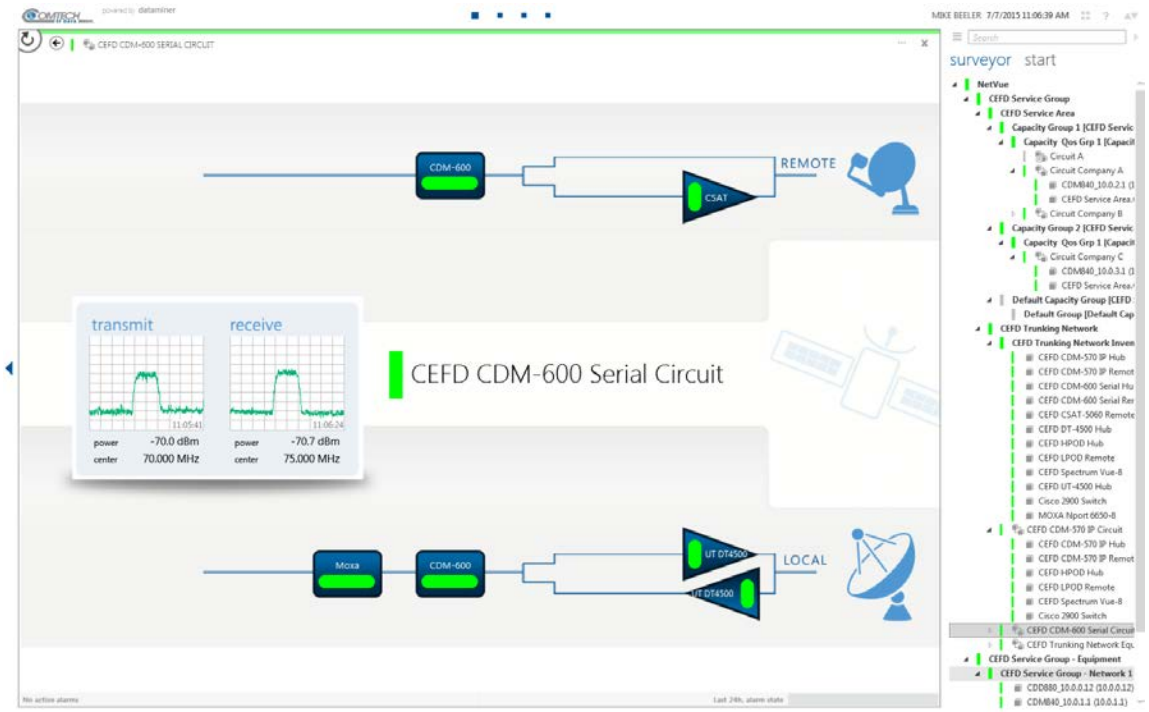


Figure 15-3. Integrated SpectrumVue-8 (Circuit View)

As described in the NetVue Provisioning Guide, use the NetVue Provisioning Tool (NVPT) to create the spectrum views and integrate the SpectrumVue-8 carrier images into the user circuit view.

15.2.2 Single-seat Operation for SpectrumVue-8

The NetVue Cube, when combined with the SpectrumVue-8, gives you a single-seat operation point. Use it to view the spectrum, CEFD equipment and any third-party device that is being monitored. You can troubleshoot, diagnose or monitor the spectrum locally or remotely in the NetVue™ network.

15.3 Configure the SpectrumVue-8 for Real-time Spectrum Analysis

Use the NetVue Cube to configure the SpectrumVue-8 to do real-time spectral analysis. See Figure 15-4.

To configure the import port:

1. Select the SpectrumVue-8 as a device.
2. Select an input port:
    a. Select the **Manual** column.
    b. Select **Measurement Points.**
    c. Select the points from the list at the right.

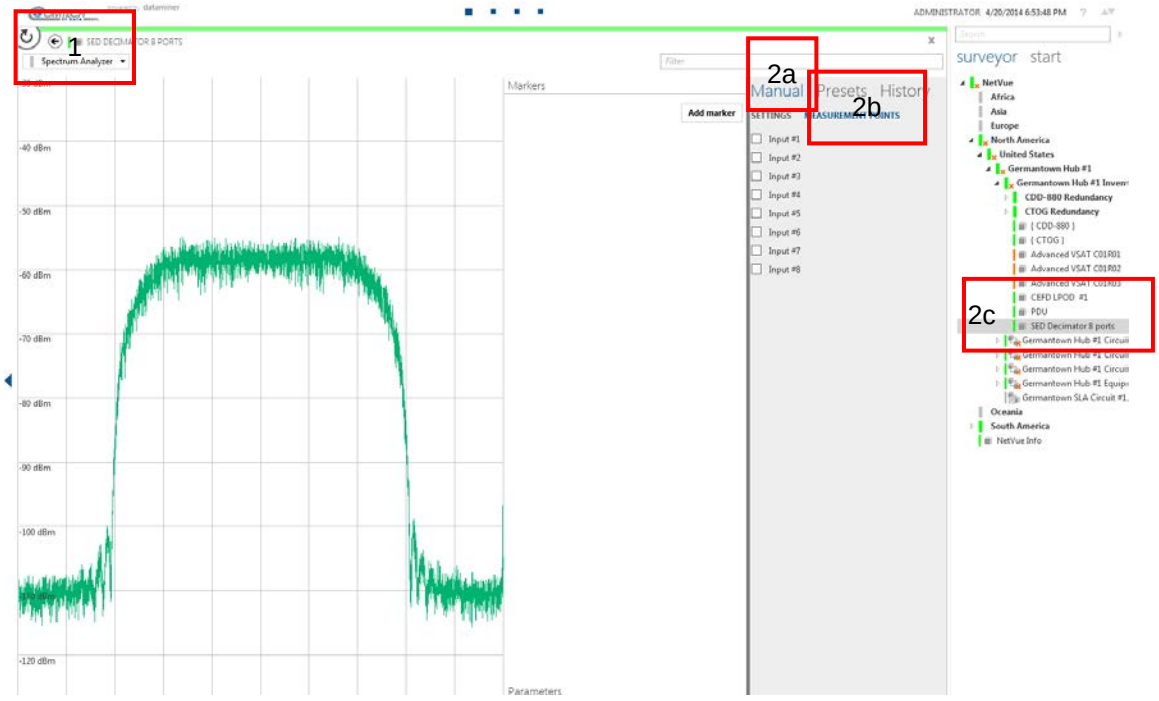


Figure 15-4. SpectrumVue-8 Input Configuration

To configure the settings (See Figure 15-5):

1. Select **Settings**.
2. Enter the **Start**, **Stop**, or **Center** frequency and **Sweep Range**.

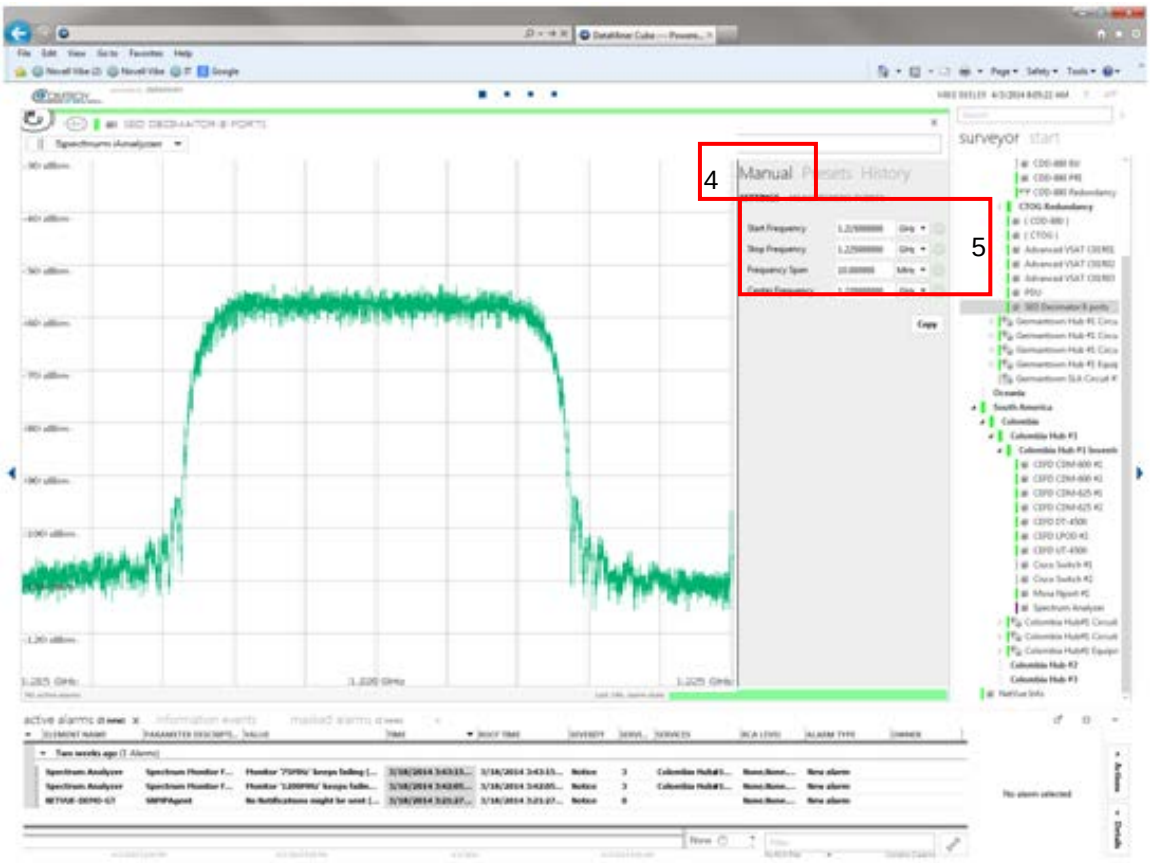


Figure 15-5 SpectrumVue-8 Spectrum Configuration

Chapter 16. NETVUE CUBE DESKTOP APPLICATION

16.1 Introduction

The NetVue Cube Desktop is a stand-alone application that gives you the Cube interface to a NetVue server without using a standard Web browser.

16.2 Install the NetVue Cube Desktop Application

1. Install the application on a computer that connects to the NetVue server.
2. Open a web browser and navigate to http://*<NetVue_Server_IP>*/tools/
3. Under the **Stand-alone Applications** section, do either one of these install options:
   a. Left-click the **NetVue Cube Desktop Application: install via click-once web installer** link.
   - or -
   b. Right-click **install manually via MSI installer** link.

Figure 16-1. Desktop Application Installer

4. Select **Save target as…** and choose a download location.
5. If using the MSI installer, after the download has finished, go to the download location.
6. Run the DataMiner Cube.msi file to start the installation wizard.

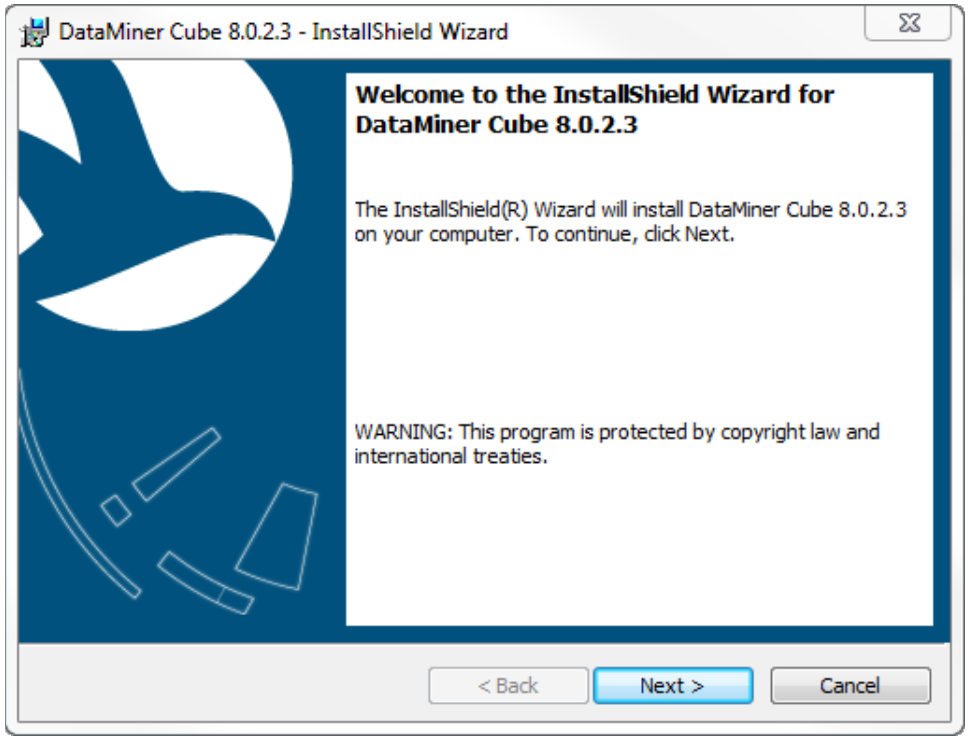


Figure 16-2. Installation Wizard Window

7. Click **Next** to start the installation.

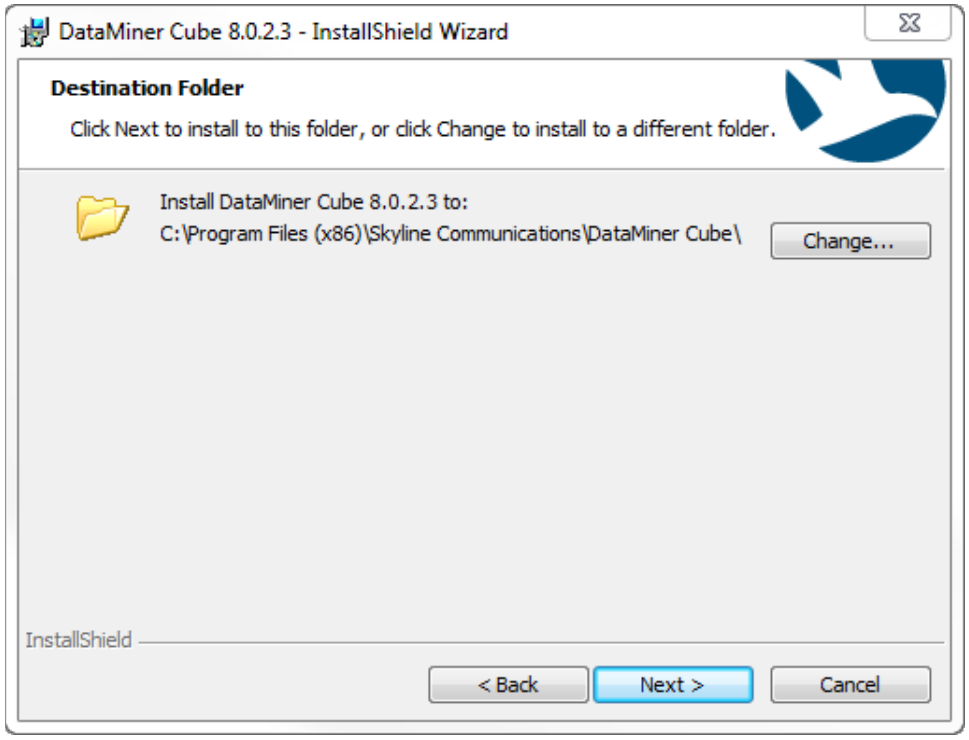


Figure 16-3. Select Installation Folder Window

8. Select an installation location and click **Next**.
9. After the installation is completed, choose whether or not to **Launch the program**, and then click **Finish**.

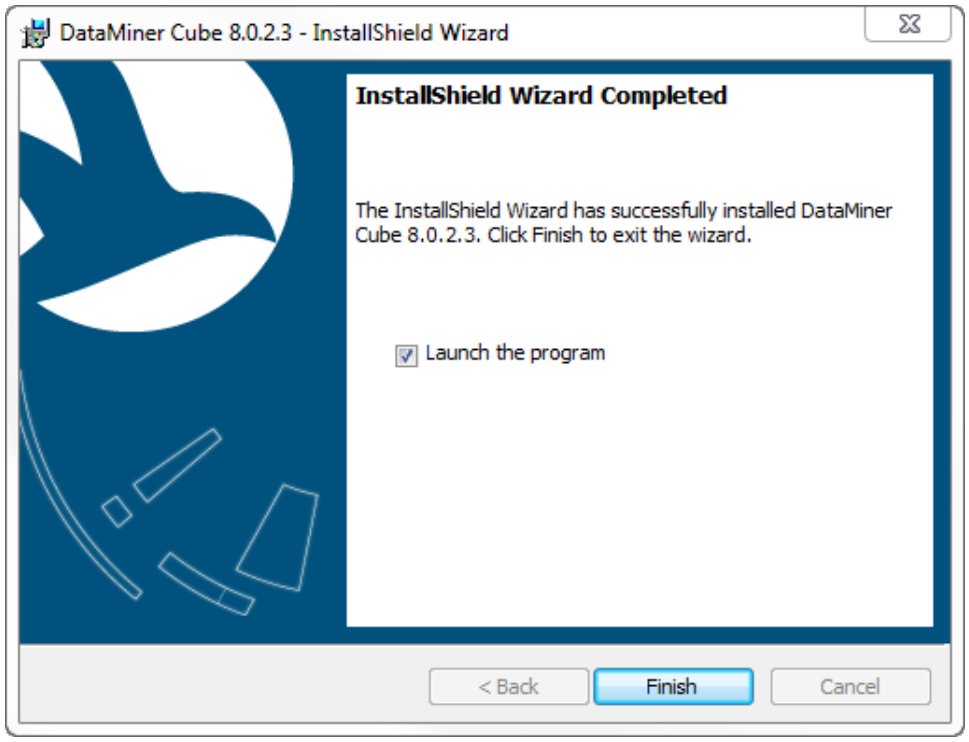


Figure 16-4. Installation Complete Window

16.3 Start the NetVue Cube Desktop Application

To start the NetVue Cube Desktop Application:

1. Go to **Start | All Programs | Skyline Communications** and click the **DataMiner Cube** shortcut.

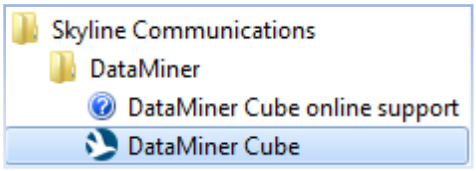


Figure 16-5. DataMiner Cube Shortcut

2. On the log-on window:
   a. Enter the **Connect to** –name or IP address of the NetVue Agent to be connected.
   b. Enter the **Domain\User name** – the domain (if applicable) and user name of the NetVue account to be connected.
   c. Enter the **Password** – the password of the NetVue account to be connected.
3. Click **Log on**.

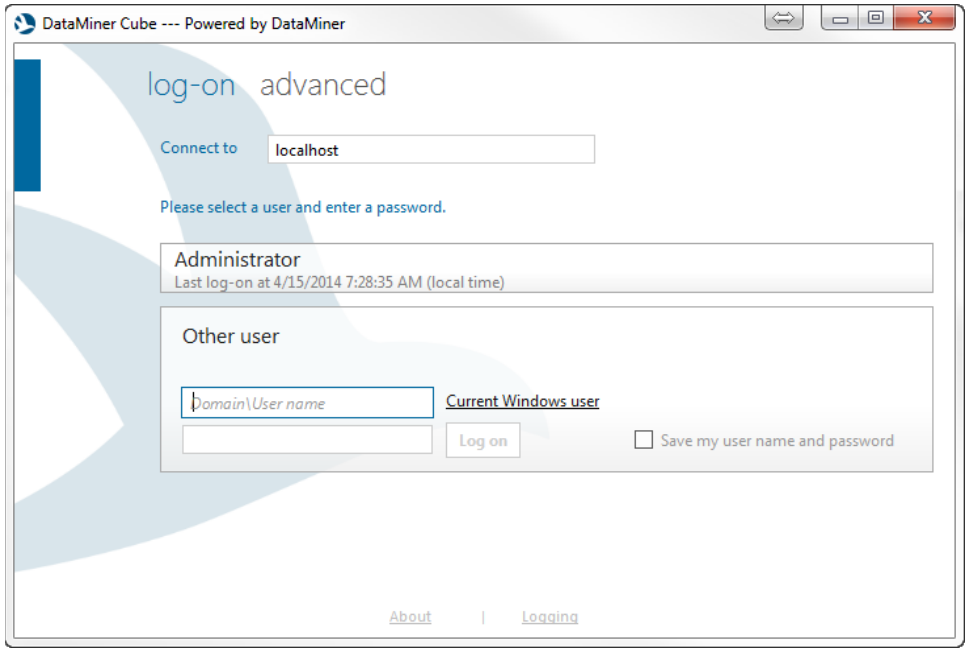


Figure 16-6. Log-on Window

The NetVue Cube Desktop application connects to the specified NetVue Agent. The interface is identical to the Web GUI described in Chapter 2.3.2.

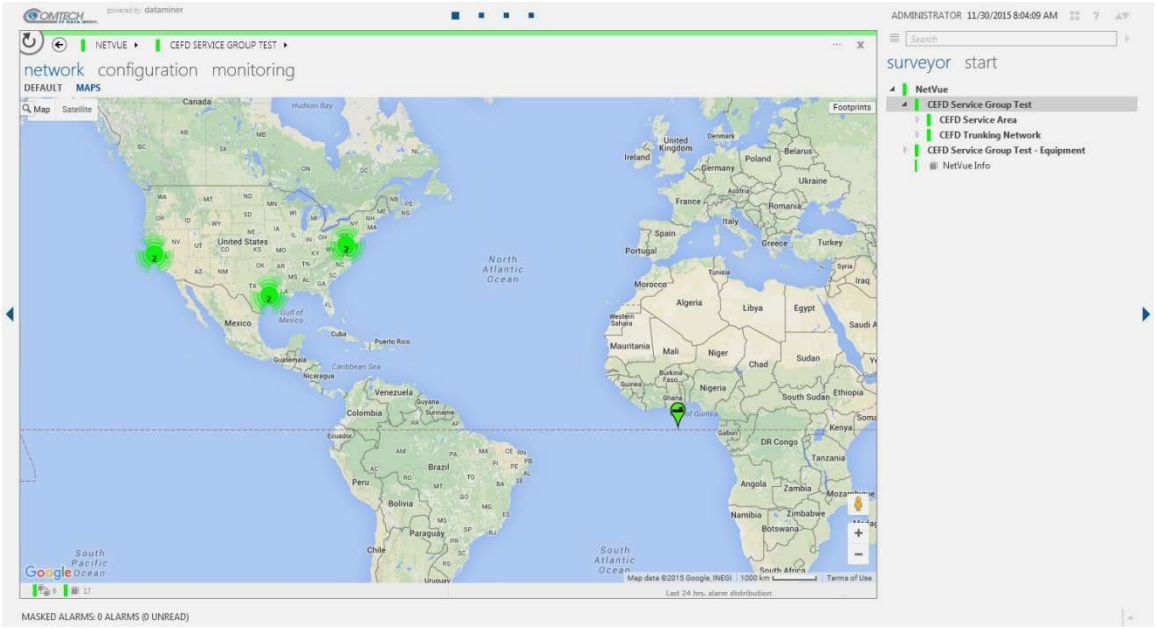


Figure 16-7. NetVue Cube Interface Window

Chapter 17. ALERTER

17.1 Introduction to the Alerter

The Alerter, also known as the Skyline Alerter, is a system tray application. When an alarm occurs in the connected NetVue System, the Skyline Alerter generates a popup balloon to notify users.

Install the Skyline Alerter application, then configure these parameters.

- Connection Accounts
- Alarm Filters
- Notification Options
- Program Preferences

17.2 Install the Alerter

To install the Alterter:

1. Open a web browser and go to http://<*NetVue_Server_IP*>/tools/.
2. In the Stand-alone Applications section, right-click **Skyline Alerter: install manually via MSI installer.**
3. Select **Save target as**… and choose a download location.
4. After the download has finished, go to the download location.
5. Run the SLAlerterSetup.msi file to start the **Skyline Alerter Setup Wizard.**
6. Click **Next** to start the setup.

Figure 17-1. MSI Installer

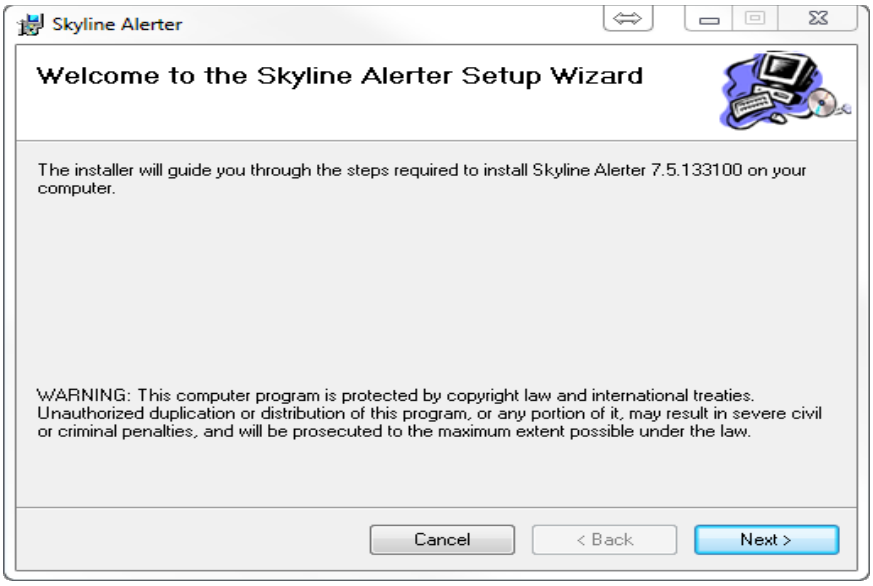


Figure 17-2. Setup Wizard Window

7. On the **Select Installation Folder** window, browse to and select a folder.
8. Under **Install Skyline Alerter for yourself, or for anyone who uses this computer**, select one of these options:
   - Everyone
   - Just me
9. Click **Next** to continue.

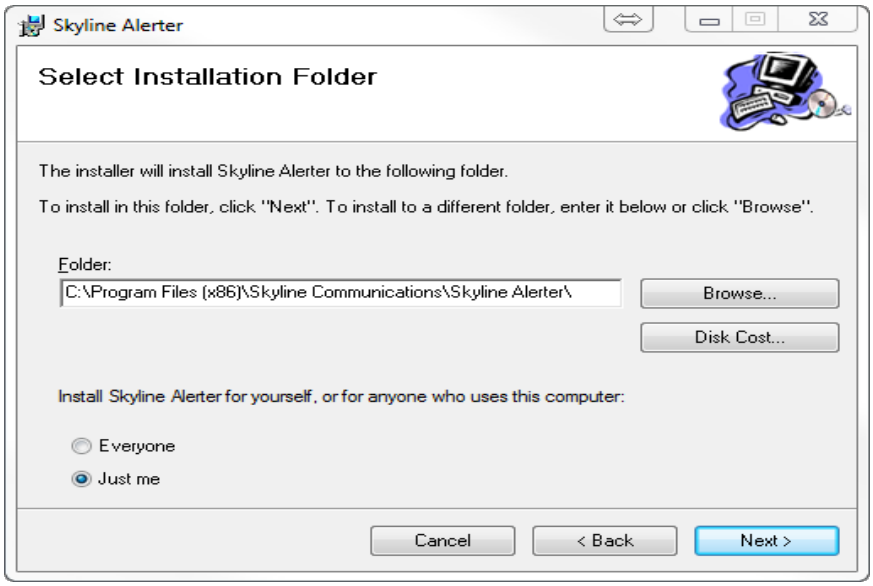


Figure 17-3. Select Installation Folder Window

10. On the **Confirm Installation** window, click **Next** to confirm and start the installation.

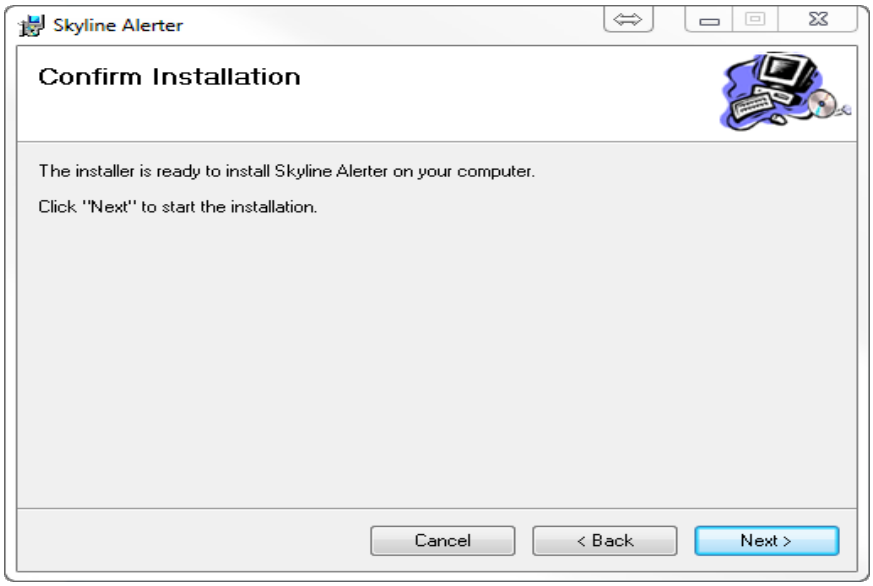


Figure 17-4. Confirm Installation Window

11. When the **Installation Complete** window opens, click **Close**.

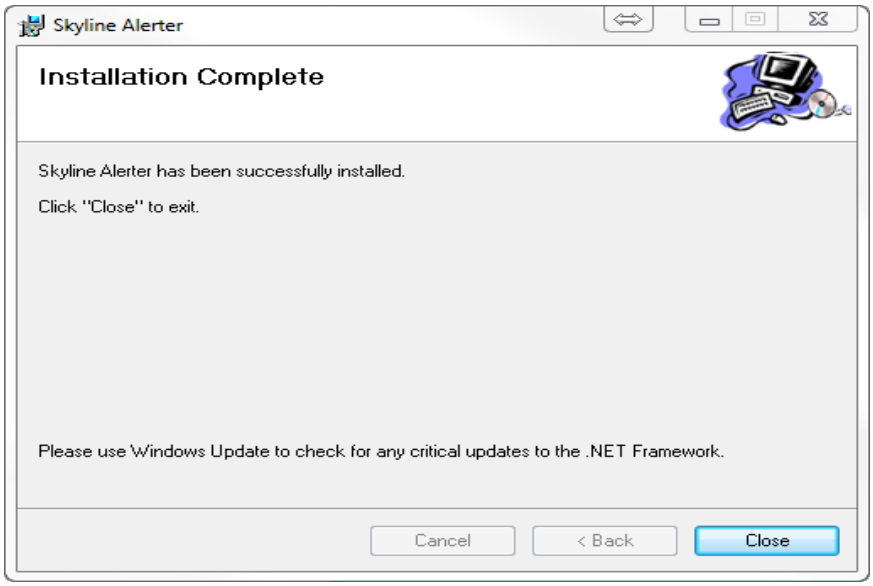


Figure 17-5. Installation Complete Window

It is recommended that you update Windows, and install any .NET Framework updates that are available for this computer.

17.3 Start the Alerter

To start the Skyline Alerter for the first time:

1. Go to **Start | All Programs**.
2. Click the **Skyline Alerter** shortcut.

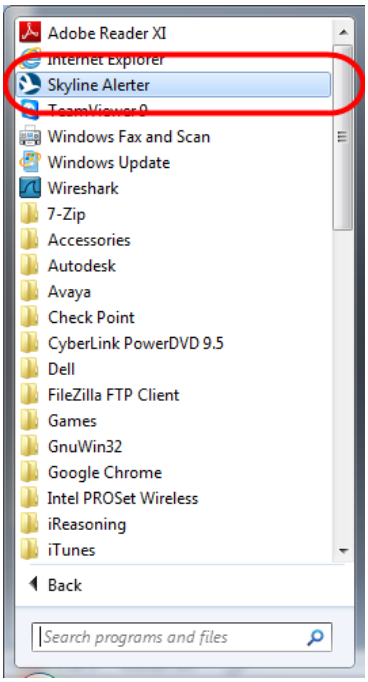


Figure 17-6. Skyline Alerter Shortcut Window

3. On the **Add Account** window:
   a. Enter the **connect to** – name or IP address of the NetVue Agent to be connected.
   b. Enter the **domain\user** – the domain (if applicable) and user name of the NetVue account to be connected.
   c. Enter the **password** – the password of the NetVue account to be connected.

4. Click **Add account**.

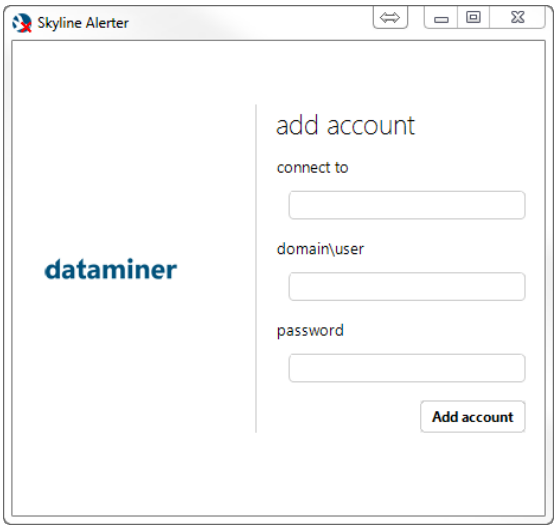


Figure 17-7. Add Account Window

The Skyline Alerter connects to the specified NetVue Agent, and two additional tabs show on the Skyline Alerter main window.

- **alarms tab** – a listing of the last 100 alarms received by the Skyline Alerter; this is the default tab view at the time of startup.
- **collaboration tab** – the NetVue chat collaboration, which allows you to exchange chat messages with other users logged into the NetVue System; identical to the NetVue Cube chat collaboration.

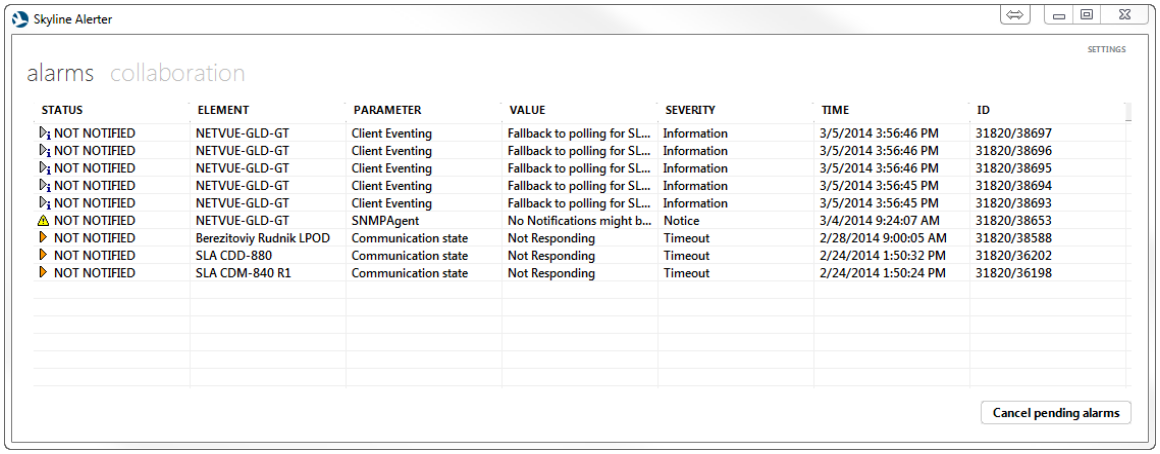


Figure 17-8. Skyline Alerter Main Window

17.4 Configure the Alerter

17.4.1 Connect to a Different NetVue System

You can connect the Skyline Alerter to a NetVue System other than the originally configured system.

1. On the Skyline Alerter main window, click the **Settings** button.

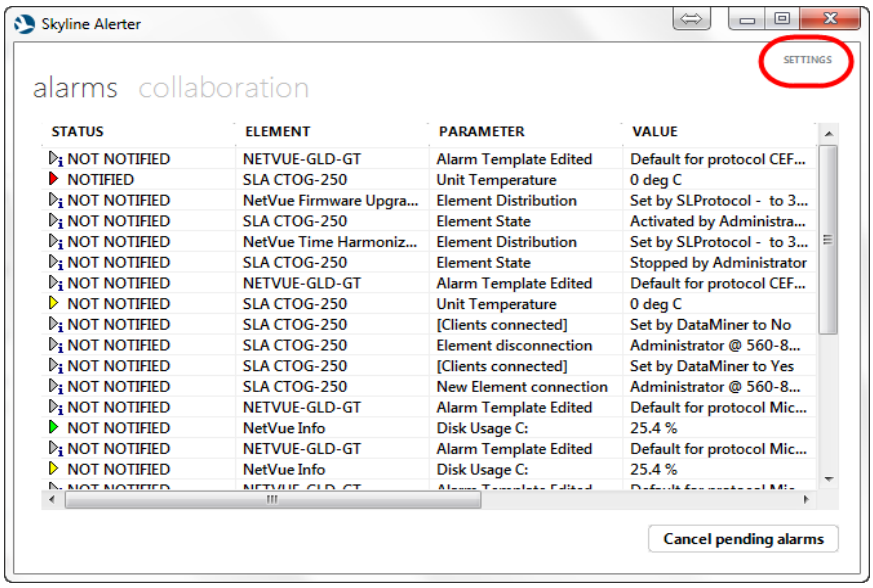


Figure 17-9. Skyline Alerter Window | Settings Button

2. On the **Options** window, select the **DMS Connections** tab.
3. Click **Edit Account.**

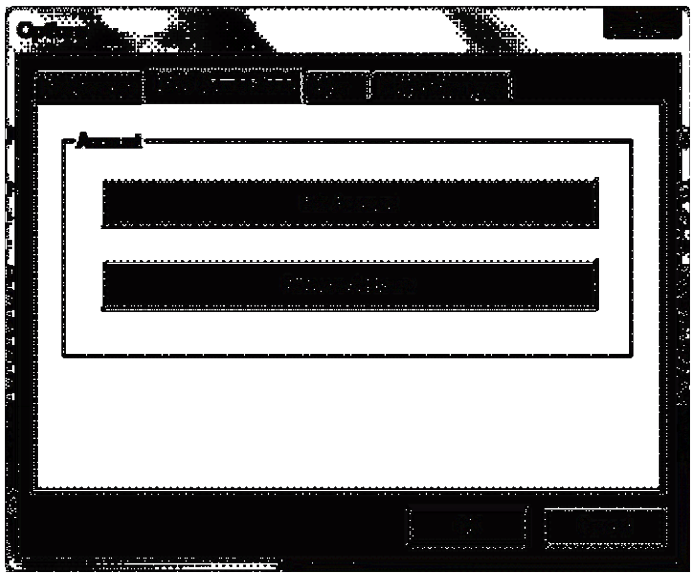


Figure 17-10. Options Window | DMS Connections Tab

4. The **Add Connection** window opens.
    a. Enter the **Name of DMS**. This is a name you create for the NetVue System.
    b. Enter the **Host** name or IP address of the NetVue Agent to be connected.

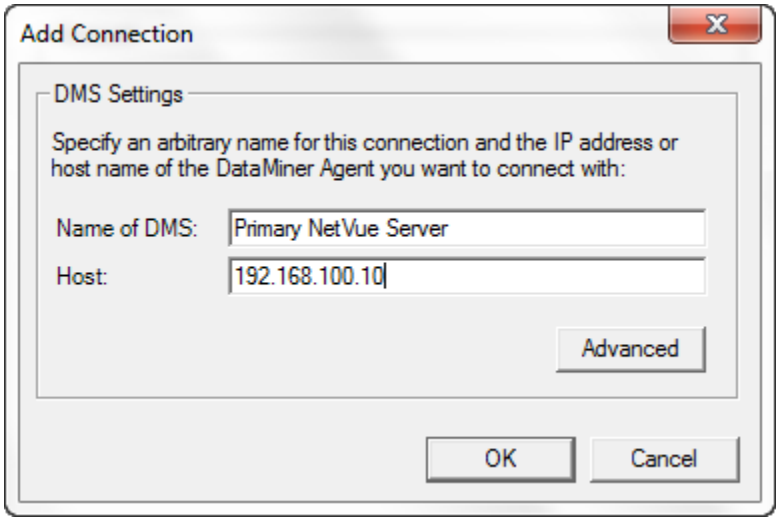


Figure 17-11. Add Connection Window

5. If the default connection settings need to be changed, click the **Advanced** button to open the **Connection Settings** window. Make the necessary **Connection Settings** changes.

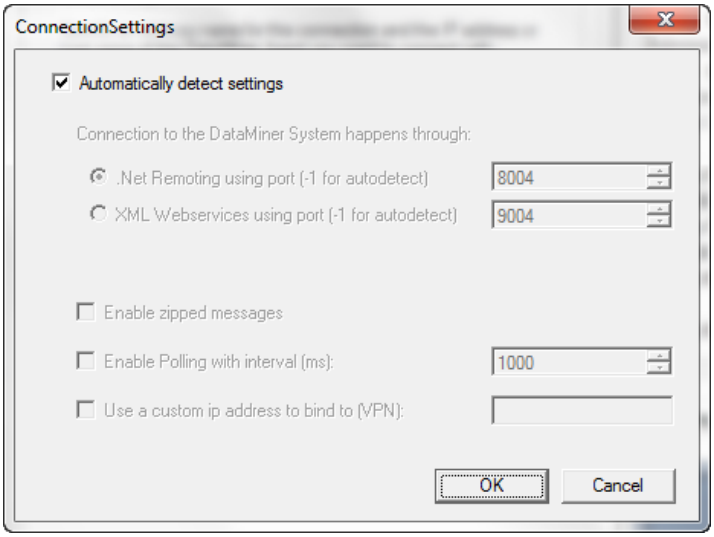


Figure 17-12. Connection Settings Window

6. Click **OK**
7. When prompted, select **Yes** to apply the changes and reconnect to the new NetVue System.

17.4.2 Set the Alarm Filter

You can set the Skyline Alerter to filter specified parameters. This filtering restricts alerts to a specific subset of alarms.

Decide whether to use a simple client-side filter, an advanced client-side filter or a server-side filter. If you use any client-side filter, all alarms are sent to the client. If you use a server-side filter, only the unacknowledged alarms are sent to the client.

1. On the Skyline Alerter main window, click the **Settings** button (see Figure 17-9).
2. On the **Options** window, select the **Filter** tab.

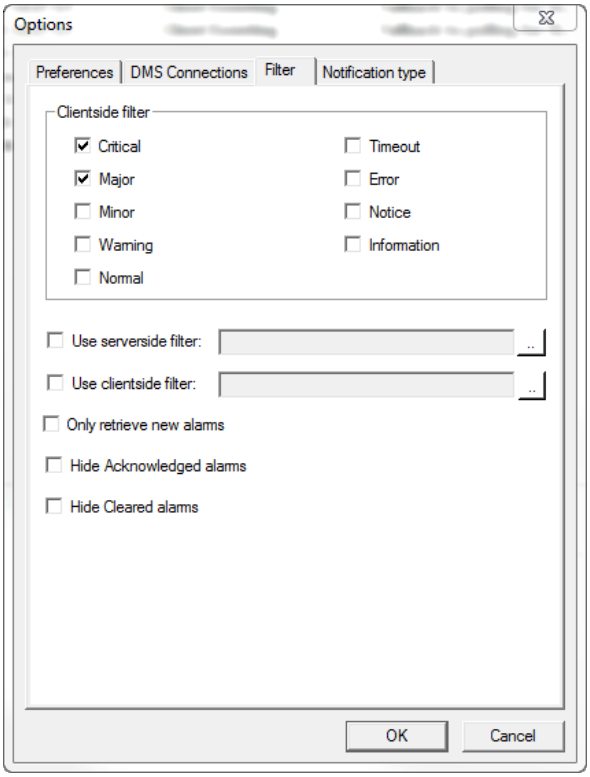


Figure 17-13. Options Window | Filter Tab

3. If you use **Client-side filtering**, select the applicable options:
    - Simple Client-side filter – in the Clientside filter section.
    - Select which alarm types must cause alerts.
    - Advanced Client-side filter.
4. Select the **Use clientside filter** option.
5. Click the ellipsis button on the right to open a list.
6. Select one of the available client-side filters (as configured in System Display).
7. If you use **Server-side filtering** select the applicable options.
8. Select the **Use serverside filter** option.
9. Click the ellipsis button on the right to open a list.
10. Select one of the available server-side filters (as configured in System Display).
11. If desired, select these options:
    - **Only retrieve new alarms** – when a NetVue System is connected, any existing alarms do not cause alerts. New alarms will cause alerts.
    - **Hide acknowledged alarms** – any alarms that have already been acknowledged do not cause alerts.
    - **Hide cleared alarms** – alarms that have already been cleared do not cause alerts.
12. Click **OK** to accept and apply the changes.

The Skyline Alerter never shows masked alarms.

17.4.3 Set the Notification Options

You can set these notification options:

- Limit the time that popup balloons remain visible.
- Enable or disable sounds to play when popup balloons open
- Choose the computer default beep or other sounds.

To set the Notification options:

1. On the Skyline Alerter main window, click the **Settings** button (see Figure 17-9).
2. On the **Options** popup window, select the **Notification type** tab.

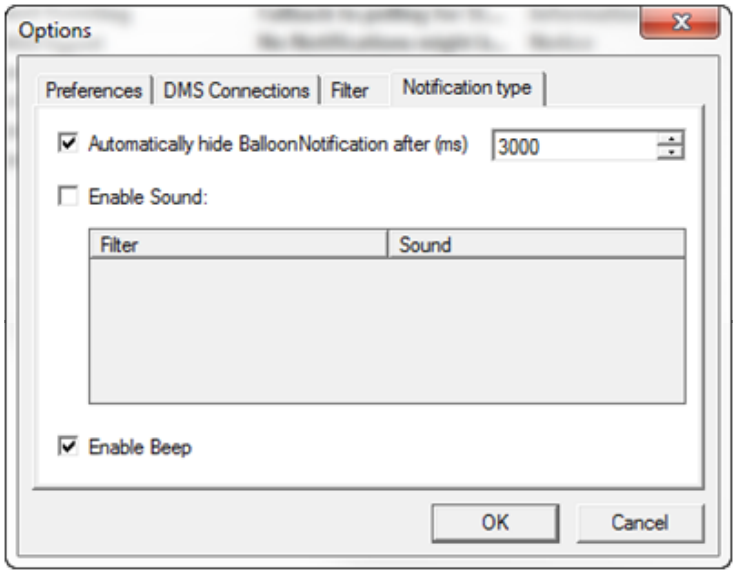


Figure 17-14. Options Window | Notification Type Tab

3. To cause the popup balloons to close automatically after a set amount of time:
    a. Select **Automatically hide Balloon Notification.**
    b. Select the length of time (in milliseconds) for the popup balloon to be visible.
4. To play specified sounds (instead of the computer's default beep) when a popup balloon opens, select the **Enable Sound** option. The **Filter and Sound Selection** window will open.

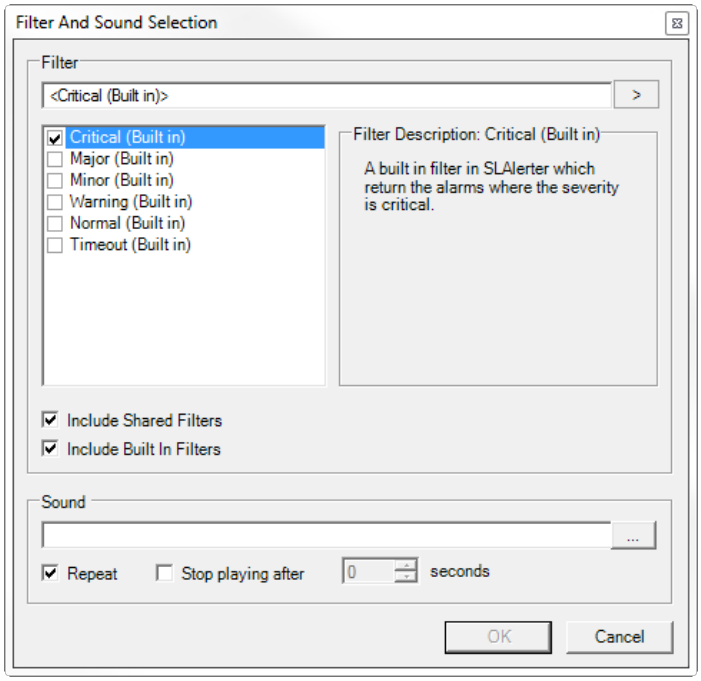


Figure 17-15. Filter and Sound Selection Window

5. For each alarm severity, select these options:
    a. Click the severity type.
    b. Select the .wav sound file.
    c. Select **Repeat** to cause the .wav file to play repeatedly, if desired.
    d. Select **Stop playing after** and enter how long (in seconds) the .wav file must keep playing.
    e. Select **Include Shared Filters** to include all the user-configured shared filters in the system when you select a filter from the list shown.
    f. Select **Include Built-in Filters** to include all the pre-configured filters that are standard in the system.
    g. To play the computer's default beep sound (instead of specified sounds) when a popup balloon opens, select the **Enable Beep** option on the **Options** window. See Figure 17-14.
6. Click **OK** to save the changes.

17.4.4 Set the Program Preferences

Program Preferences include:

- **Run Skyline Alerter when Windows starts** – automatically starts the Skyline Alerter when Windows starts.
- **Automatic login** – automatically logs in to the NetVue System when the Skyline Alerter is started.
- **As windows user** – the Skyline Alerter connects to the NetVue System using the current Windows login credentials.
- **As custom user** – the Skyline Alerter connects to the NetVue System using the user-defined login credentials.

To set the Program Preferences:

1. On the Skyline Alerter main window, click the **Settings** button. See Figure 17-9.
2. On the **Options** window, select the **Preferences** tab.

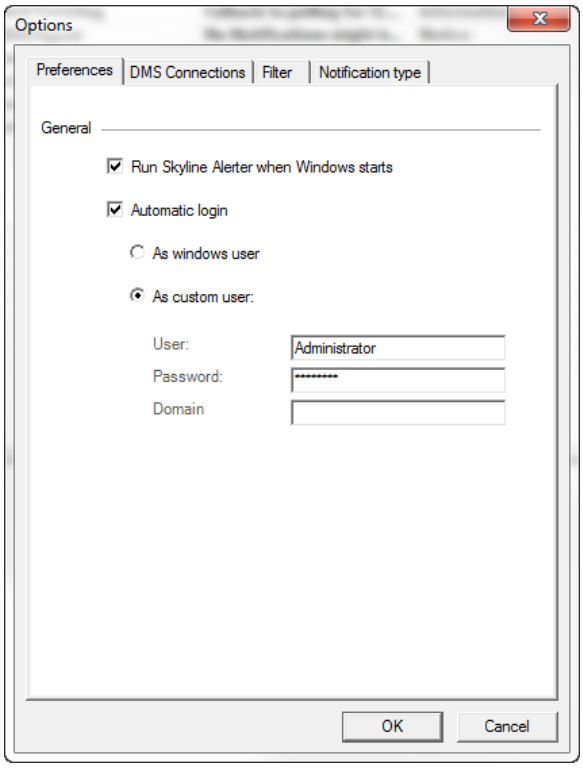


Figure 17-16. Options Window | Preferences Tab

3. Select **Run Skyline Alerter when Windows starts** to start the Skyline Alerter automatically with Windows.
4. Select **Automatic login** to automatically log in to the NetVue System when the Skyline Alerter is started.
5. Select **As windows user** to cause the Skyline Alerter to connect to the NetVue System with the current Windows login credentials.
6. Select **As custom user** to cause the Skyline Alerter to connect to the NetVue System with user-defined login credentials.
7. Enter the **User**, **Password** and **Domain** for the **custom user**.
8. Click **OK** to apply the changes.

17.5 Alarms List

The alarms list shows the last 100 alarms received by the Skyline Alerter. For each listed alarm, the Status column shows whether or not:

- An alarm has already been processed
- A popup balloon has already opened

Cancel pending alarms – Click this button if an alarm storm occurs (when too many alarms are occurring at once).

17.6 Popup Balloons

A popup balloon opens when a new alarm is received by the Skyline Alerter. A popup balloon shows this information about an alarm:

- Alarm severity – the status bar color shows the alarm severity. See 17.6.1 Alarm Severity Levels.
- Element name – Appears next to the status bar in bold text.
- Parameter name – Appears under the Element name.
- Parameter value - Appears below the Parameter name.
- Time stamp – Appears on the right side of the balloon.

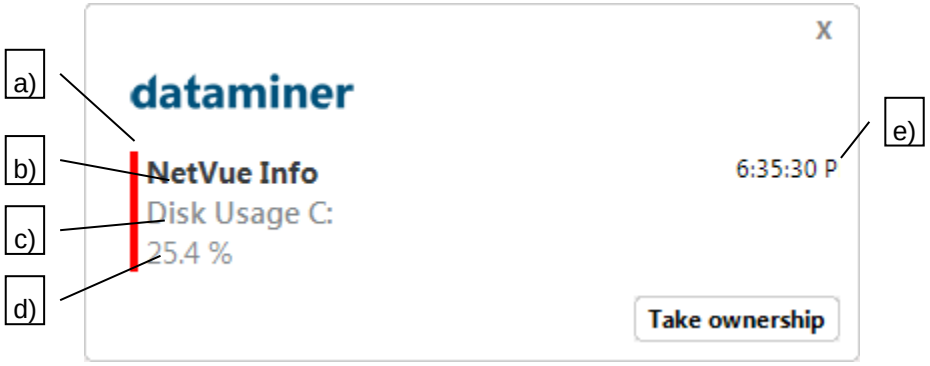


Figure 17-17. Popup Balloon Example

1. **Take ownership** – Click this button to take ownership of the alarm.
2. To close a popup balloon, click the **x** in the upper right corner of the balloon.

17.6.1 Alarm Severity Levels

There are five threshold severity levels, each indicated by a color:

Normal	**Green**
Warning	**Blue**
Minor	**Cyan**
Major	**Yellow**
Critical	**Red**

System administrators can change these default colors, if necessary (e.g., to match other systems).

Appendix A. NETVUE SERVER FIREWALL CONFIGURATION

A.1 Manual Configuration of the Standalone NetVue Server Firewall

When you receive your NetVue IMS server, the Windows Firewall is configured. If you want to reconfigure the server firewall manually, do these steps:

1. If the **Icons** display is in effect, choose **Start → Control Panel → Windows Firewall**.
   a. Hold the mouse cursor in the lower left corner of the screen to use the **Start** menu.

Figure A-1. Start Menu Icon

2. If the **Category** display is in effect, choose **System & Security → Windows Firewall**.

3. Click the **Control Panel** icon.

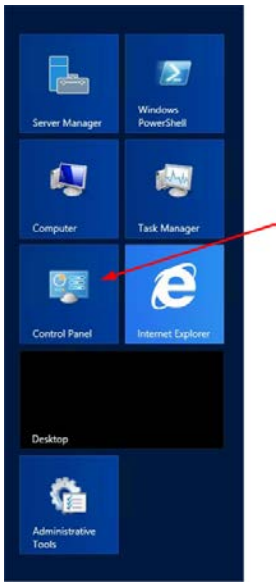


Figure A-2. Control Panel Icon

4. Click **System Security**.

Figure A-3. System and Security Menu

5. Click **Windows Firewall**.

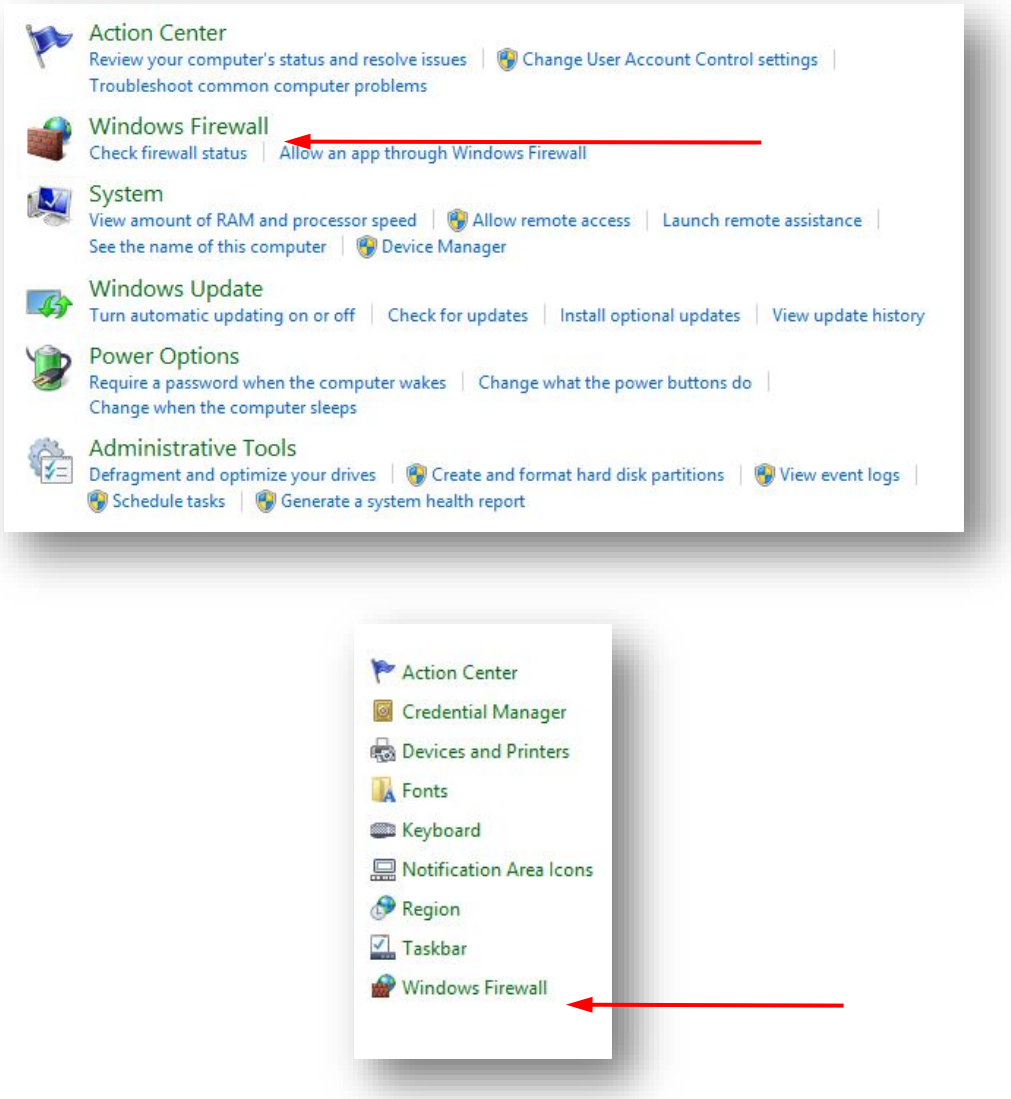


Figure A-4. Windows Firewall option in the System and Security Menu (two examples)

6. In the left-hand pane of the **Windows Firewall** configuration panel, click **Advanced Settings.**

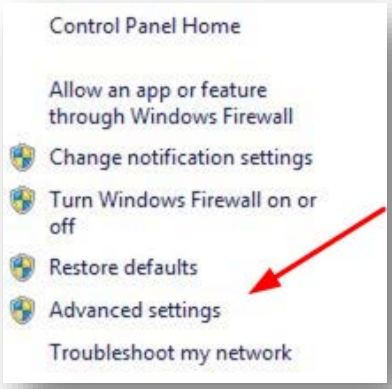


Figure A-5. Advanced Settings

7. Select **Inbound Rules,** which is found at the top of the left-hand panel of **Advanced Settings.**

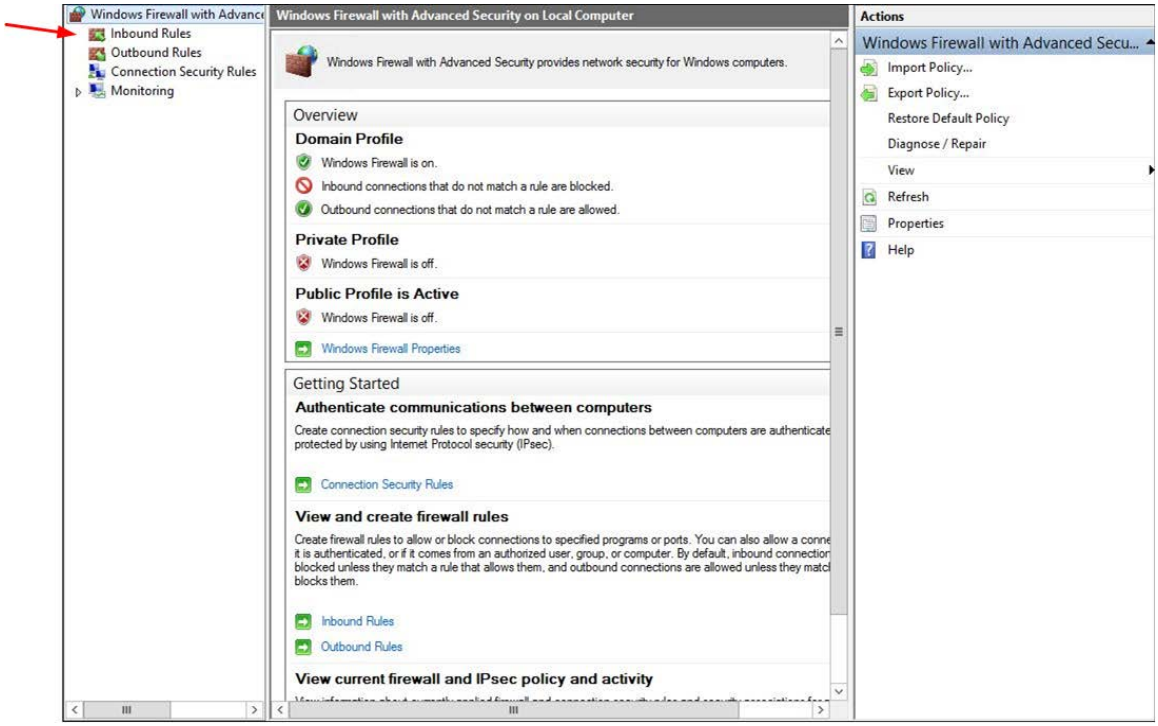


Figure A-6. Inbound Rules

8. Select **New Rule...**, which is found in the right-hand panel**.**

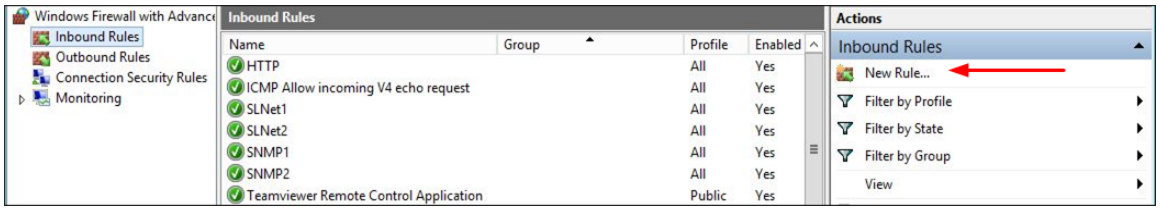


Figure A-7. New Rule

9. To allow access to/from a specific port, select **Port**, then **Next.**
    a. Other available rule options include **Program**, **Predefined** or **Custom.**

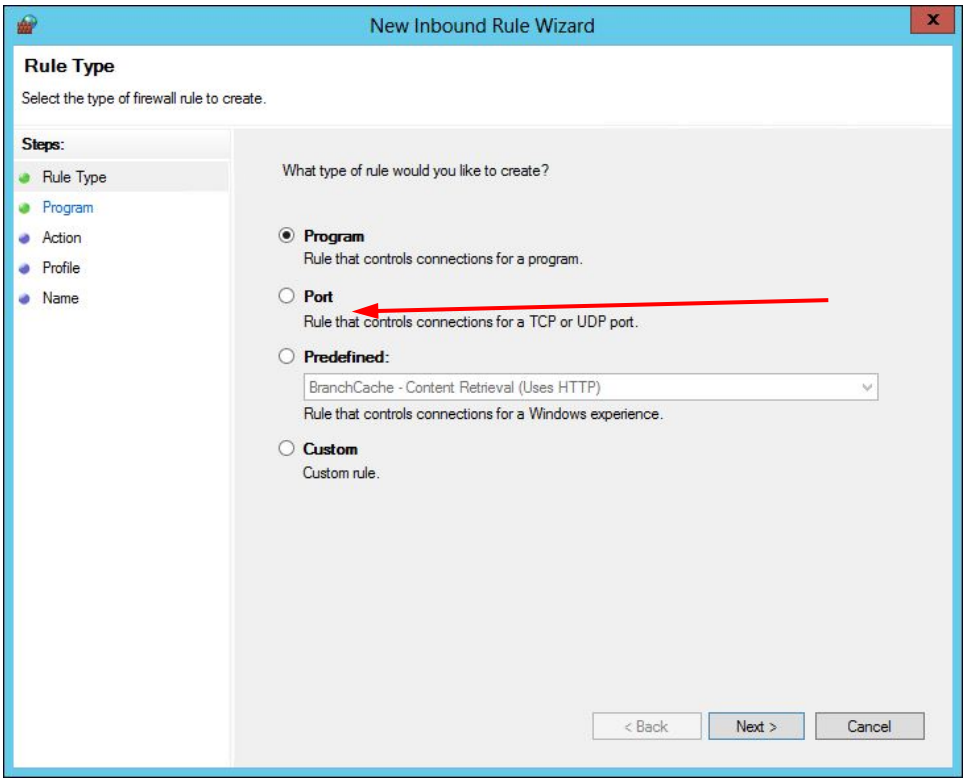


Figure A-8. New Inbound Rule Wizard Screen Example

10. Select the traffic type for this rule, **TCP** or **UDC**.
11. Specify the allowed port number(s).

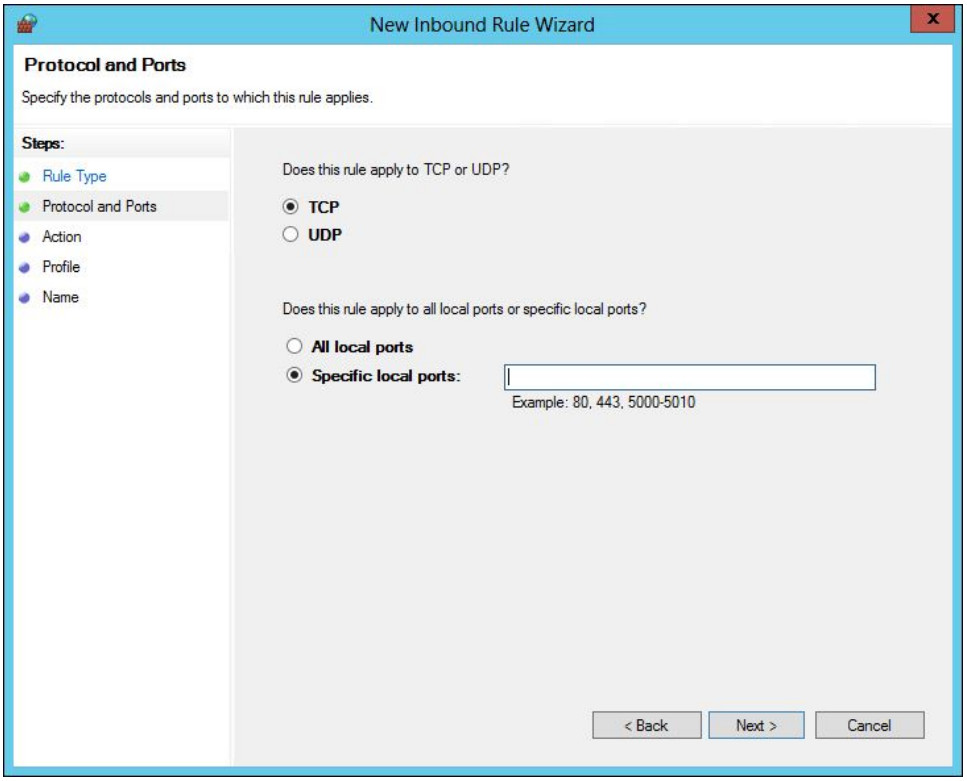


Figure A-9. Rule Protocol and Ports Screen Example

12. Click **Next.**

13. Select one of the connection actions:
    Allow the connection
    Allow the connection if it is secure
    Block the connection

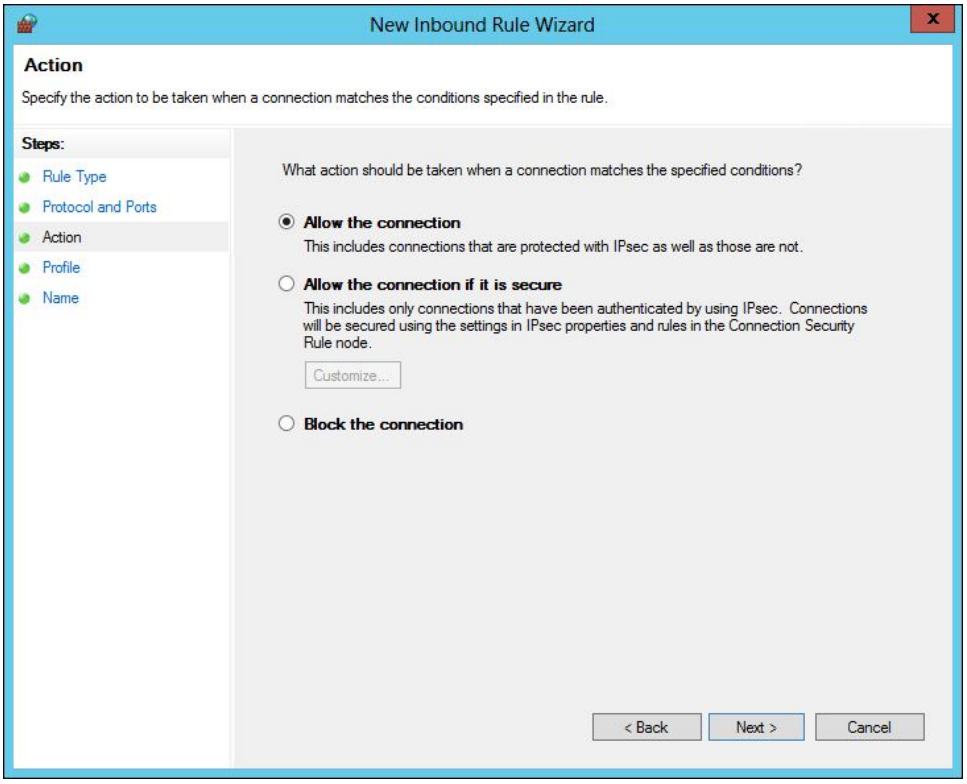


Figure A-10. Rule Connection Action Screen Example

14. Click **Next.**

15. Selet one or any combination of the connection profiles:
    Domain
    Private Network
    Public Network.

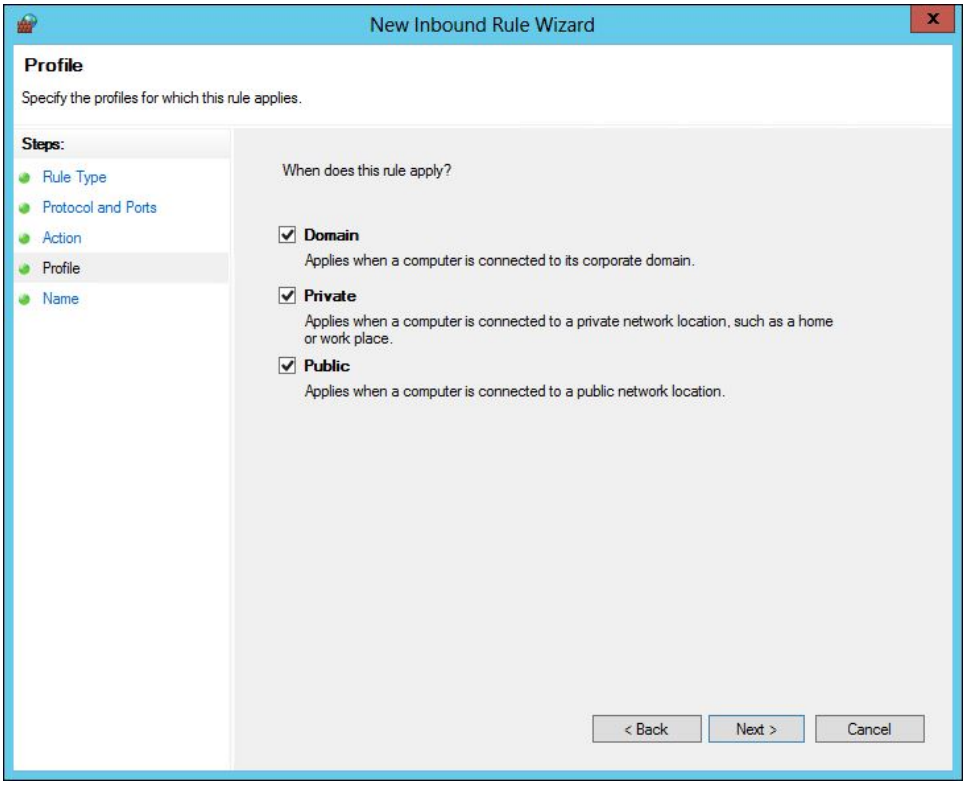


Figure A-11. Rule Profile Screen Example

16. Click **Next.**

17. Specify the **Name** for the rule.
18. Optional: Specify a **Description** for the rule, if desired.
19. Click **Finish.**

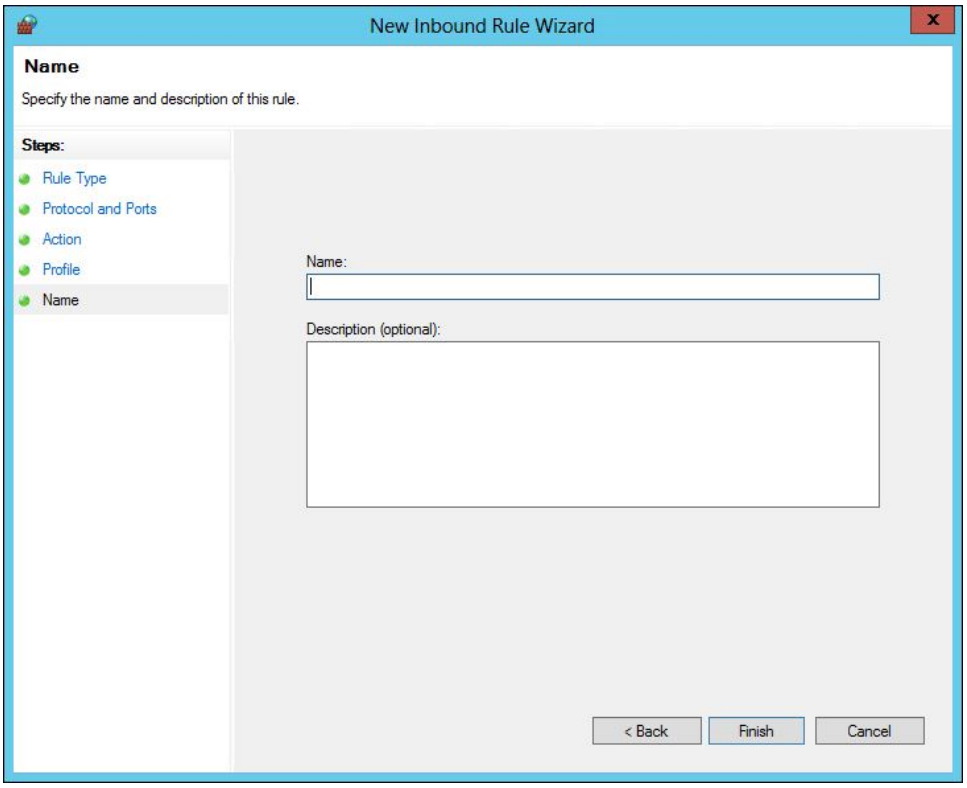


Figure A-12. Rule Name Screen Example

It is recommended that you set up these rules, at a minimum:

Table A-1. Inbound Rules

NAME	PORT NUMBER	PROTOCOL
HTTP	80	TCP
Telnet	23	TCP
SNMP Agent	161	UDP
SNMP Trap	162	UDP
SLNet Remoting	8004	TCP
SLNet Web Services	9004	TCP

BLANK PAGE

Appendix B. EQUIPMENT REDUNDANCY

Hub Redundancy is controlled by the bandwidth manager but can be configured via NetVue. It can be imported from the bandwidth manager during a re-build or manually configured. In order to properly configure hub redundancy, the follow steps need to be taken:

1. Enable Device Redundancy.
2. Manually create an HTO backup element.
3. Perform a Force Registration on the devices that are being used for Hub Redundancy.
4. Verify devices are in the Network container.
5. Create Redundancy Groups.
6. Add power strip.
7. Add devices.
8. Enable Heartbeat on devices.

Make sure Device Redundancy is enabled. Go to the **Service Group->Configuration View** and highlight the desired bandwidth manager. Click on the Vipersat Details button and select the Redundancy view to see the Device Redundancy field.

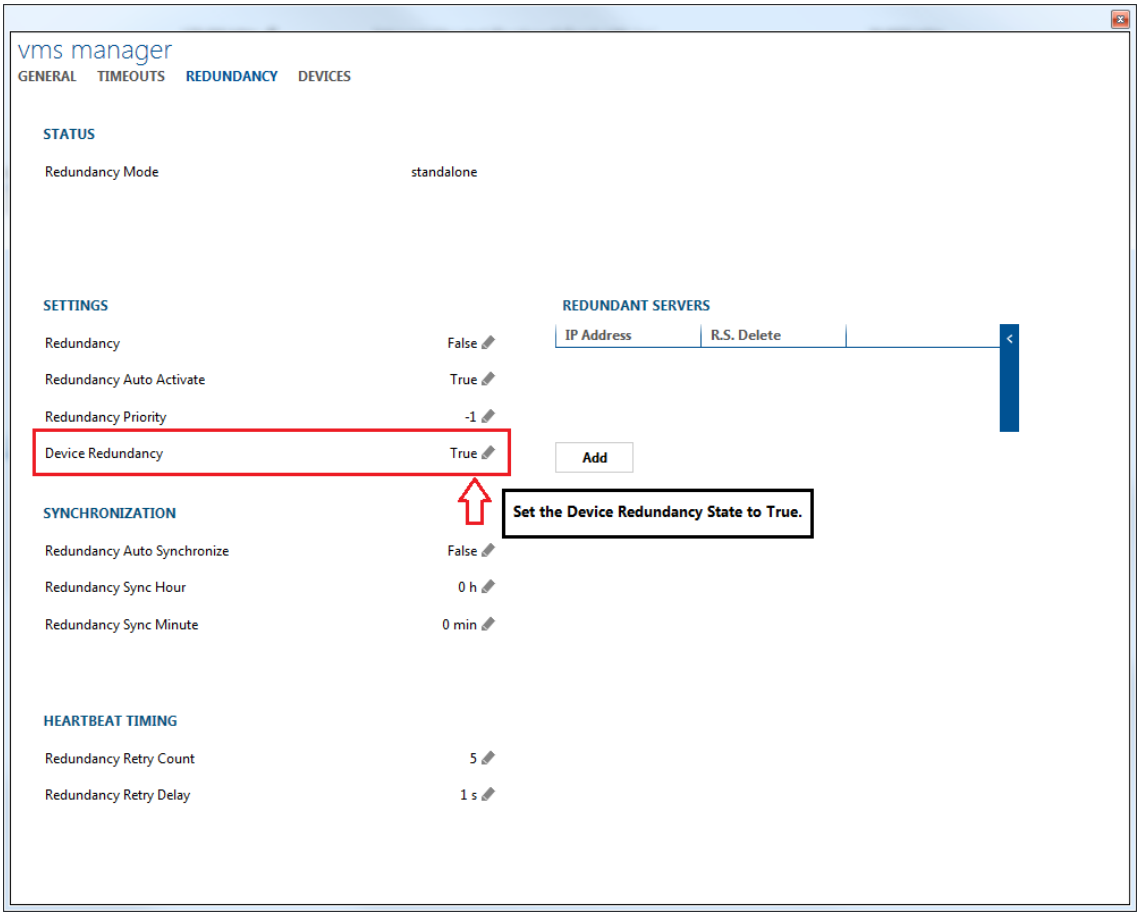


Figure B-1. Enabling Device Redundancy

When configuring the HTO/CTOG hub redundancy, the backup device element needs to be manually created. To create the element, right-click on the Network container that contains the primary device and select **New->Element**. Name Fill in the information for the new element and select the proper protocol.

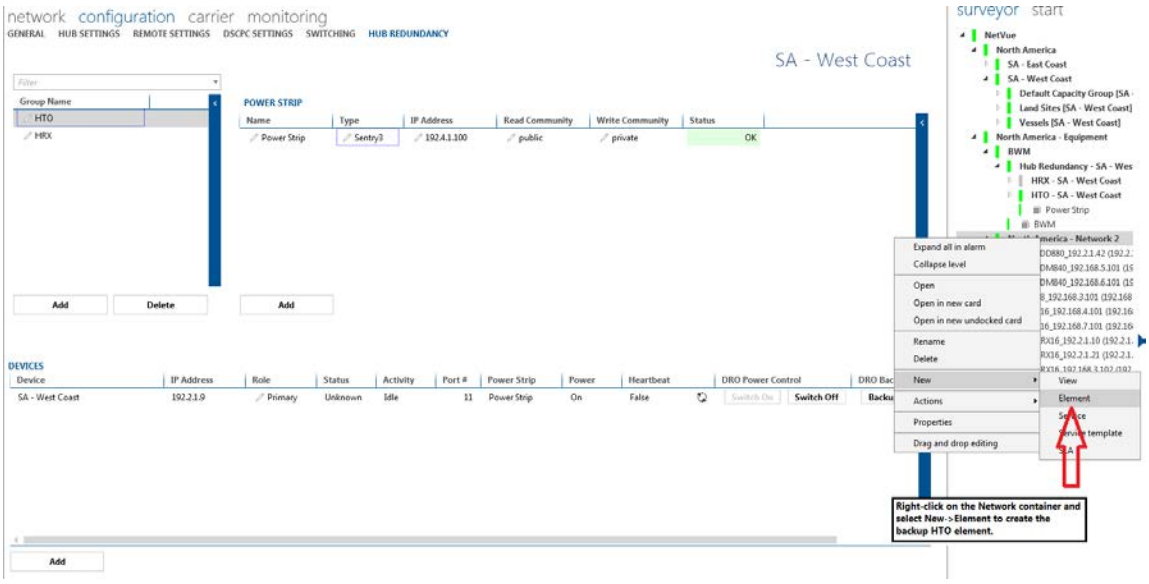


Figure B-2. Backup HTO Element

To ensure that the devices are properly registered with the VMS, go to the Devices view of the Bandwidth Manager and select each device and click on the “Force Registration” button. If the devices aren’t properly registered, then NetVue will fail to add the device to the power strip port.

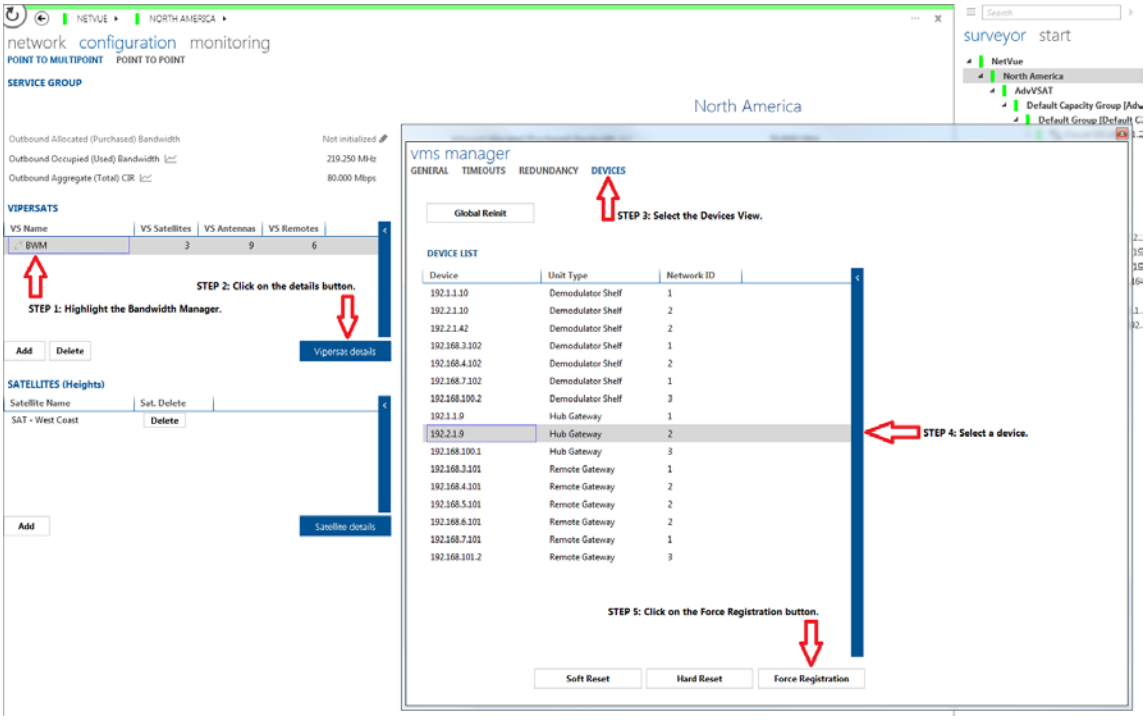


Figure B-3. Force Registration for Hub Redundancy

Verify that the devices that are to be used in hub redundancy are present in the Network container.

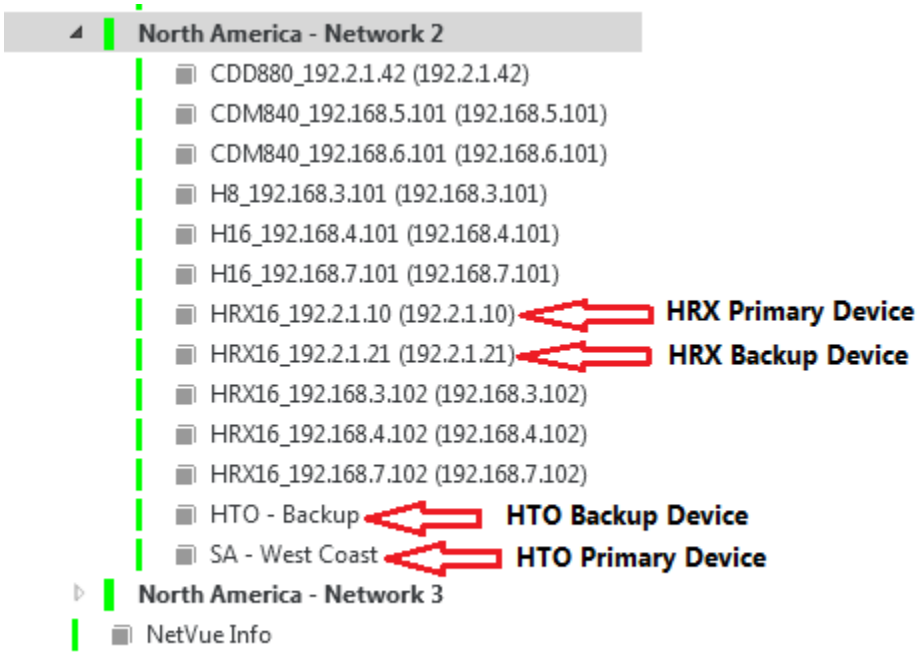


Figure B-4. Verify Devices

Go to the **Service Area->Configuration->Hub Redundancy View** and perform the following steps:

1. Add a group for each device type (Modulator/Demodulator).
2. Add a power strip.
3. Select a group and add devices to the group.
4. Enable the heartbeat for each device.
5. Backup the device configurations.

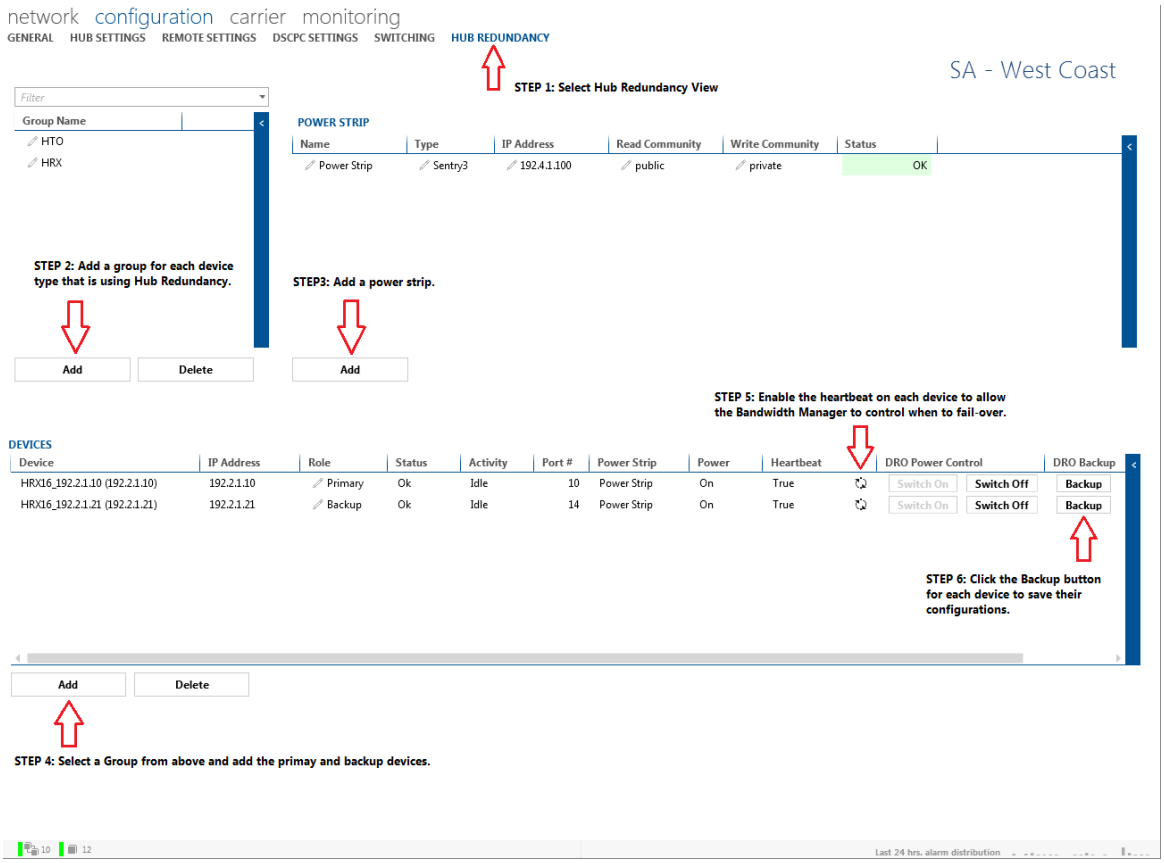


Figure B-5. Configure Hub Redundancy

In the Surveyor, under the Bandwidth Manager container, a Hub Redundancy container is created which contains all of the hub redundancy groups and devices.

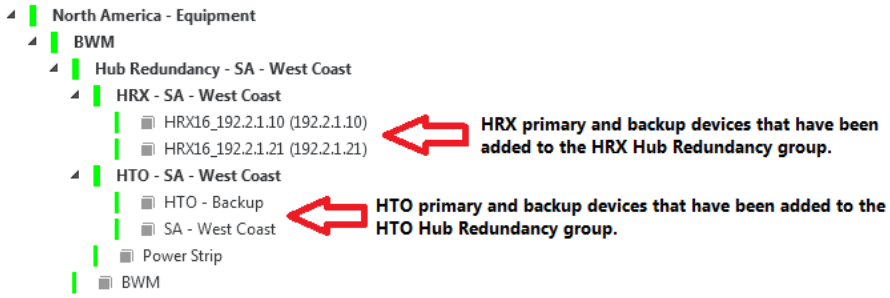


Figure B-6. Hub Equipment Assigned to Hub Redundancy

In the event that a fail-over does occur, the failed unit is deactivated and removed from hub redundancy configuration. When the and the failed unit is ready to be added back to the Hub Redundancy configuration, it first needs to be re-registered with the Bandwidth Manager before it is assigned to a power strip port (See Figure B-3).

Appendix C. NETVUE AND BANDWIDTH MANAGER REDUNDANCY

C.1 Server Redundancy Requirement

The Hub Network Topology requires two separate LAN segments to support DUO Server redundancy. One segment is the Hub modem's acquisition LAN. The other segment is a corporate management LAN for NetVue clients' M&C.

C.2 Server Description

DUO servers have two Network Interface Cards (NIC).

Typically, for standard NetVue redundancy purposes, at least one NIC must be used. The heartbeat management packets communicate from this NIC.

In the DUO configuration, a VMS Bandwidth Manager service runs independently as well, in the same physical DUO servers as the NetVue services. Additionally, NetVue uses a third IP address to control which server is active. The clients always point to this third, virtual IP. This works because the DUO redundant system alternates the virtual/failover Corporate IP from the online to offline server by adding a secondary/alternate IP to the server's NIC.

In NetVue version 2.1 and VMS 3.13.1, the VMS bandwidth manager redundancy does not operate with multiple IPs for the same NIC. Subsequent versions are expected to allow the full DUO failover redundancy to be configured with one NIC per server.

At this time, VMS Redundancy configurations must be set up using VMS. See the VMS user manual for information about how to configure VMS Redundancy.

C.3 NetVue Setup

To configure the DUO server redundancy:

1. Open NetVue client interface.
2. Go to the **Surveyor Tree**.
3. Go to **Start > APPS > Modules > System Center**.

   The **System Center** opens in a new card.

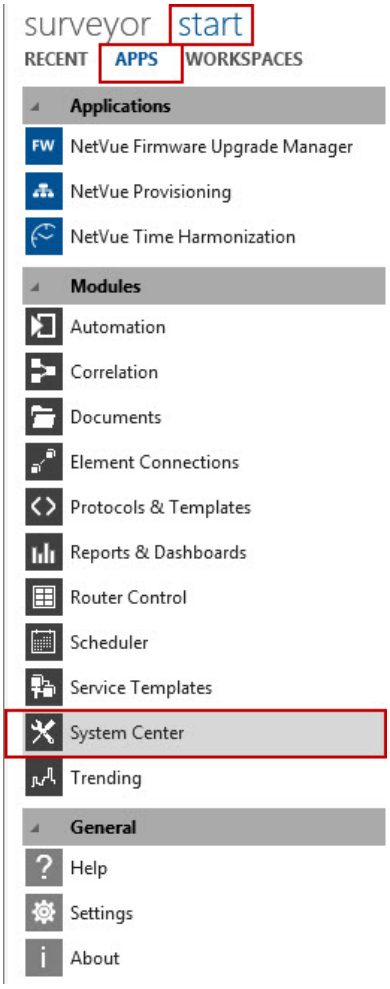


Figure C-1. Surveyor Tree

4. Select **Agents**.
5. Select the **Manage** tab.
6. Select the active, running server.
7. Click the **Failover…** button.

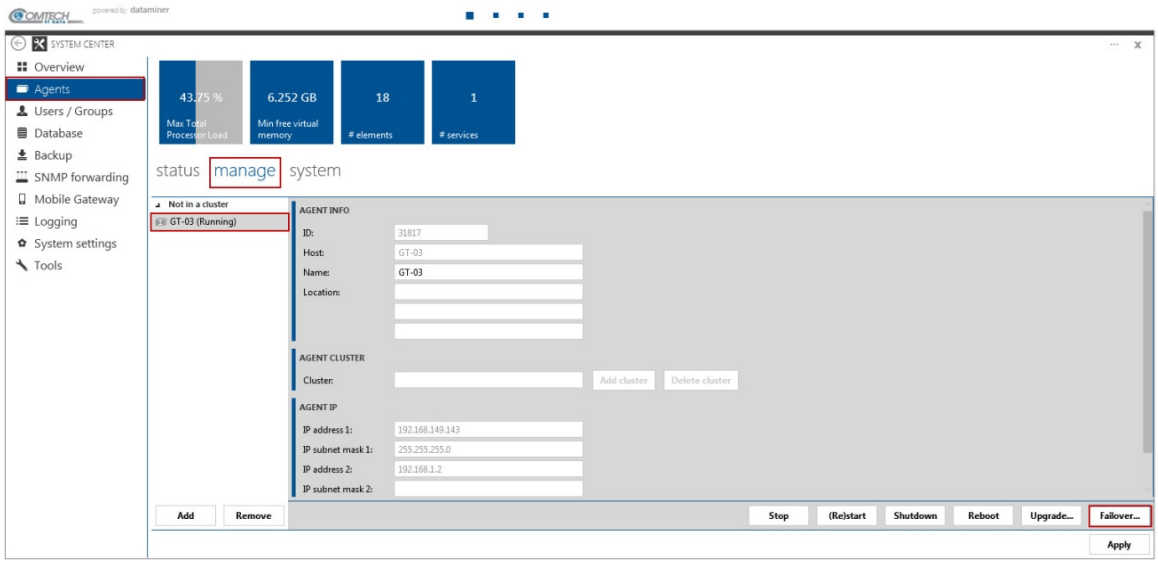


Figure C-2. System Center – Agents

8. On the Failover screen, configure the IP addresses:
   a. Only **Corporate** virtual IP is required.
   This IP is used to connect any NetVue client.
   b. Do not change the **Acquisition** virtual IP. It must be x.x.x.x, as default.

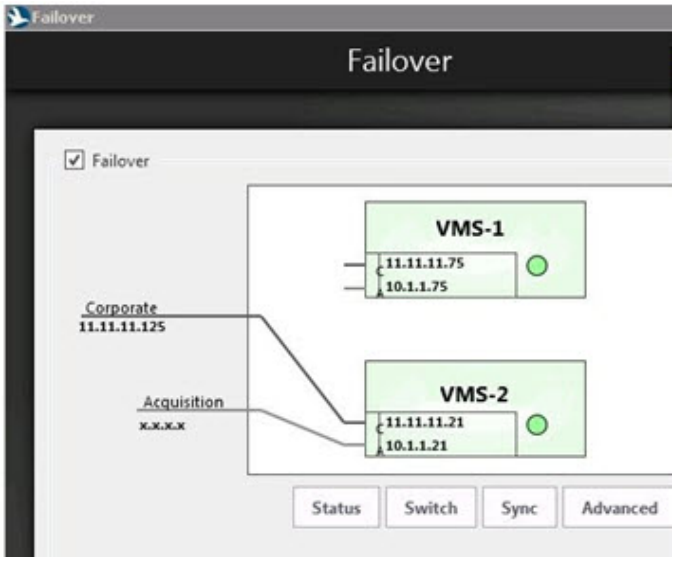


Figure C-3. Failover Configuration

9. Click the **Advanced** button to open a new window. Make sure the **Type** is **Automatic.**

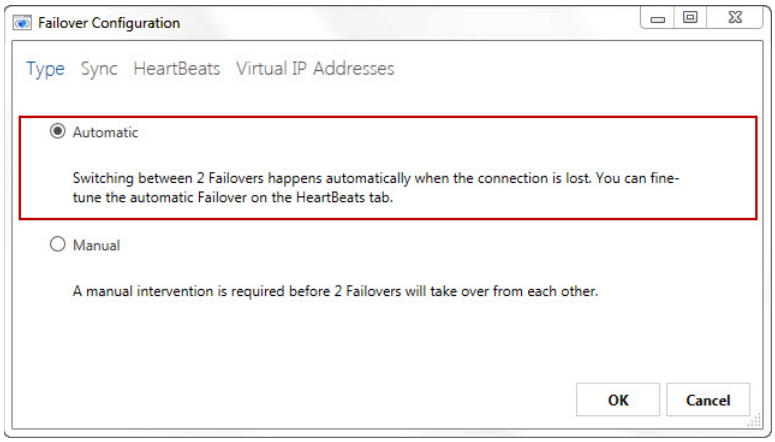


Figure C-4. Failover Configuration – Type

10. Select the **Sync** tab. Make sure it shows **Corporate** as the interface.

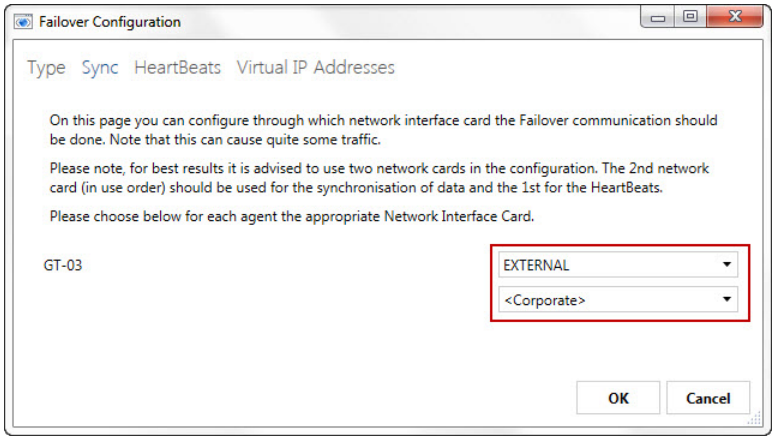


Figure C-5. Failover Configurations - Sync

11. Select the **HeartBeats** tab. Make sure it matches **Corporate** interface.

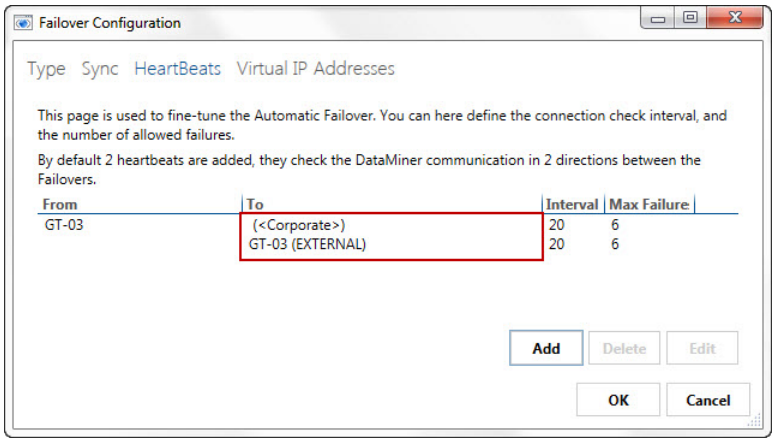


Figure C-6. Failover Configuration - Heartbeats

12. Click **OK**.
    The **Failover** settings are configured.
13. Click **Status** to see the details for the redundancy connection.

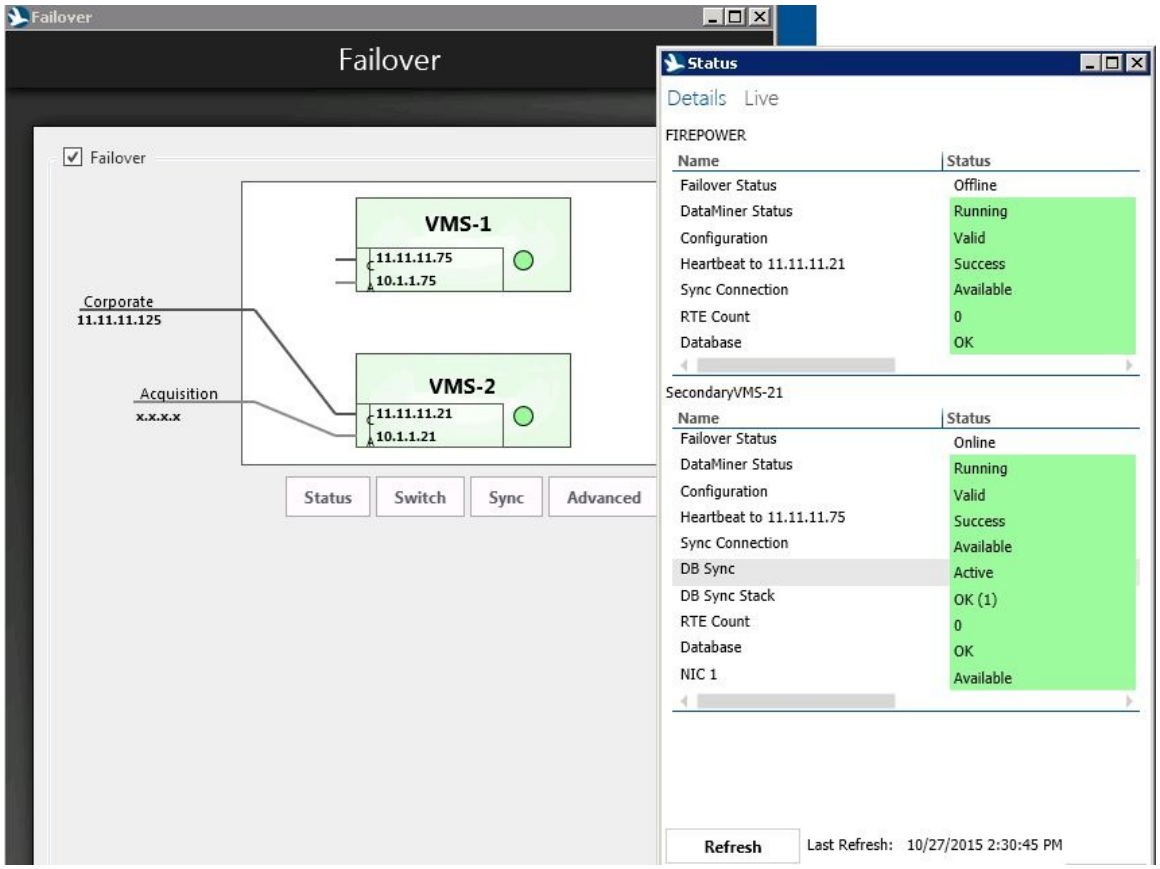


Figure C-7. Failover Status

Physical NICs on the server must match. The Virtual Corporate IP is active immediately for the corresponding server. See Figure C-8 for an example:

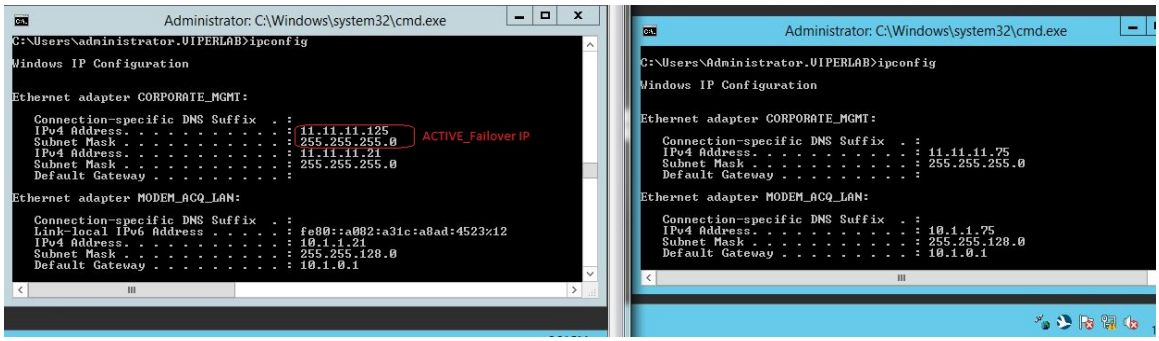


Figure C-8. Network Interface IP Configuration

C.4 Recover VMS Failover

With VMS 1:N server redundancy, the physical IP address of each server's interface card is never changed. When a failover switch occurs, the standby server changes its status from deactivated to Active.

The newly activated server sends a multicast announcement. It registers all modems in the network, and continues to service dSCPC switch requests as necessary.

A problem occurs with the NetVue database configuration, because the original, active VMS IP was linked to the Service Area(s) of any CTOG/HTO registered in that VMS. In NetVue, this setting is a static value. However, you can change it on the fly manually, without a service restart.

Figure C-9 shows the configuration setting that binds the VMS IP address with the Service Area.

To add a new Service Area:

1. Click the **Add** button.
2. Select the **Vipersat** bandwidth manager from the drop-down menu, listed by name.
3. Select the **Satellite**.
4. Select the **IP address**.
5. Click **Enter**.

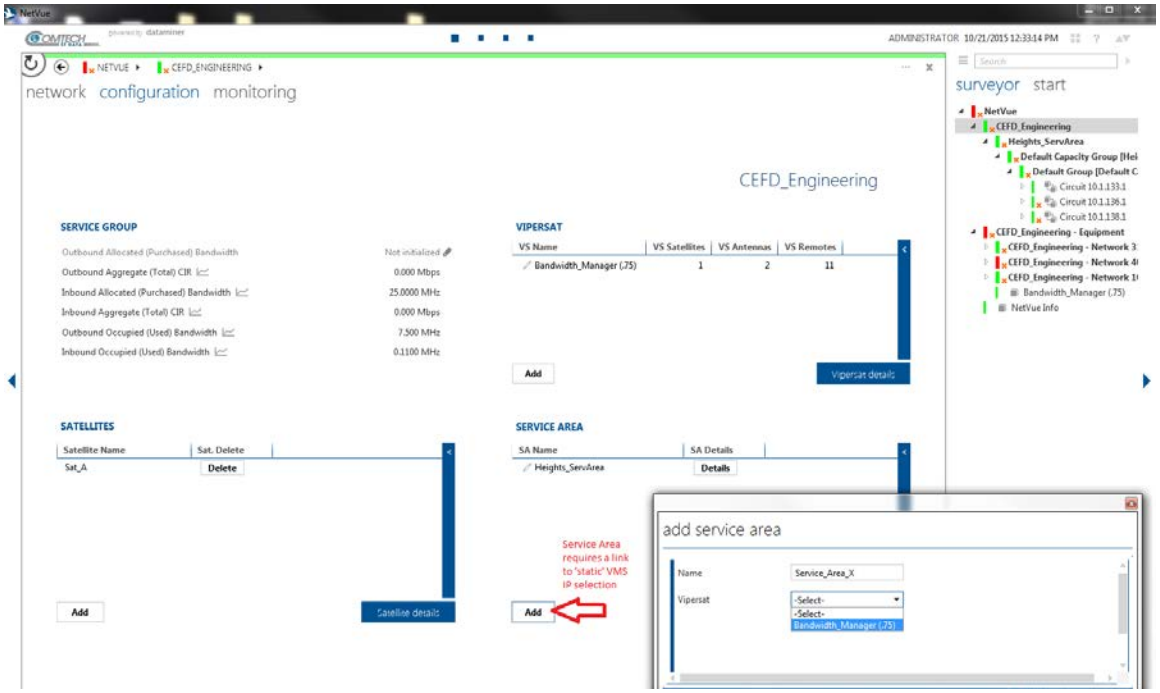


Figure C-9. VMS Selection

After the new service area is created, there is no place in the graphic interface to change the linkage. However, you can edit the bandwidth manager VMS IP so that the pointer remains associated to that same element. This is an advantage if there are multiple service areas routed to the same VMS. Edit the VMS container IP, then all associated elements remain updated.

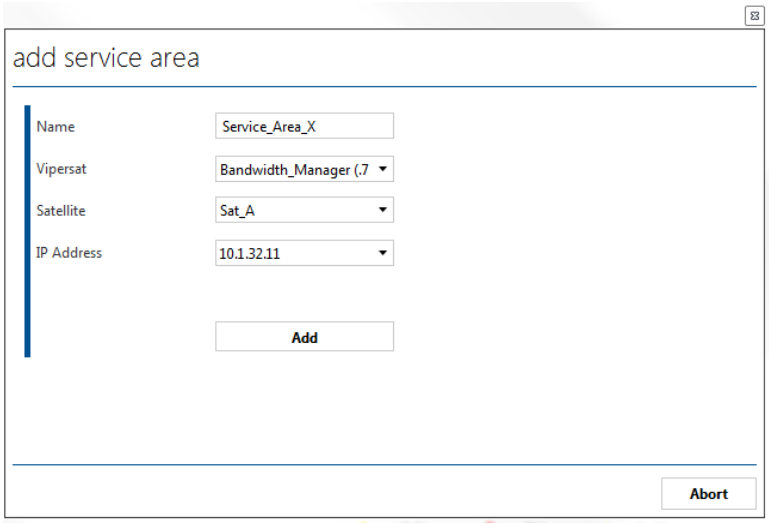


Figure C-10. Service Area Configuration

The consequences of a VMS failure and redundancy failover are not as critical. The VMS redundancy system works independently to the NetVue management system. Therefore, during a failover, remote site modems are controlled by the new active server. This keeps customer traffic and network operation running normally.

When you manually update the VMS IP address, you mitigate these potential problems:

- Out of sync real time reports displayed on the NetVue for that service area
- Future network control changes, such as new site additions and database modifications to the dSCPC engine

C.4.1 Manual Update for the VMS IP Address

To update the VMS IP address after any VMS server redundancy failover:

1. Find out if a VMS redundancy failover has occurred.
2. If a VMS redundancy failover has occurred, go to the VMS element in the NetVue Surveyor tree:

   NetVue > Equipment > VMS_BW_manager
3. Right click the VMS element.
4. Click **Edit**.

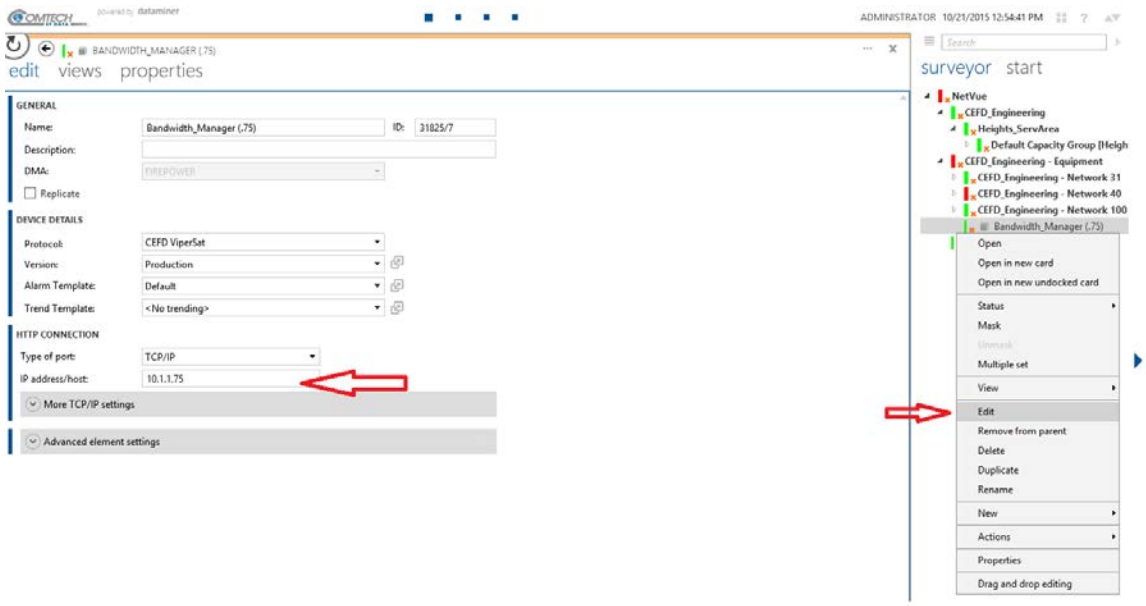


Figure C-11. Element Configuration

5. On the **edit views properties** window, find the **HTTP CONNECTION** submenu.
6. In the **IP address/host** parameter, enter the active **VMS IP** address.
7. Click **Apply**.
8. As recommended, restart the element:
   a. Right click the VMS element from the tree view.
   b. Under the **Status** option, select **Restart**.

This command re-enables polling to the VMS server.

Restarting or Activating the VMS element in the tree, does NOT restart VMS service. It activates any changes made to the NetVue polling status.

Make sure that all sites within the Service Area(s) are reinitialized.

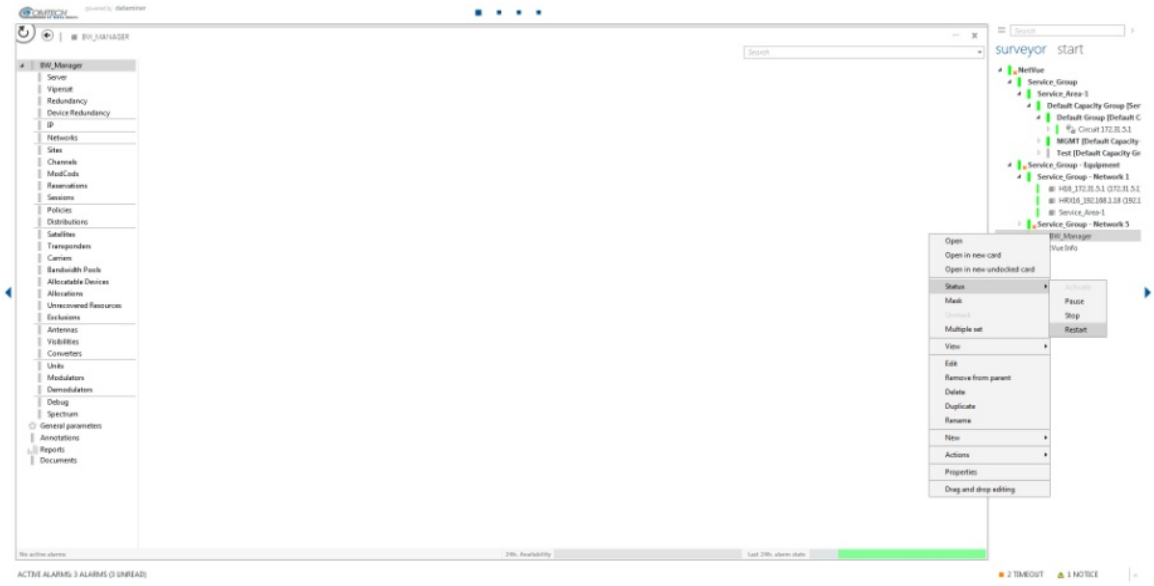


Figure C-12. Restart Polling

C.4.2 Future Automation

In a future releae, NetVue is expected to have an automated version of the VMS redundancy failover process that needs no human intervention. It will check the state of all VMS servers and make a dynamic assignment of the IP from the pool of redundant VMS peers.

Appendix D. NETVUE BACKUP AND RESTORE

D.1 Create a Backup of NetVue IMS

This appendix describes the steps necessary to create a backup of the NetVue IMS. These topics are described:

- Backing up NetVue IMS using the Taskbar Utility
- Backing up NetVue IMS in Cube

D.1.1 Back Up NetVue IMS using the Taskbar Utility

By default, backup filters are put in `C:\Skyline DataMiner Backups\`. If another backup folder is to be specified, right-click the **DataMiner Taskbar Utility** icon, click **Options**, and specify a different folder in the **General** tab.

To create a backup of NetVue IMS using the Taskbar Utility, do these steps:

1. In the Windows task bar, right-click the **DataMiner Taskbar Utility** icon and click **Backup/Restore** > **Backup**.

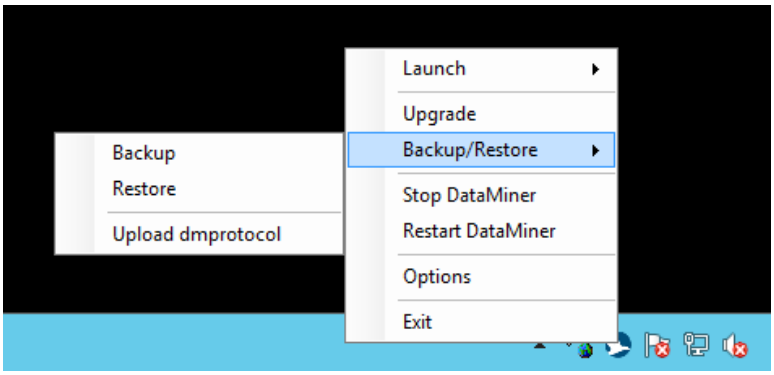


Figure D-1. DataMiner Taskbar Utility

2. If the backup must include the local database of the NetVue IMS, select **Include Database**.

3. In the **Backup** dialog box, select the type of backup you want to create.

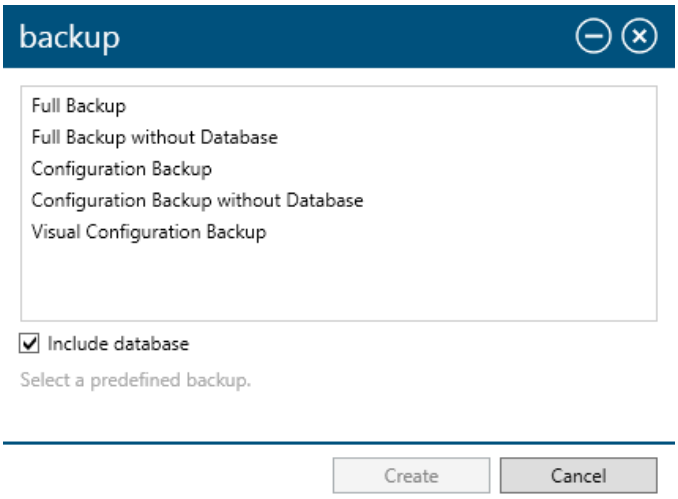


Figure D-2. Backup Dialog Box

If you select ...	Then the backup will include ...
Full backup	All data necessary to restore the entire NetVue IMS
Configuration backup	All data necessary to restore the configuration of the NetVue IMS. NOTE: Does not include NetVue Files and Logging
Element backup	All data necessary to restore one or more elements. Includes element data and element protocol. Use for test purposes only.
Element migration backup	All data necessary to migrate one or more elements or services from one NetVure IMS to another. Includes configuration files, scripts Visio drawings, user filters, views, etc.

4. If you selected **Element backup**, the **Element Backup** dialog box opens:
    a. Select the elements to be included in the backup.
    b. Select whether or not to include the alarms and the trending information associated with those selected elements.
5. If you selected **Element migration backup** , the **Element Migration Backup** dialog box opens:
    a. Select the elements and the services to be included in the backup.
6. If necessary, click **Options** to change a number of backup options.
7. Click **Create**.

D.1.2 Back Up NetVue IMS in Cube

In the System Center app, you can do these tasks:

- Configure automatic backups to run at regular intervals
- Run an immediate backup when necessary

D.1.2.1 Configure the NetVue Backups

To configure the backups for NetVue IMS, do these steps:

1. Go to **Start** > **Apps** > **System Center** > **Backup**.

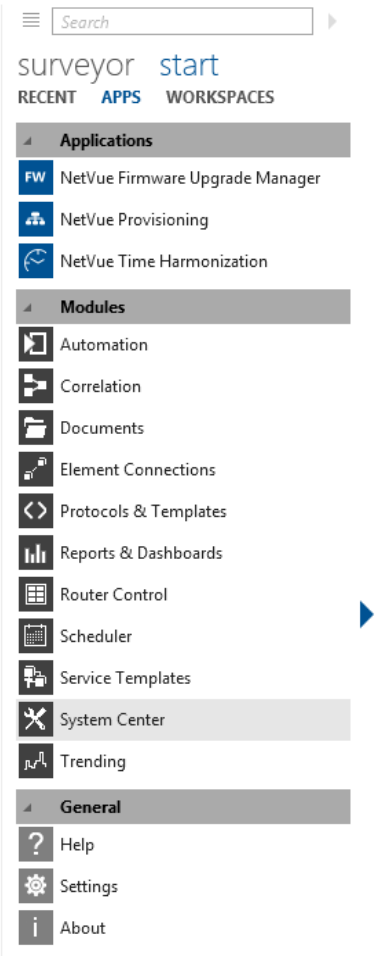


Figure D-3. NetVue Apps to Access System Center

2. In the **General** tab, under **Location**, select and configure a path to where the backups are stored. Set up a local path or a network path.
   For a network path, you can use one network path for all NetVue IMS in the system, or a different network path for each NetVue IMS in the system.
3. In the **General** tab, under **Policy**, enter the number of backups to keep.

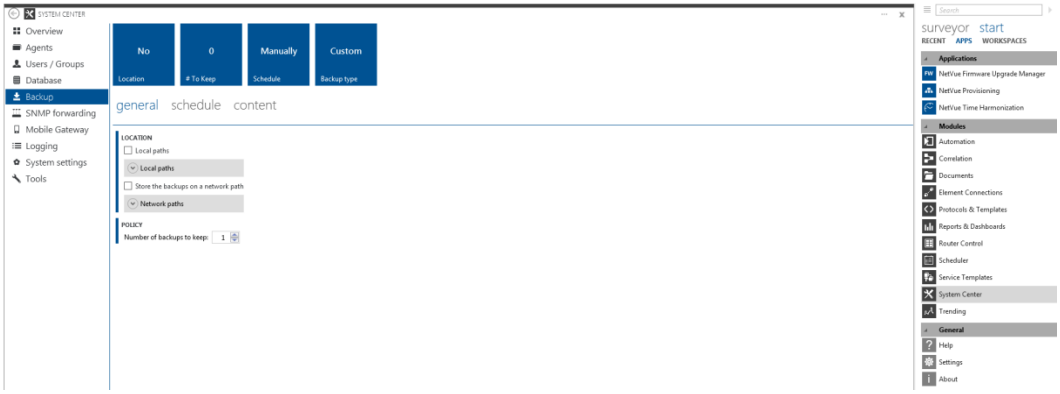


Figure D-4. Create a Backup in the NetVue Cube

4. In the **Schedule** tab, select when the backup must occur: **Monthly**, **Weekly**, **Daily** or only when **Manually** initiated.

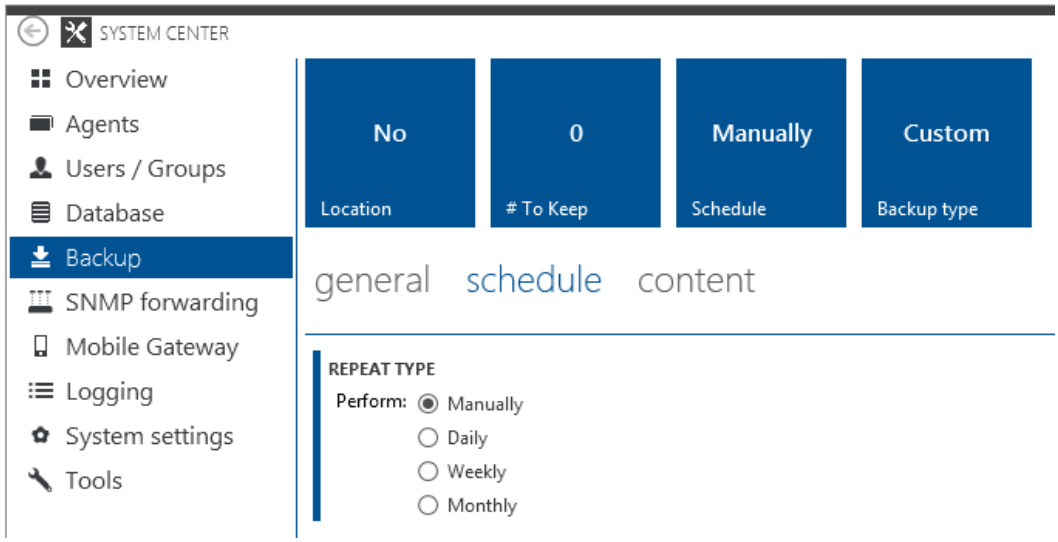


Figure D-5. Schedule a NetVue Backup

5. In the **Content** tab, select the backup type:
   - For **Use predefined backup**, select the type of backup in the drop-down list.
   - For **Use custom backup**, select what must be included in the backup.

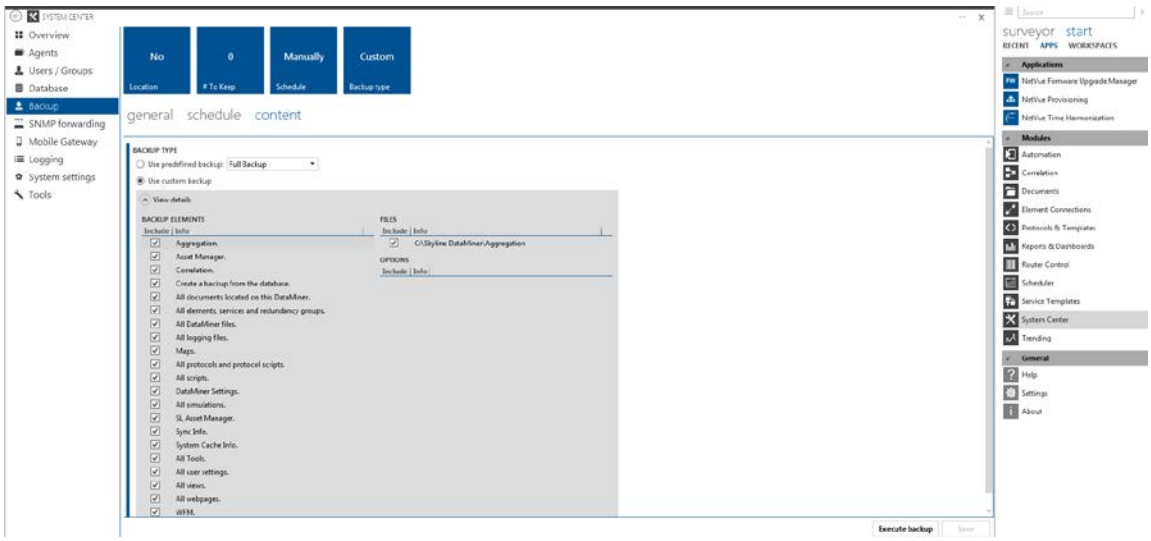


Figure D-6. Select NetVue Content to Back Up

If you use a local Microsoft MySQL Server database, an extra option is available in the Options section. You can use this option to back up the transaction log as well. This allows Microsoft MySQL Server to shrink the log file.

6. Click the **Save** button to save the settings.

D.1.2.2 Instant Backup

To start an immediate backup of NetVue IMS:

1. Go to **Start** > **Apps** > **System Center** > **Backup**.
2. Make sure the backup configuration is correct. If necessary, and change it.
3. Click the **Execute backup** button.
4. Select one or more of the NetVue IMS to backup.
5. Click **Start backup**.

D.2 Restore a NetVue IMS

This section describes the steps necessary to restore a NetVue IMS from a backup that was caused manually, or caused by a scheduled interval at an earlier time.

D.2.1 Restore a NetVue IMS using the Taskbar Utility

To restore a NetVue IMS from the Taskbar Utility:

1. In the Windows task bar, right-click the **DataMiner Taskbar Utility** icon.
2. Click **Backup/Restore** > **Restore**.

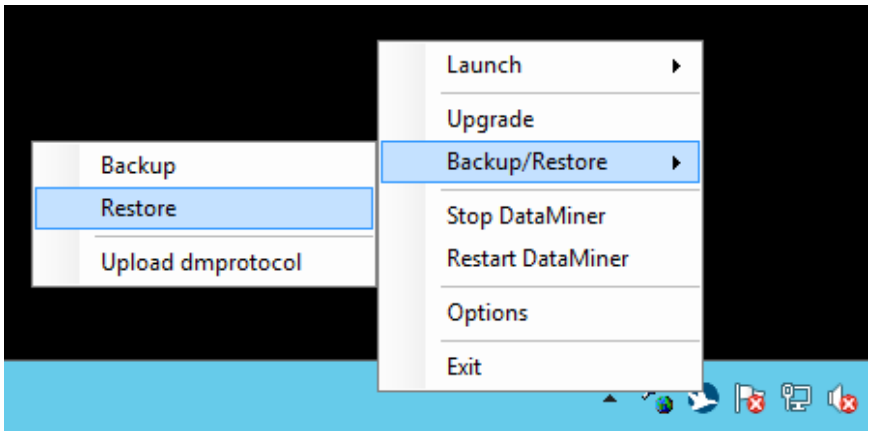


Figure D-7. Select Restore from the Taskbar Utility

3. In the **Restore** window, click the **…** button to select a backup package. A description of the contents in the package shows under **Description**.

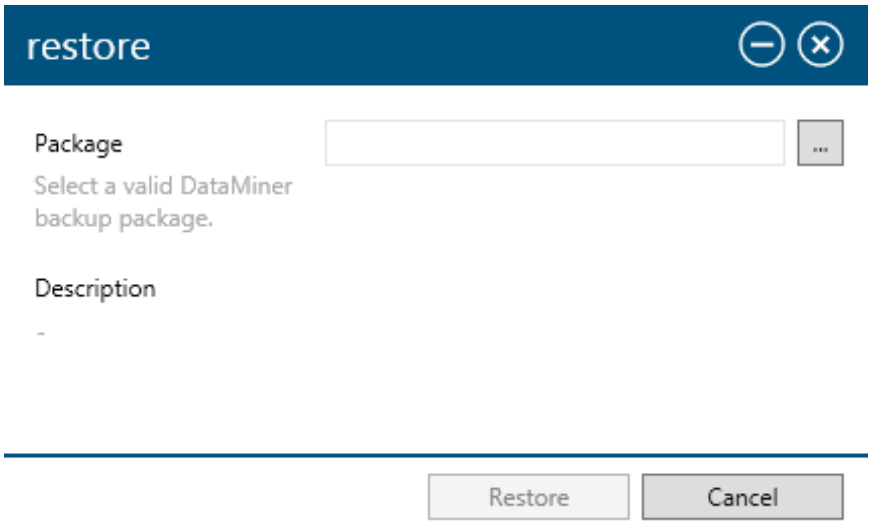


Figure D-8. Restore Dialog Box

4. Click **Restore** to start restoring the NetVue IMS.
   The restore window shows the different steps of the restoration process.

   During the restore process, any open Internet Explorer windows close automatically.

5. When the restoration process is done, click **Finished**.

D.2.2 Restore the Configuration Separately

There are two alternate ways to restore the NetVue configuration:

- Manually
- Using **StandAloneUpgrade.exe**

D.2.2.1 Restore the Configuration Manually

You can restore a NetVue IMS configuration by copying the **C:\Skyline DataMiner** directory from one server to another:

1. Copy the entire **C:\Skyline DataMiner** directory from the original server to the destination server. Make sure that all existing files are overwritten.
2. In the **C:\Skyline DataMiner** directory, delete the **DMS.xml** file.

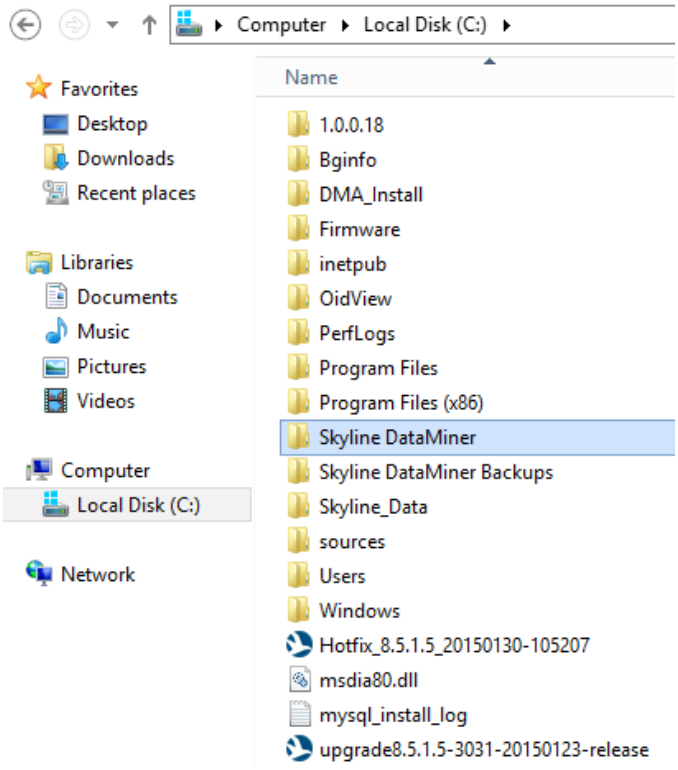


Figure D-9. Locate the C:\Skyline DataMiner\ Folder

D.2.2.2 Restore the Configuration Using StandAloneUpgrade.exe

To restore a NetVue IMS configuration using StandAloneUpgrade.exe:

1. In the **C:\Skyline DataMiner\Tools** directory, double-click **StandAloneUpgrade.exe.**

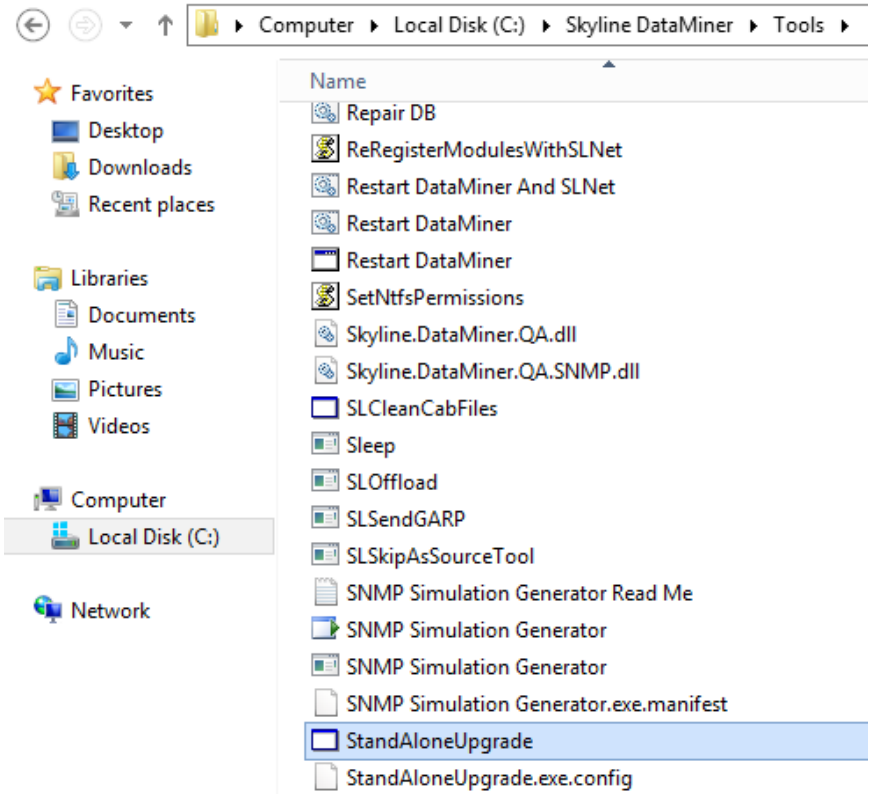


Figure D-10. Locate the StandAloneUpgrade.exe file

2. Click **File** > **Open**.
3. Set **Files of type** to **Zip Files** (*.zip).
4. Select the backup file **DataMinerBackup.zip**.
5. Click **Open**.
6. Wait until the backup file is loaded.
7. Click **Upgrade** > **Start...**
8. In the **Confirm** dialog box, click **Yes**.
9. Wait until you see a **Finished** message.
10. In the **C:\Skyline DataMiner** directory, delete the **DMS.xml** file.

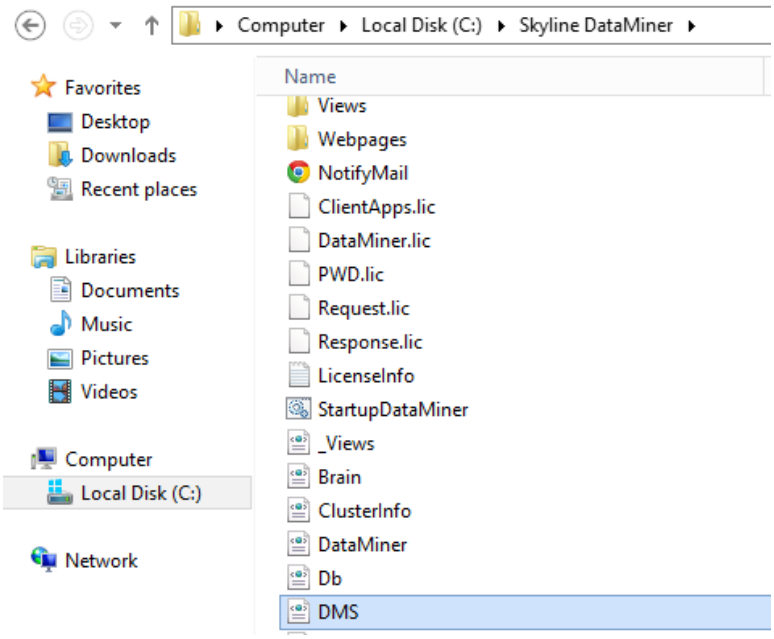


Figure D-11. Locate the DMS.xml file for Deletion

D.3 Start a Restored NetVue IMS Agent in a Cluster

If a NetVue IMS is restored in a cluster environment without using the Taskbar Utility, or if the NetVue Agent in a cluster has been restored to a new, blank NetVue Agent instead of an existing agent, you must start the NetVue Agent and add it to the NetVue IMS as described in this section.

D.3.1 Start the NetVue Agent

To start the NetVue Agent:

1. Shut down the original server, or disconnect it from the network.
2. If necessary, change the IP address and the computer name of the new server. The same IP address and/or computer name that was on the original server can be used. However, this is not required.
3. Connect the new server to the network.
4. Make sure that the **DMS.xml** file has been deleted from the directory **C:\Skyline DataMiner**.
5. Start the NetVue/DataMiner software.

D.3.2 Add the NetVue Agent to the NetVue IMS

When you are using the Cube, do these steps to add the NetVue Agent to the NetVue IMS:

1. Go to **Start** > **Apps** > **System Center** > **Agents.**
2. Click the **Manage** tab.
3. In the bottom-left corner, click **Add**.
4. Enter the IP address of the NetVue Agent and click **Add.**

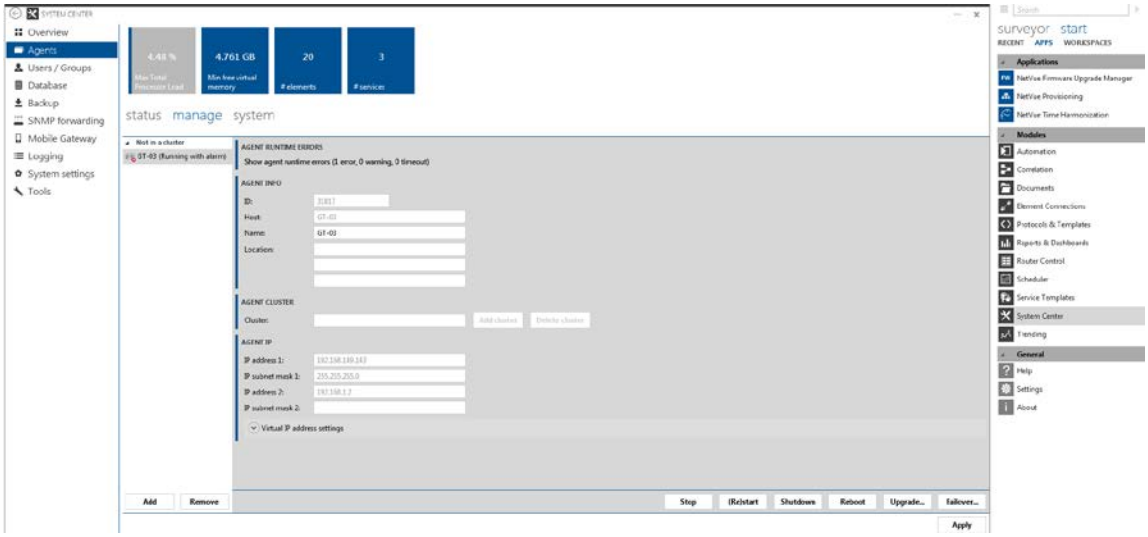


Figure D-12. Add a NetVue Agent to NetVue IMS

After the steps are completed, NetVue begins to synchronize with the other NetVue Agents in the cluster. This is a lengthy process that can take some time. Click on the **Information Events** tab of the Alarm Console to see the status of this process.

Appendix E. CUSTOMIZATION

Contact CEFD Product Support about options for customizing a NetVue system.

E.1 Non-CEFD Element/Device Management

Comtech EF Data supplies the NetVue protocols (drivers) in serial or SNMP formats.

A standard NetVue system includes protocols for these available Comtech EF Data (CEFD) products:

- Modems
- Advanced VSAT platform
- Traffic Optimization devices

The core platform can support some additional non-Comtech devices, such as UPS, routers, switches, antenna controllers, HVAC and security video cameras.

Contact CEFD Sales or Product Management about having custom protocols made for devices that are not included in the standard NetVue product.

E.1.1 Additional Device Management

NetVue also supports:

- SED Decimator, to measure and monitor RF signals
- Moxa Serial Gateway, for devices that have only serial console for management

E.2 Custom Backgrounds [1]

E.2.1 NetVue Background Maps

A map structure of the world and continents is included in the standard NetVue product.

[1] Custom maps, views, reports and dashboards are available. Contact CEFD Product Support about having custom items created.

E.2.2 Rack Elevation Views

NetVue includes standard hub inventory lists. The inventory lists provide a list of the equipment (elements) that are included at a site or given location.

You can create additional rack or computer room views with Visio. Visio views are drawings with active elements. A Visio view can show the status of a device and let you click on the site to see a more detailed view of the device.

E.3 Custom Reports [1]

NetVue includes a set of standard reports. Custom reports are available.

E.4 Dashboards

NetVue gives authorized users Dashboards for access to both real-time and historical NetVue System information. These flexible Dashboards combine critical information and key performance indicators (KPI) from many data sources. Sources include devices, locations, services and SLAs available in the operational environment.

Dashboards give authorized users a detailed view of operations. The intuitive Dashboard web interface is available directly through a web browser. In NetVue applications, the information feeds into the selected Dashboard layout automatically.

E.4.1 Custom Dashboards[1]

The NetVue does not come with pre-configured Dashboards. Operators with applicable security permissions can create Dashboards tailored for specific needs. The complete set of building blocks included in NetVue helps those operators create useful Dashboards.

E.5 Notifications

In the Notifications module, set up NetVue to send notification messages based on these parameters:

- If specific events occur
- To groups of users
- To individual users
- To users on duty, optional

Notifications occur as email messages by default. See Chapter 6 for more information about setting up Notifications.

Appendix F. SERVICE LEVEL AGREEMENT (SLA) (OPTIONAL FEATURE)

F.1 Introduction to SLA

NetVue SLA Monitoring gives operators a business perspective view of their operations. Operators define SLAs to be tracked by NetVue in real time. While NetVue provides device and service information, SLA Monitoring adds the historical performance weighed against the defined objective. This combination yields valuable business impact information. SLA is an optional feature that can be included with your NetVue platform.

A partial list of SLA features includes:

- User-defined alarm thresholds
- Predictive compliance
- Notifications
- Reporting
- Trending

F.2 SLA Interface Overview

The SLA Element has these sections:

Main View – Shows overall compliance information, performance indicators and general information about the SLA.

Outage List – Shows a time-stamped history of all severity changes for the tracked SLA. The administrator can correct the impact of the violation, and define a motivation for the correction percentage.

Active Service Alarms – Shows all active alarms that are currently affecting the SLA.

History – Shows a history of all alarms that affect the SLA.

SLA Configuration – Configure SLA Time Frame, Alarm Settings, SLA tracking, SLA outage history retention period, save and load SLA Configuration settings; reset SLA statistics.

Compliance Configuration – Configure violation time, violation counts,single violation settings, and save and load Compliance Configuration settings.

Violation Configuration – Configure violation filter types, violation filter property name, violation filter value, violation filter impact, violation filter exclusive, violation filter sequence, violation filter state, and save and load Violation Configuration settings..

Ticket Creation – If a third-party ticketing system interfaces with NetVue via the North-Bound Interface, Ticket Creation can generate a trouble ticket with the third-party ticketing system.

Offline Window – Define a daily window of time, during which the service is considered offline. Most alarms raised during this time window do not affect the SLA. Exceptions are those alarms with parameters that have been explicitly set to disregard the offline window settings.

General Parameters – Shows parameters, the SLA element creator, the device state, when an alarm template for the SLA itself was changed and who changed it.

Annotations – HTML based page that can be used to define custom information about the specific SLA itself.

Reports – Alarm distribution, Alarm events, and Alarm States for the SLA itself. This page does not define alarm distributions or events for the Service it is monitoring.

Documentation – A folder that is shared among all SLAs and used to store SLA agreements or other documentation.

F.2.1 Main View

The this section provides an overview of the SLA performance indicators. Figure F-1 shows a general overview of the Main View.

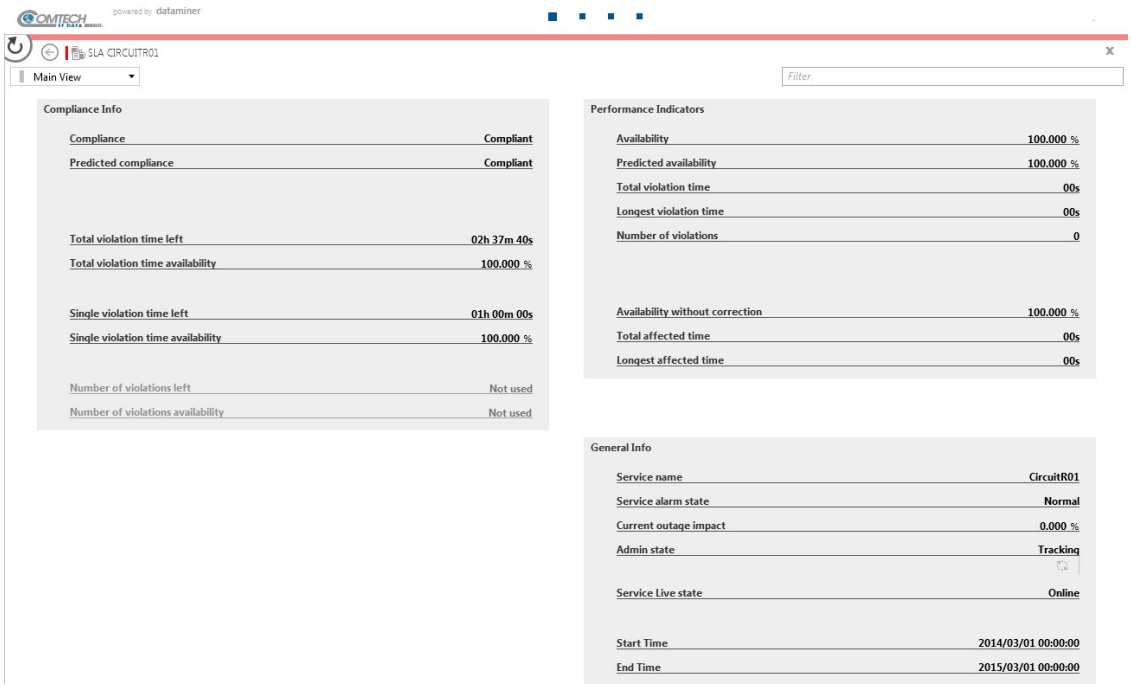


Figure F-1. Main View Overview

F.2.1.1 Compliance Info

Compliance Info shows details about the compliancy status of an SLA, predictions of compliancy based on current and past outages, and detailed violation information. See Figure F-2.

Compliance:

- **Compliant:** The SLA is not and has never been violated.
- **Breached:** The SLA has been violated beyond acceptable limits.
- **Compliant (Degraded):** The SLA has been violated, but not beyond acceptable limits.
- **Compliant (Degrading):** The SLA is being violated now, though not beyond acceptable limits.

Predicted Compliance:

- **Compliant:** The SLA is 100 percent compliant
- **Breached:** The SLA has been violated beyond acceptable limits.
- **Jeopardy:** If the Service keeps failing at the current ratio, then the SLA will be breached by the end of the window.

Detailed information shows the time left and time availability for both total and single violations. Additional detail may show the number of violations left and the number of violations availability.

Figure F-2. Compliance Info

F.2.1.2 Performance Indicators

Performance indicators show (See Figure F-3):

- Availability of the service
- Predicted availability, taking into account current and past outages
- Total duration of all violations, including the longest, that occurred in the time window
- Number of violations that occurred in the time window
- Availability without correction indicates the availability as a percentage taking into account no modifications because of changes made by an Administrator level user.

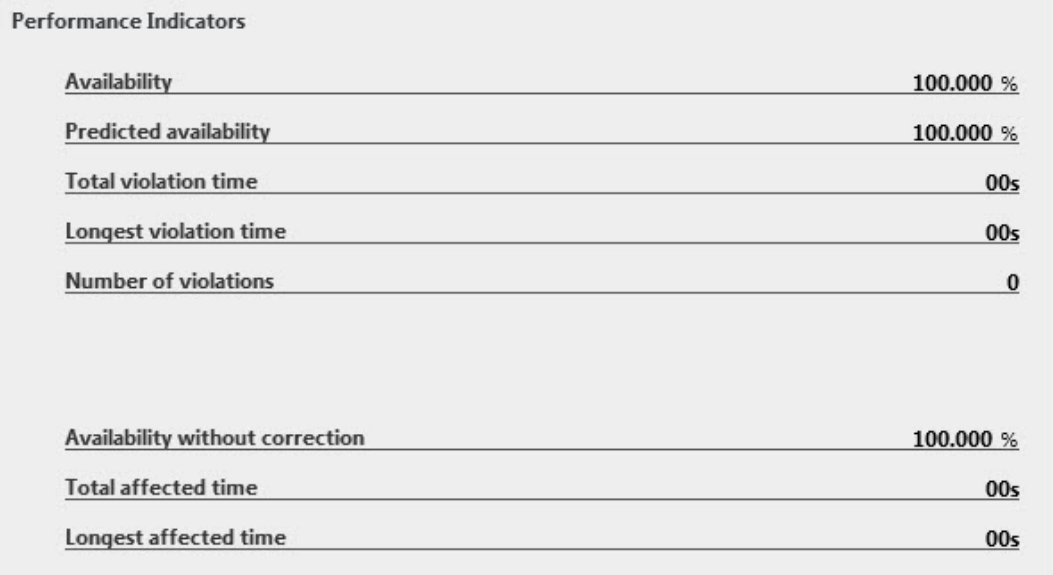


Figure F-3. Performance Indicators

F.2.1.3 General Info

General Info shows data for (See Figure F-4):

- Service Name
- Current Alarm State
- Current Outage Impact
- Tracking or Disabled
- Service Live State
- Start Time of SLA
- End Time of SLA

Figure F-4. General Info

F.2.2 Outage List

The outage list shows a history of all severity changes to the tracked service (See Figure F-5).

- **Admin State** – shows whether the SLA was active when the outage occurred
- **Current Window** – shows whether the outage occurred in the current window
- **Begin and End Timestamp** – shows when the outage occurred and ended
- **Outage** – shows the duration of the outage
- **Violation** – shows the duration of the violation, taking into account the SLA settings (e.g., violation filter settings)
- **Correction and Motivation** – shows a possible correction on the outage and the motivation for the correction
- **Ticket** – shows a ticket number, if linked to third party ticketing system

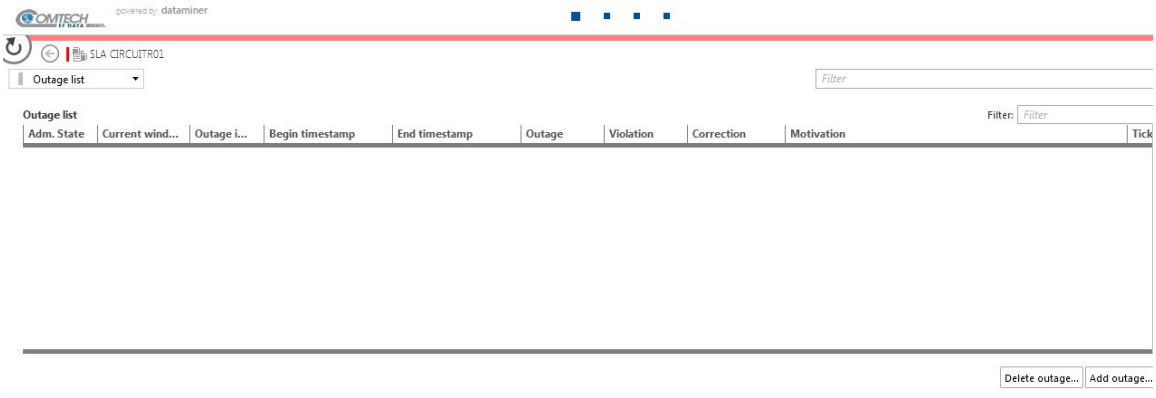


Figure F-5. Outage List

F.2.3 Affecting Alarms

This view shows an overview of the current alarms, with detailed information on each alarm.

Each column in the affecting alarm list is described as:

Current Active Service Alarm ID – shows the Alarm ID associated in NetVue.

Current Active Service Alarm severity – shows the alarm severity.

Current Active Service Alarm Calculated inclusion state – shows the percentage of impact on the SLA for the alarm. The value is calculated using data from the violation filters and the offline window.

Current Active Service Alarm Overruled inclusion state – shows whether the alarm is included in the impact to the SLA.

Current Active Service Alarm time – shows the time when the alarm triggered.

Current Active Service Alarm Element – shows the element affected by the alarm.

Current Active Service Alarm parameter – shows which parameter is generating the alarm.

Current Active Service Alarm Value – shows the value of the alarm parameter

Current Active Service Alarm state – shows the current state of the alarm.

Current Active Service Alarm type – shows whether the service impacted has changed.

Current Active Service Alarm user state – shows if the alarm is assigned to a user.

Current Active Service Alarm source – shows the source generating the alarm.

Current Active Service Alarm category – shows the category of the alarm.

Current Active Service Alarm offline impact – shows whether the alarm also has an impact during the offline window.

By default, no alarms are taken into account during the offline windows. However, this can be overruled at a parameter level.

Figure F-6. Affecting Alarms

F.2.4 History

The history view shows an overview of all alarms that have occurred, including detailed information on compliance, availability and violations.

- **Tracking Period** – shows the time frame window.
- **Start Time & End Time** – shows the start and end times of the time frame window.
- **Compliance History** – shows the compliance of the SLA.
- **Availability & Availability without correction** – As a percentage, shows the availability of the SLA and the availability of the SLA without corrections made.
- **Total Violation Time**
- **Longest Violation Time**
- **Number of violations**

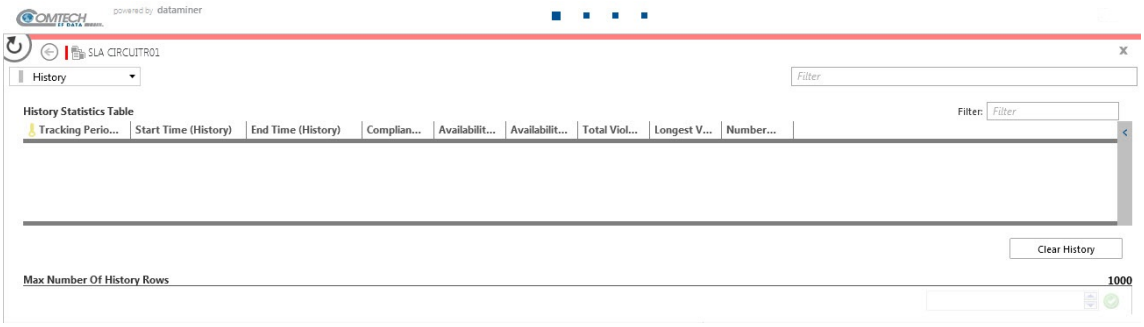


Figure F-7. History Statistics

F.2.5 SLA Configuration Page

Figure F-8 shows a general view of the SLA Configuration view.

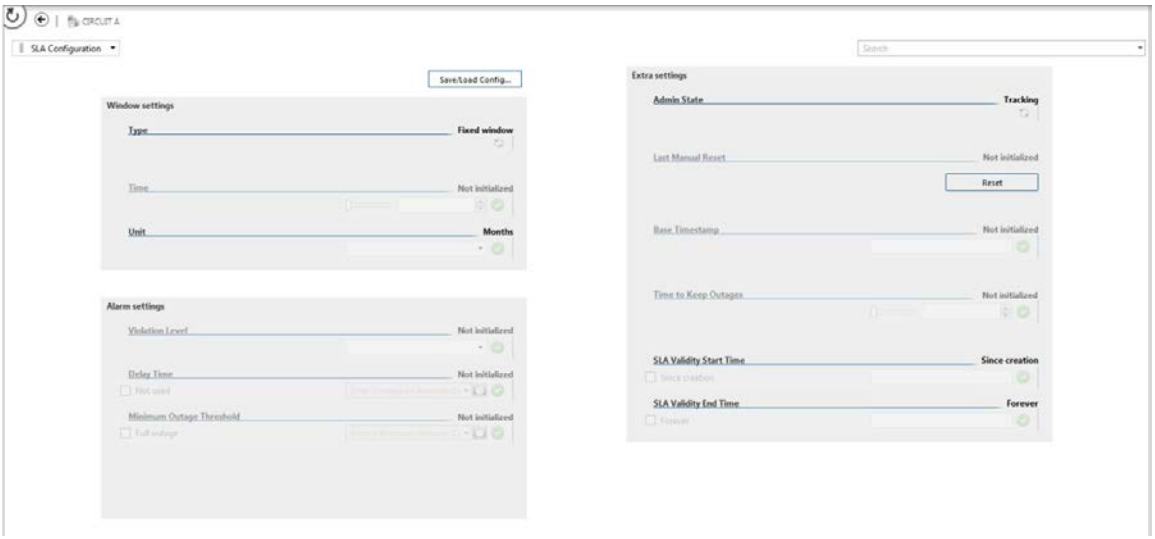


Figure F-8. SLA Configuration Overview

F.2.5.1 Window Settings

Use the Window setting to configure the time window in which the SLA operates. Figure F-9 shows the windows setting view in detail.

Type –

- **Fixed Time Window**: The window starts at a fixed point in time, such as at midnight every day. You can define a fixed window that starts at a specified time, instead of at the beginning of the month. To do this, enter a time value in the format **yyyy/mm/dd hh:mm:ss** under base timestamp in the **Extra** settings.
- **Sliding Time Window**: The window changes with the current time.
    - **Time** – Values: 1 through 100
    - **Unit** – Seconds, Hours, Days, Weeks, Months

Figure F-9. SLA Windows Setting

F.2.5.2 Alarm Settings

Use **Alarm Settings** to define these parameters (See Figure F-10):

- Alarm level the SLA must violate
- Delay before the SLA indicates it has been violated
- Minimum outage threshold for the SLA to trigger

Figure F-10. Alarm Settings

Violation Level – sets the Alarm Level at which the SLA must start to indicate violations

Delay Time – sets a delay period in seconds; after this delay, the SLA starts to indicate violations (e.g., for backup delays)

Minimum Outage Threshold – sets the minimum outage period before the SLA starts to indicate violations

The duration of an alarm includes any delay time in effect. It does not include any minimum outage threshold in effect.

F.2.5.3 Extra Settings

Use the **Extra Settings** to define these parameters (See Figure F-11):

- Activate or deactivate tracking for the SLA
- See the last time the SLA was reset
- Reset the SLA counters
- Set a base timestamp
- Set the length of time to keep outage history

Figure F-11. Extra Settings

Admin State – activate or deactivate tracking for the SLA

Last Manual Reset/Reset – shows the last reset time, and you can use it to reset the SLA counters

Base Timestamp – useful when you need to define a fixed time window that does not start at the beginning of the month

Time to Keep Outages – set the length of time to keep outage history (24 months, maximum)

SLA validity start time – set the start of the time period when the SLA is valid

SLA validity end time – set the end of the time period when the SLA is valid

F.2.6 Compliance Configuration Page

Use the **Compliance Configuration** page to configure these parameters (See Figure F-12):

- Total violation times
- Single violation times
- Violation count

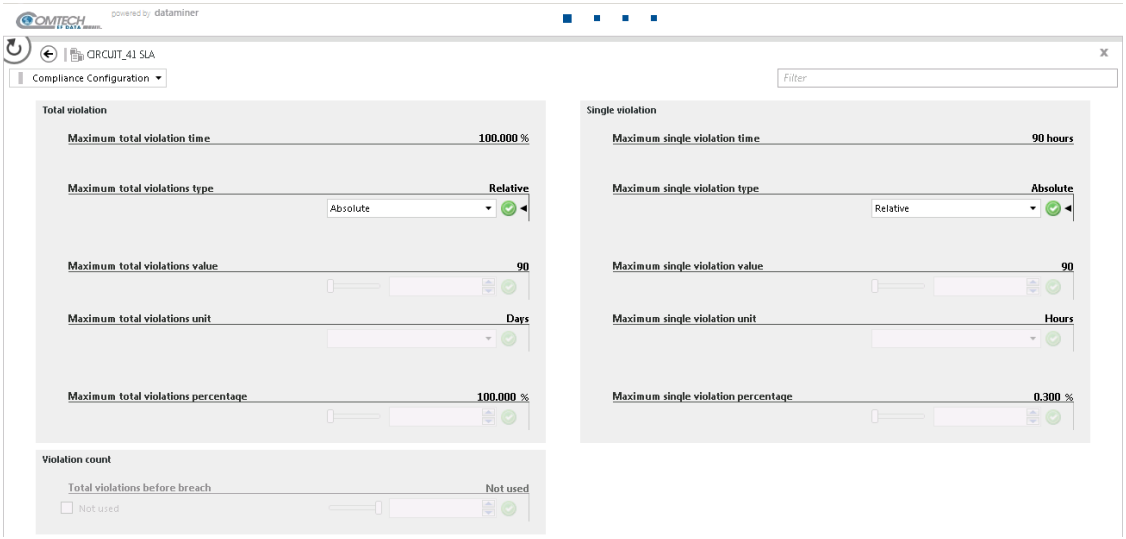


Figure F-12. Compliance Configuration

F.2.6.1 Total Violation

Use the **Total Violation** section to set the maximum violation time for all violations (See Figure F-13). **Total Violation** defines how long the SLA may be violated (during the SLA window) before it is considered breached.

You can configure two types of total violations:

- Absolute (Fixed): e.g., 5 minutes
- Relative: e.g., 0.010 percent of the total window duration

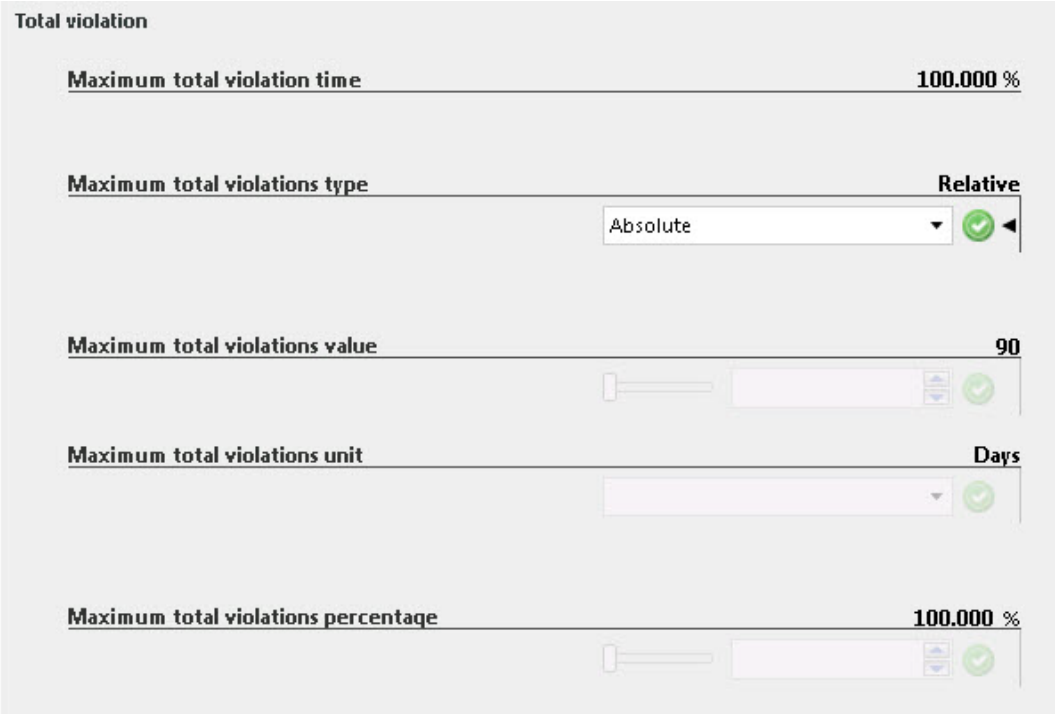


Figure F-13. Total Violation

Maximum violation time – shows the **Maximum violation time** in fixed units or percentage, depending on which violation type is selected

Maximum violations type – select **Absolute** (fixed) or **Relative** (percent of total window size)

Maximum total violation value – set the **Maximum total violation time** in **Maximum total violation units** for the **Absolute** violation type. Valid range is 1 through 90 units

Maximum total violation unit – set the unit of measure for the **Maximum total violation value** (e.g., days).

Maximum total violations percentage – set the **Maximum total violation time** in percent for the **Relative** violation type. Valid range is 0.001 – 100%

F.2.6.2 Violation Count

Violation count specifies how many violations can occur before the SLA is considered breached. Valid range is 1 through 100 (See Figure F-14).

Figure F-14. Violation Count

F.2.6.3 Single Violation

Use **Single violation** to configure the parameters of a single violation SLA breach (See Figure F-15**)**.

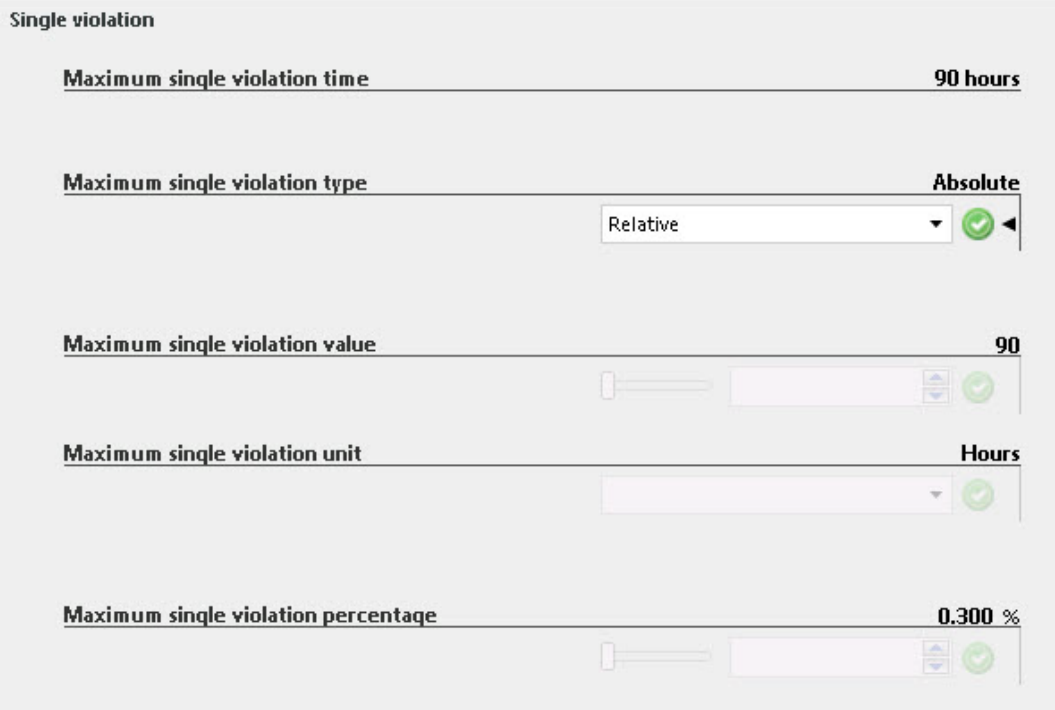


Figure F-15. Single Violation

Maximum single violation time – shows the **Maximum single violation time** in fixed units or percentage, depending on which violation type is selected

Maximum single violation type – select **Absolute** (fixed) or **Relative** (percent of total window size)

Maximum single total violation value – set the **Maximum single total violation time** in **Maximum single total violation units** for the **Absolute** violation type. Valid range is 1 through 90 units

Maximum single total violation unit – set the unit of measure for the **Maximum single total violation value** (e.g., days).

Maximum single total violations percentage – set the **Maximum single total violation time** in percent for the **Relative** violation type. Valid range is 0.001 – 100%

F.2.7 Violation Configuration

Use Violation Configuration to define these parameters (see Figure F-16):

Violation Filter Type – Choose the Violation Filter Type in the drop-down list and confirm. This is the alarm field on which you wish to filter, eg. Severity. The violation filter type Key point and Component info refer to parameter data that can be set in the protocol information template.

Violation Filter Property Name – If the filter type is a custom property define the property name.

Violation Filter Value- Define the value, e.g. if the violation filter type is a Severity, this can be set to critical. It is possible to use an asterisk or question mark as wild cards here.

Violation Filter Impact – Enter the impact you want the violation to have as a percentage under Violation Filter Impact.

Violation Filter Exclusive- Toggle whether the filter should be exclusive or not.

- If set to **Filter**, an alarm that does not match the filter will not be evaluated further and the weight specified in the last matching rule is taken. If it did not match a previous rule, then the weight for that alarm is set to 0%
- If set to **Continue**, the following filters are also processed, and if in the end none of the filters match, the weight ofr that alarm is set to 100%. If seveeal alarms match several of the violation filters set to Continue, the weightings will be added together. If one alarm matches several of the violation filters, the matching filter is applied.

Violation Filter Sequence – Define the sequence number in which you wish different filters to be used. The lowest number will be sequenced first.

Violation Filter State- Enable or disable the Filter Rule.

The table is interpreted by NetVue form top to bottom. It is sorted first on Violation Filter State and then on ascending Violation Filter Sequence.

For your SLA, Warnings should count for only 10% and Minor alarms for 30%. Also, if an element is in maintenance, ht ealarms should not count at all. Any other alarms should count for the full 100%.

To get this result, set these filters:

Type	Property Name	Value	Impact	Exclusive	Sequence	State
Severity	…	Warning	10%	Continue	1	Enabled
Severity	…	Minor	30%	Continue	2	Enabled
Custom Element Property	State	Maintenance	0%	Continue	3	Enabled

Figure F-16 .Violation Configuration Window

F.2.8 Save/Load Configuration Page

Use Save/Load Configuration to define these parameters (See Figure F-17):

- **Configuration Name –** Label used to define each unique Configuration
- **Load Configurations –** Loads all saved configuration
- **Delete –** Deletes a selected configuration
- **Load –** Loads a selected configuration
- **Save –** Saves a selected configuration
- **Save/Load Status –** indicates if Save or Load is successful.

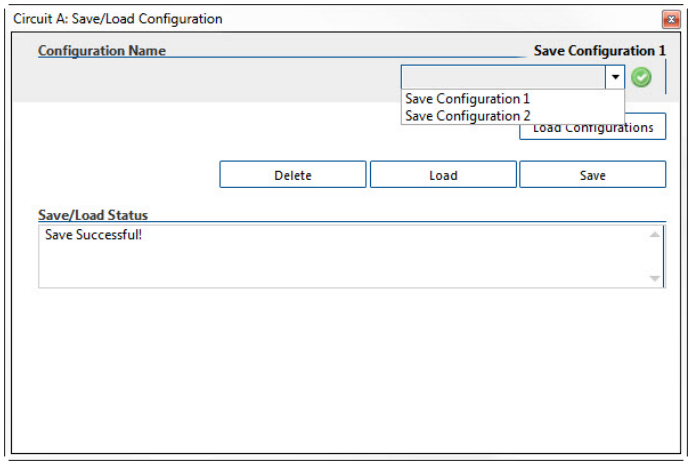


Figure F-17. Save/Load Configuration Window

F.2.9 Ticket Creation

The **Ticket Creation** page shows the configuration with a third party ticketing system (See Figure F-18). Ticket Creations requires the use of Automation and Correlation Engine to generate tickets to a third party ticketing system.

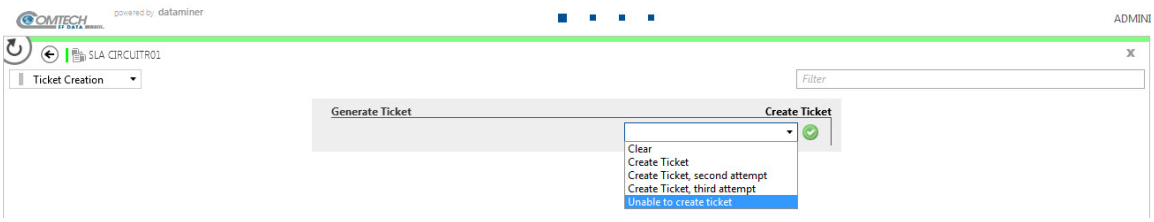


Figure F-18. Ticket Creation

F.2.10 Offline Window

Use the **Offline window** page to define a daily time window when the service is not considered to be offline (See Figure F-19). During this time window, most alarms do not affect the SLA. Exceptions are alarms associated with parameters that are explicitly set to disregard the offline windows settings.

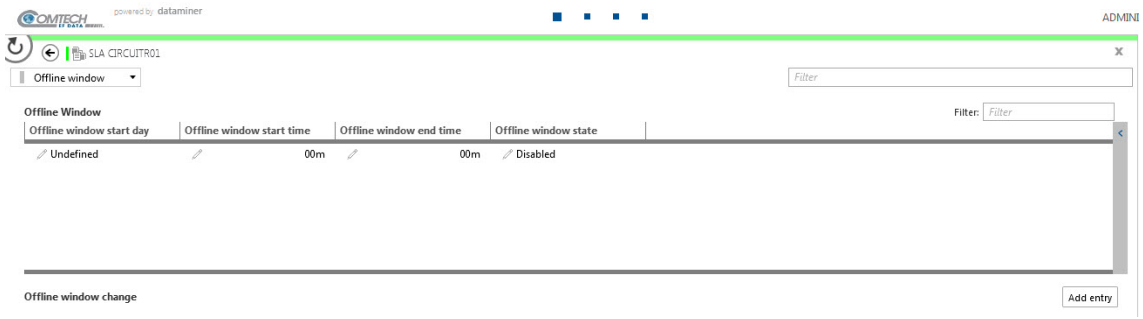


Figure F-19. Offline Window

Offline window start day – set the day of the week when the **Offline window** occurs

Offline window start time – set the start time for the **Offline window**, format: XX hours XX minutes

Offline window end time – set the end time for the **Offline window**, format: XX hours XX minutes

Offline window state – enable, disable or delete the **Offline window** entry

F.2.11 Reporting

To see reporting information for an SLA, go to the **Reports & Dashboards** app. In the left column, choose **Business**. If more than one SLA is available, choose the SLA you want to see.

Several tabs at the top of the overview screen give you access to detailed reporting information.

Summary tab – shows general information on the SLA and the service, and a graph showing alarms distribution.

Distribution tab – shows a detailed graph of alarms distribution over a specific time span. At the top of the screen, you can set this time span and the severity of alarms that are included in the graph.

Severities tab – shows a graphic representation of alarm events and alarm states for the SLA, and a timeline showing the worst alarm states. Use the drop-down menu at the top to choose the data category for the graph: a specific element, SLA availability or SLA compliance.

Alarms tab – shows data about alarms related to the SLA itself, rather than to the elements or service to which the SLA applies.

History tab – use this tab to generate a report of the SLA history.

Service History tab – use this tab to generate an SLA report for specified parameters: past time period, alarm severities and alarm types.

Status tab – shows an overview of all SLA data; this is the same data you see if you open the SLA directly.

Parameter tab – use this tab to generate a report for a parameter selected from a drop-down list.

Top tab – shows the top 10 parameters that had the most alarm events in a time span that you specify.

Trending tab – use this tab to generate a graph that shows the evolution of a specified parameter over a specified time period. Choose the parameter and time period with the drop-down lists at the top of the screen.

F.3 Create an SLA

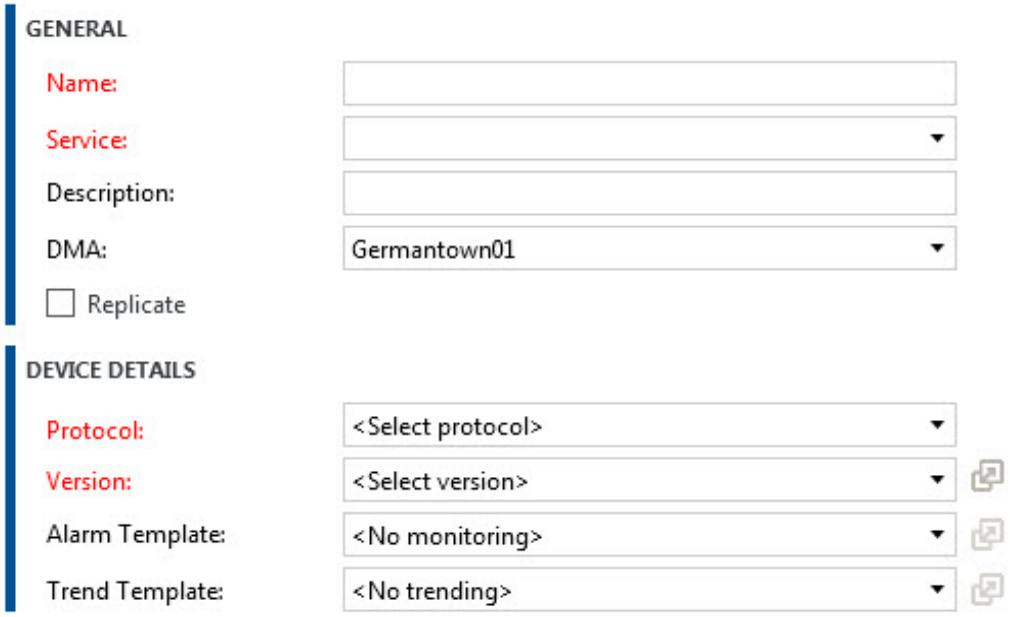


Figure F-20. Creating an SLA

F.3.1 Create an SLA in NetVue

1. In NetVue Cube, navigate to and find the circuit on the Surveyor Tree
2. Right click the Circuit and select New -> SLA
3. See Figure F-20. Creating an SLA.
4. Enter the **Name** label to identify SLA (required).
5. Select the **Service** (Circuit) that must be tracked by the SLA (required).
6. Enter a **Description**, if desired (optional).
7. Select the **DMA**, if desired (optional).
8. Select the **Protocol** (SLA Driver, required).
9. Select the **Version**, the recommended selection is **Production** (required).
10. Select the **Alarm Template**, must be configured to meet customer requirements (optional).
11. Select the **Trending Template**, must be configured to meet customer tracking requirements (optional).
12. Click **Finish** to create the SLA.

F.4 Configure an SLA

1. Define the SLA window, within the SLA configuration window.
2. Define the SLA violation Level.
3. Set the **Compliance** setting.
4. Set the **Total Violation Time.**
5. Set the **Single Violation Time.**
6. Set the **Violation Count**.
7. Set the SLA to **active tracking**.

F.4.1 Make Corrections to an Alarm

To make a correction on the impact of an existing outage:

1. Go to **Outage List** on the **SLA** card.
2. Find the **Outage** to be corrected.
3. Double-click in the **Correction** column for that outage.
4. Make a correction:
    a. To correct part of the outage time:
        i. Clear the **All** checkbox.
        ii. Enter a **Time Span** and confirm.
    b. To correct the outage for the full time span:
        i. Make sure the **All** checkbox is selected and confirm.
5. In the **Motivation** column, enter a motivation or reason for the correction.

Appendix G. MEO LINK PROVISIONING

G.1 MEO Link Manual Link Provisioning Overview

This Chapter explains the process of creating a Circuit that represents a MEO link. Before continuing with this chapter, you must already have an understanding of NetVue, how to configure a browser to access NetVue and System Display, how to navigate within NetVue, basic functionality of NetVue, and how to provision a circuit.

Prior to creating a MEO link, you must complete the prerequisites. Failure to do so can cause false alarms to occur.

G.2 Create Offline Alarm Template

The purpose of the Offline Alarm Template is to track any unit alarms for the offline unit that would affect the operation of the unit. Some unit alarms that are known to occur, such as Rx Unlock, should not be monitored by the offline unit, because they are known states.

The Default alarm template is the template assigned to an element by default. It must be modified to your environment.

When a switchover occurs, the Offline unit assumes the Online Alarm template; or, in this case, the Default Alarm template and the unit going offline assume the Offline Alarm template. This occurs automatically without any intervention from the operator; however, the alarm templates must be pre-defined.

The offline template needs to be created only once. It can be used for all future circuits. Create a new template only if a circuit or some elements need stricter monitoring. This section describes creating an alarm template and a trend template.

Internet Explorer must be configured to allow access to NetVue Cube and System Display prior to following these steps.

G.2.1 Create an Alarm Template

In this section, instructions on how to create an alarm template for an CDM-840 are used as an example. The section should be repeated for any other type of device that will be switching, such as a CDD-880.

1. Log in to NetVue Dataminer Cube with a User Account that has sufficient rights to modify an alarm template.

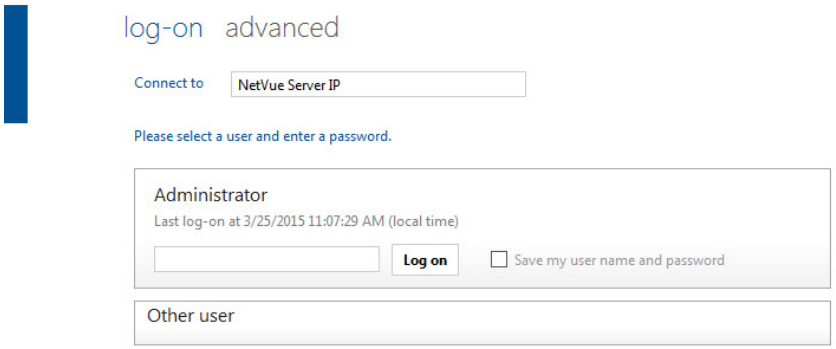


Figure G-1. NetVue Logon

2. Find the **surveyor** section.

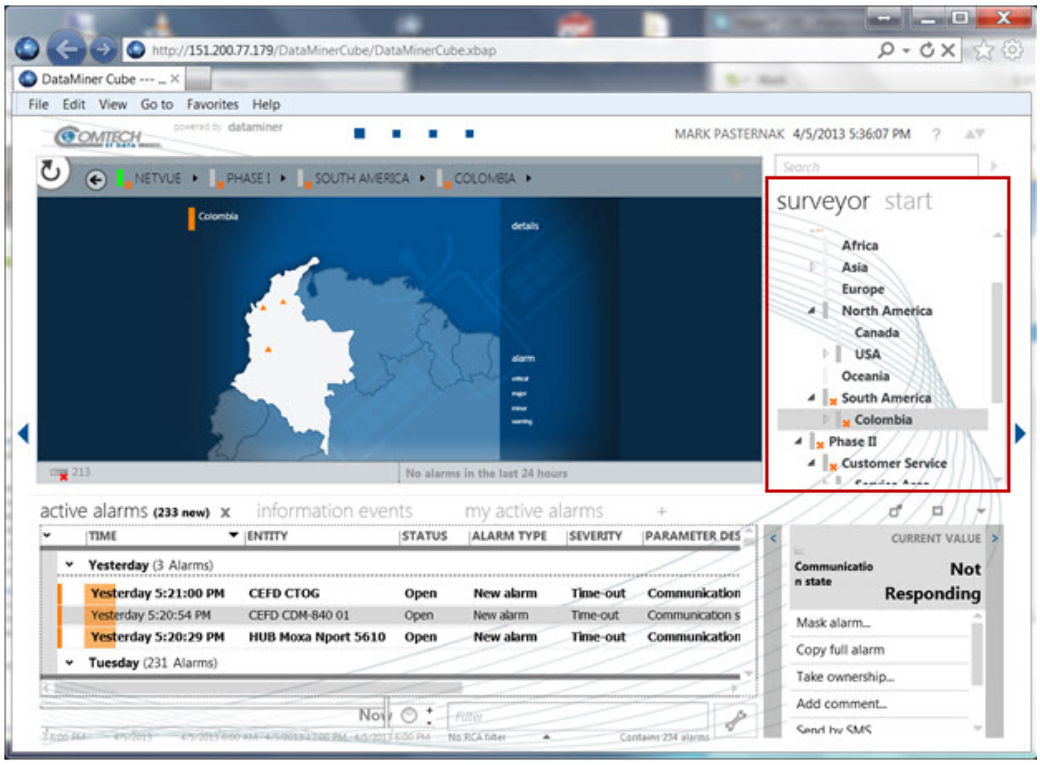


Figure G-2. NetVue Surveyor Tree

3. Click **Start ->** , click **Apps ->**, click **Protocols & Templates** in the **Modules** section.

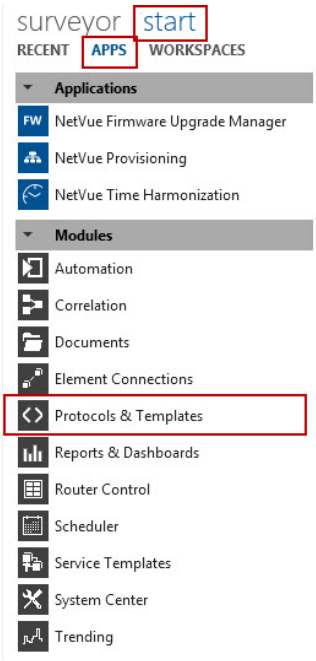


Figure G-3. Applications

4. Select **CEFD CDM-840 SNMP** protocol.

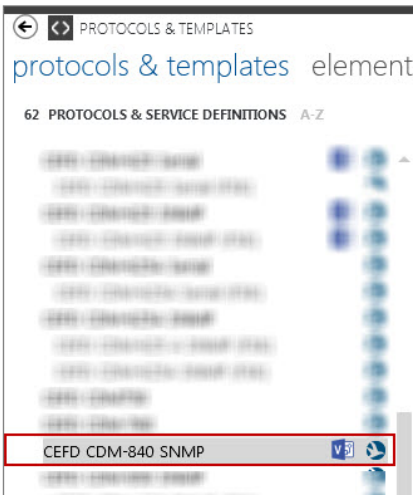


Figure G-4. CDM-840 Protocol

5. In the Alarm Column, right-click **Alarm** and select **New.**

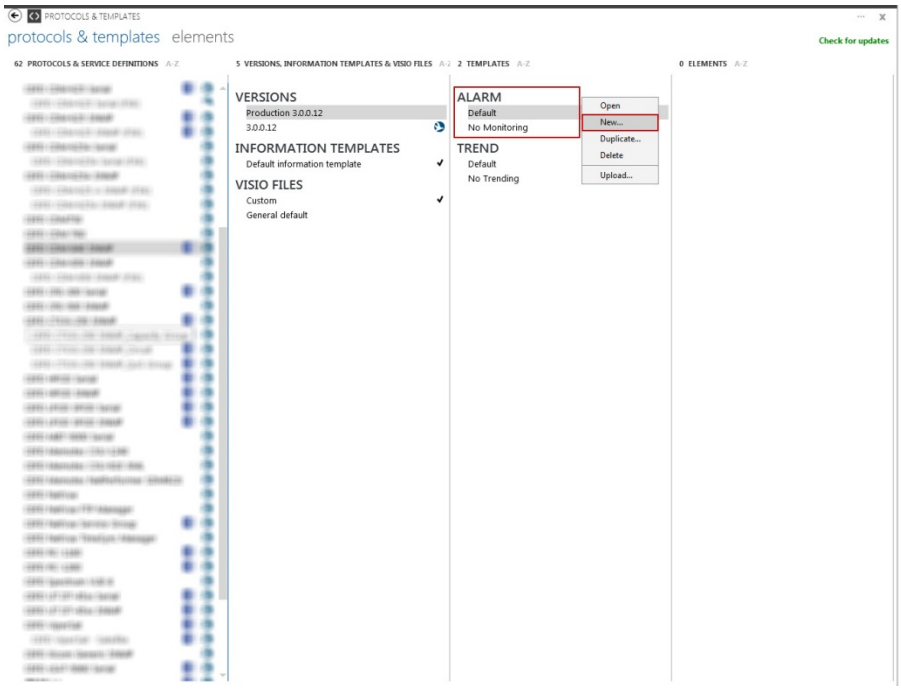


Figure G-5. Alarm Templates

6. In the new window:

   a. Select **Alarm Template**
   This is the default setting.

   b. Enter the **Name** of the label template

   c. Select the **Protocol**
   CEFD CDM-840 SNMP is the default setting

   d. Select the **Version**
   Production is the default

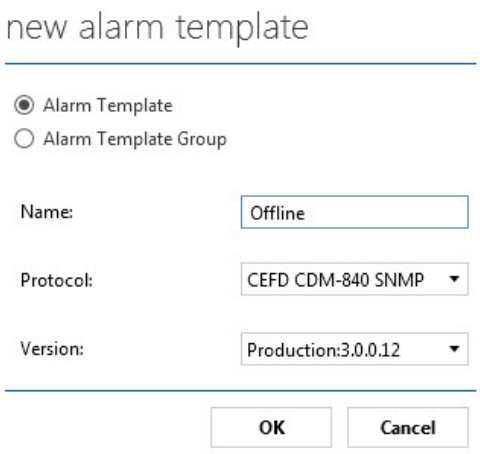


Figure G-6. New Alarm Template

7. Select the parameters to be monitored in your environment:
   a. In the MON column, click the check box next to a parameter to enable its monitoring

      For detailed information about alarm templates, refer to step 6.a.

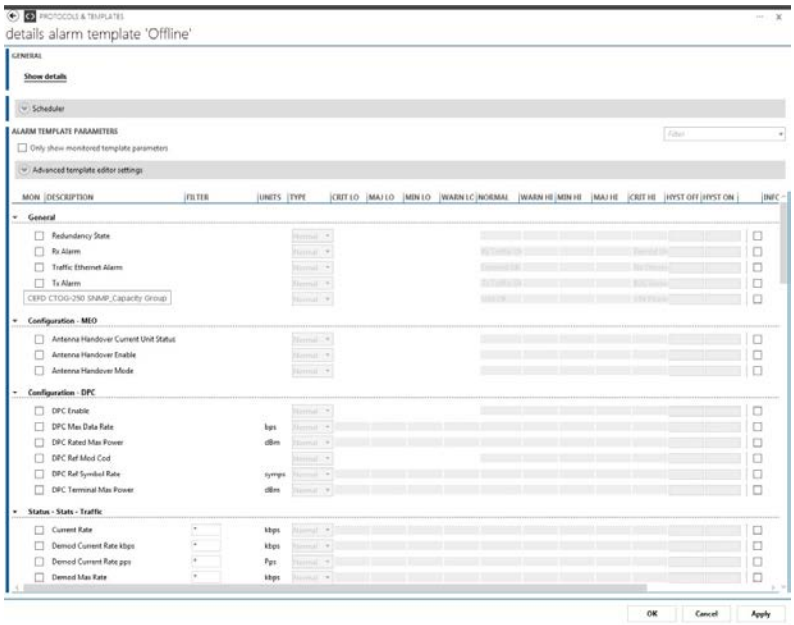


Figure G-7. Alarm Template Parameters

8. After all of the parameters have been selected, click **Apply**.

It is not necessary to use all severity levels.

G.3 Provision Circuit

The provisioning of a circuit lets you set up the circuit without having to create each of the elements and link them all to a circuit.

All CDM-880s and CDM-840s must be added to a circuit. The management IP of all equipment must be accessible from NetVue.

For instructions on how to provision a circuit, see the NetVue Provisioning Guide. It is available on the Comtech EF Data web site:

http://www.comtechefdata.com/files/manuals/mn-netvue-pdf/MN-NETVUEPVG.pdf

G.4 Redundancy Group

This section explains how to create the redundancy group.

To correctly represent an Advanced VSAT MEO link comprised of two CDM-840s and two CDD-880s, a redundancy group must be created for the CDM-840s and CDD-880s. A redundancy group in this case is not considered the primary and back up, but is a container for an Online and Offline unit. Only one unit can be online at any time, and only one CDD-880 can be locked at any time, except during a handover. During a handover, there is a period of time when both units are online and locked.

If the images and wording show **primary** and **back up**, consider these terms to mean **online** and **offline**. It does not matter which unit is the online unit, because NetVue finds which unit is online and offline automatically, and swaps accordingly.

It is best if the MEO field on the HTTP interface corresponds to which unit is the primary and which unit is the secondary, although this is not required.

G.5 Create a Redundancy Group in System Display for CDM-840

1. Log in to system display.
2. Click the **Admin** tab and select elements.

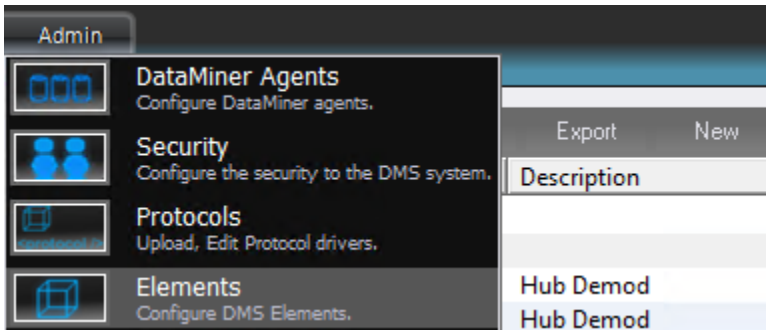


Figure G-8. System Display Elements

3. Click the down triangle that is adjacent to **New**.

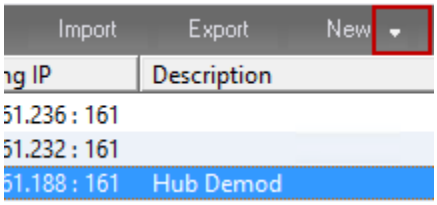


Figure G-9. System Display New Elements

The New option might not show the triangle. Select an Element in the list to add a triangle. Now, you have the option to create a redundancy group.

4. Select **New Redundancy Group** to start the Redundancy Group Wizard.

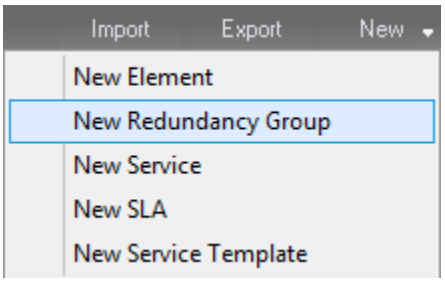


Figure G-10. System Display New Redundancy Group

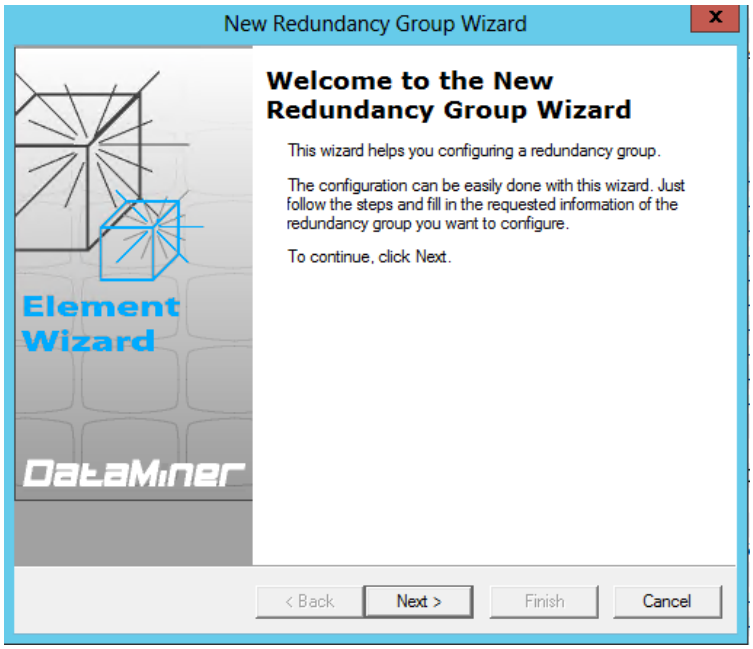


Figure G-11. New Redundancy Group Wizard

5. Enter a unique **Name** for the Redundancy Group.
6. Optionally, enter a **Description.**
7. Click **Next.**

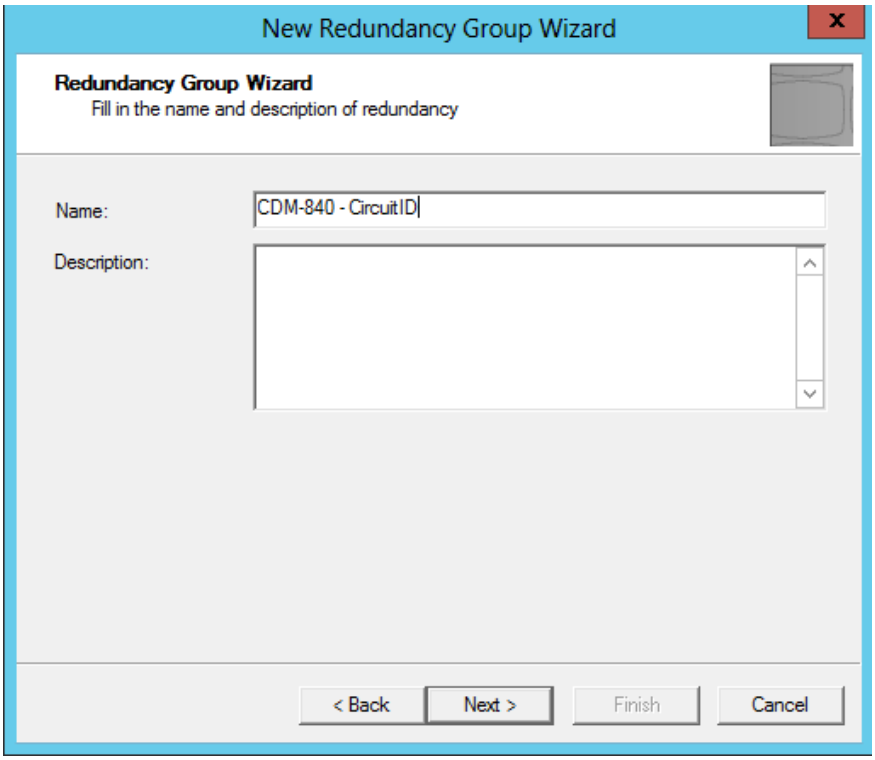


Figure G-12. Redundancy Group Name

8. Make sure that **Configure the masking for all elements at once** is not selected.

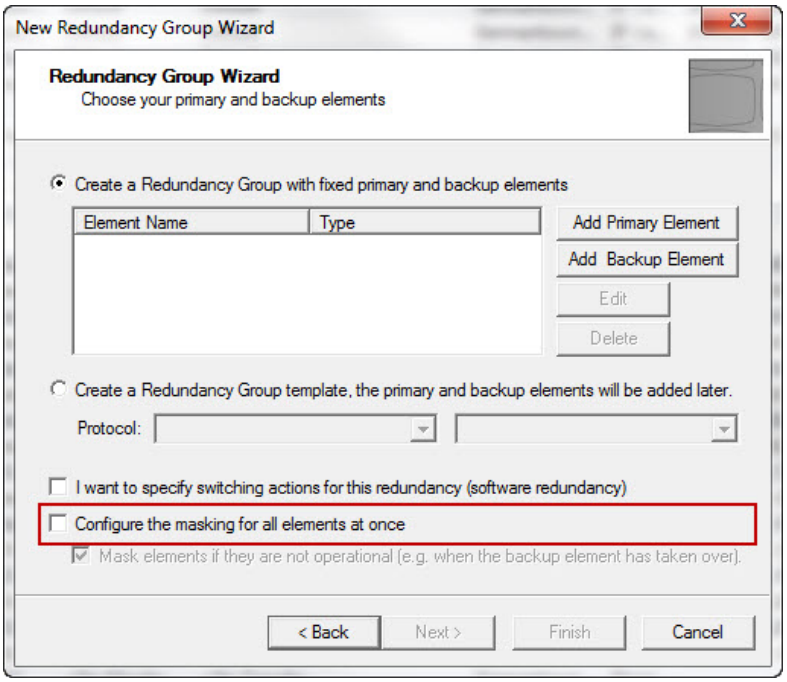


Figure G-13. Redundancy Group Masking

9. Click **Add Primary Element.**

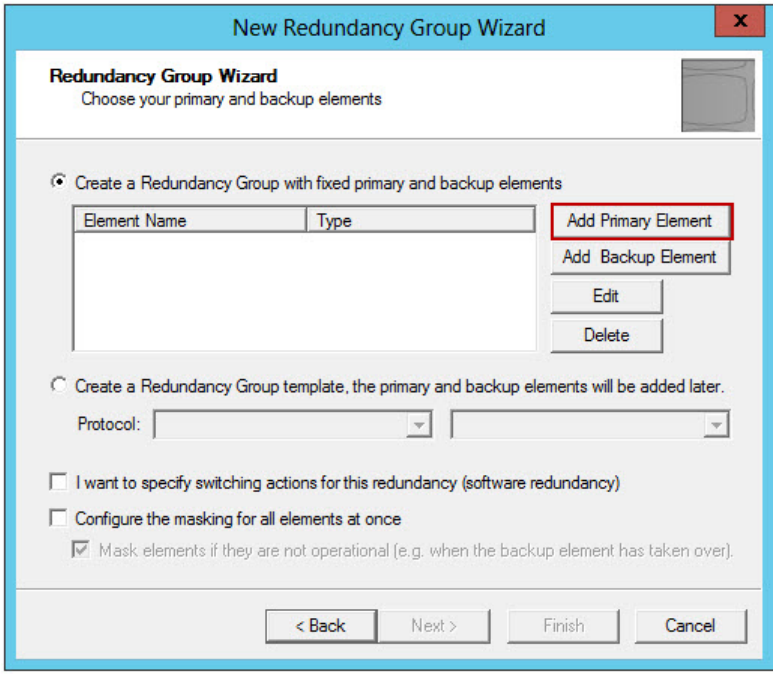


Figure G-14. Add Primary Element

10. Select the **Element** from the drop down list.

    The **Derived Name** is the **Element** name of the active unit.

At first, the Element name is that of the primary device. Change this so that the VNO cannot distinguish which device it is choosing. For example, delete the A or B and keep only the Unique Identifier, such as the Circuit ID.

11. Make sure **Mask this element if it is not operational** is not selected.
12. Select **Custom Templates after switching.**
13. Set the **Alarm** and **Trending Templates** for when the unit is operational and non operational.

The templates can always be changed later.

14. Click **OK.**

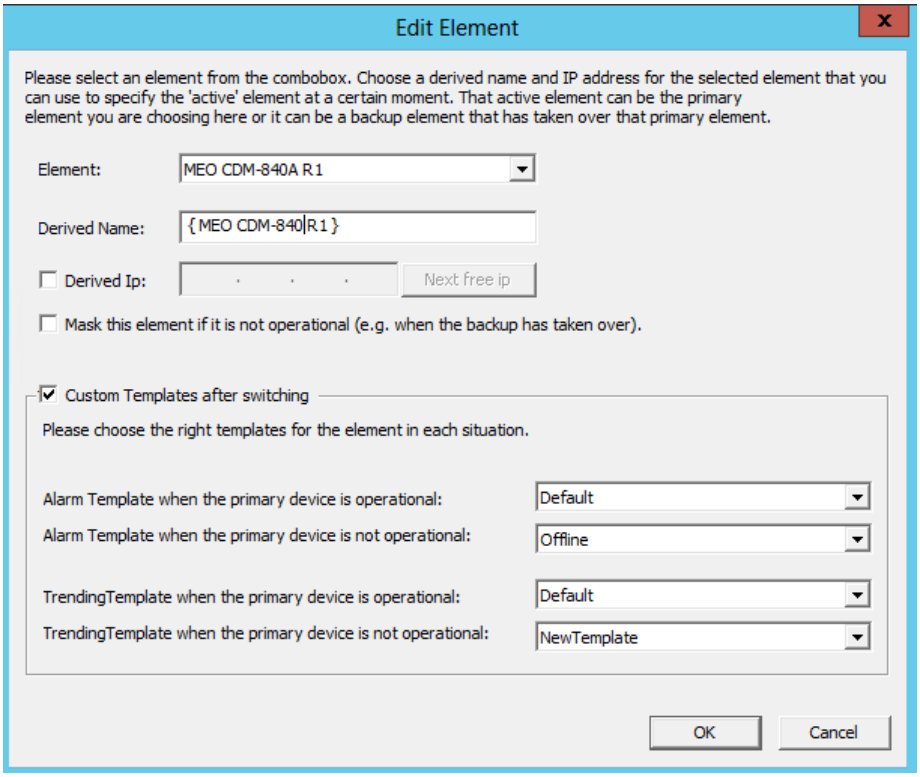


Figure G-15. Custom Templates

15. Click **Add Backup Element.**

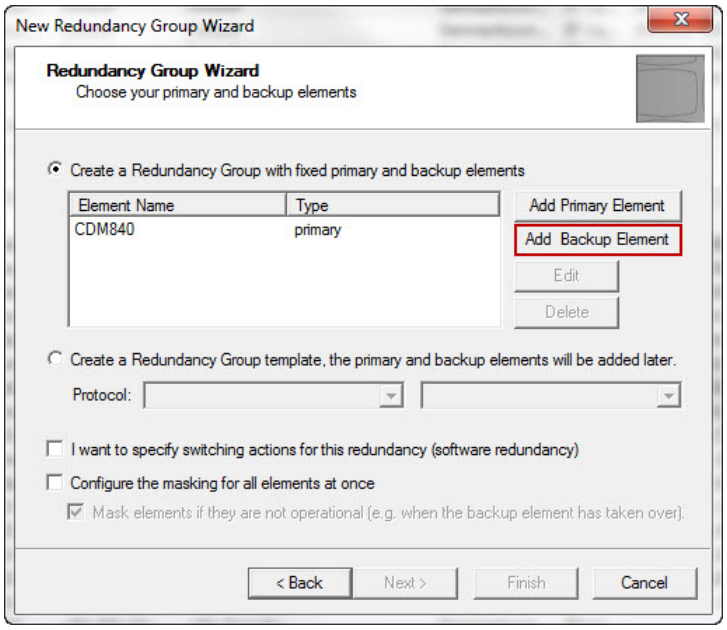


Figure G-16. Backup Element

16. Choose the **Backup Element** from the drop down list.

The drop down list shows only the same type of element as the primary element.

17. Choose the **Alarm Template** and the **Trend Template** for when the device is not operating. This must be the offline template that you set up in the previous section.
18. Click **OK.**

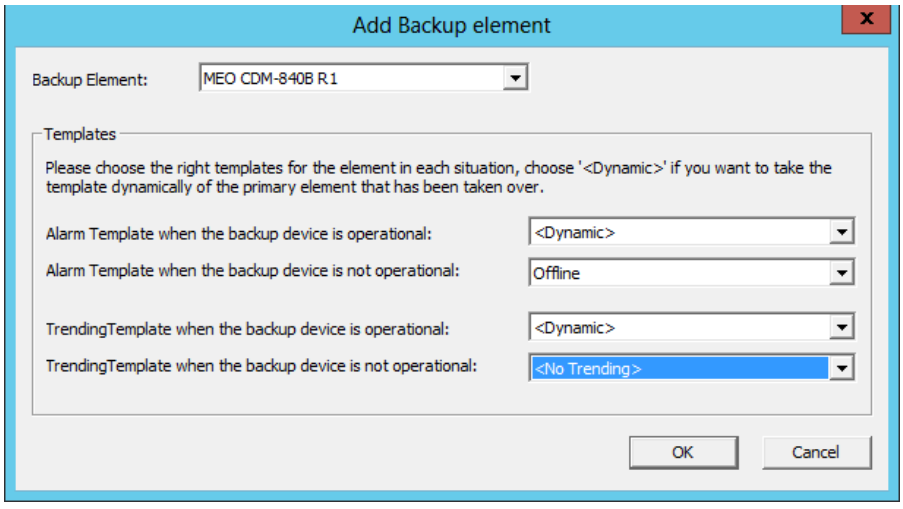


Figure G-17. Backup Element Templates

19. Make sure that both primary and backup elements are set up, then click **Next.**

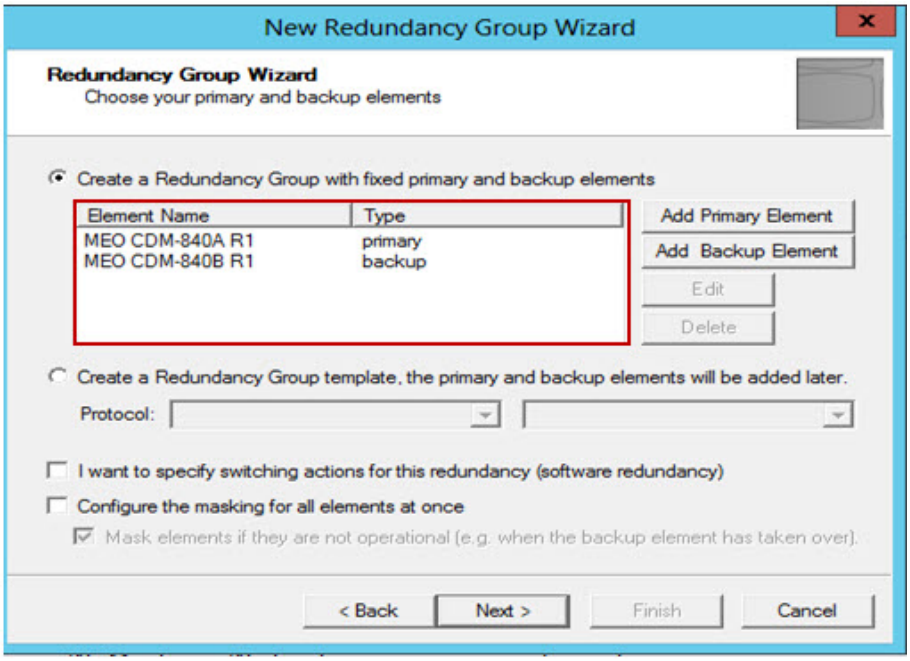


Figure G-18. Primary and Backup Elements Added

20. Set the switching criteria for when the offline element must take over from the online, and vice versa.
21. Click **Advanced Switching.**

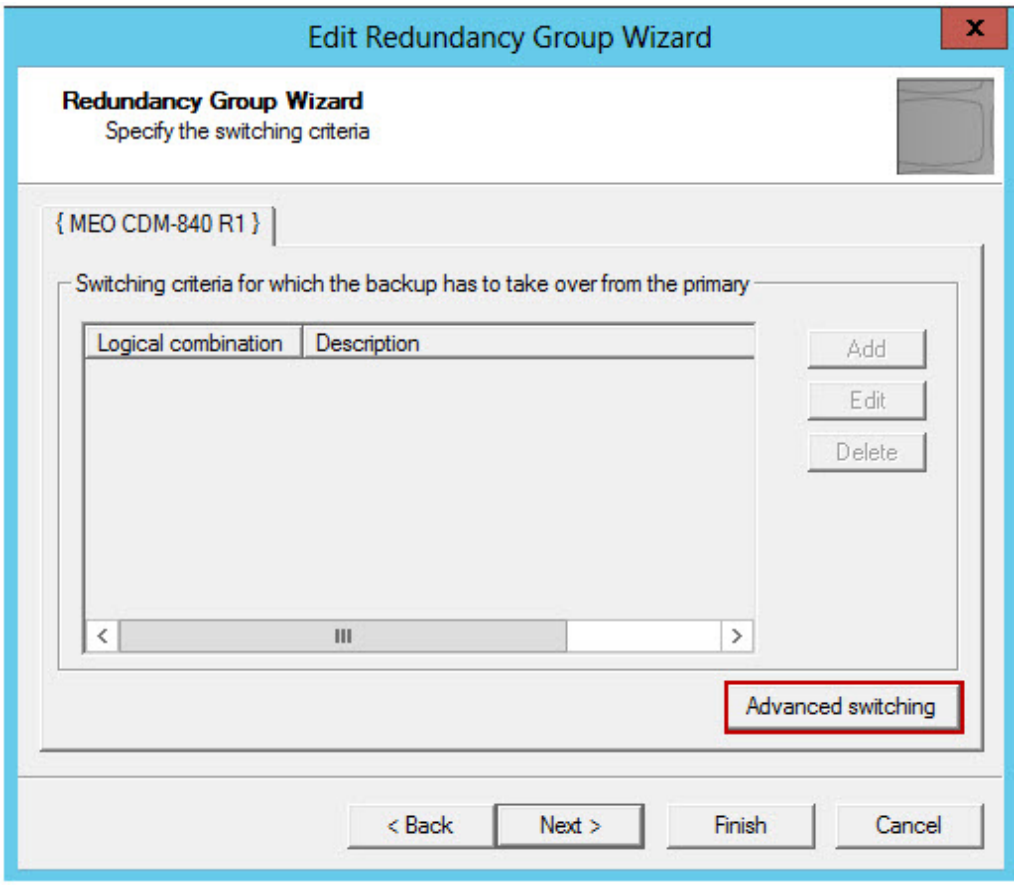


Figure G-19. Advanced Switching

22. Click **Add** to specify the criteria for switching to the backup element.

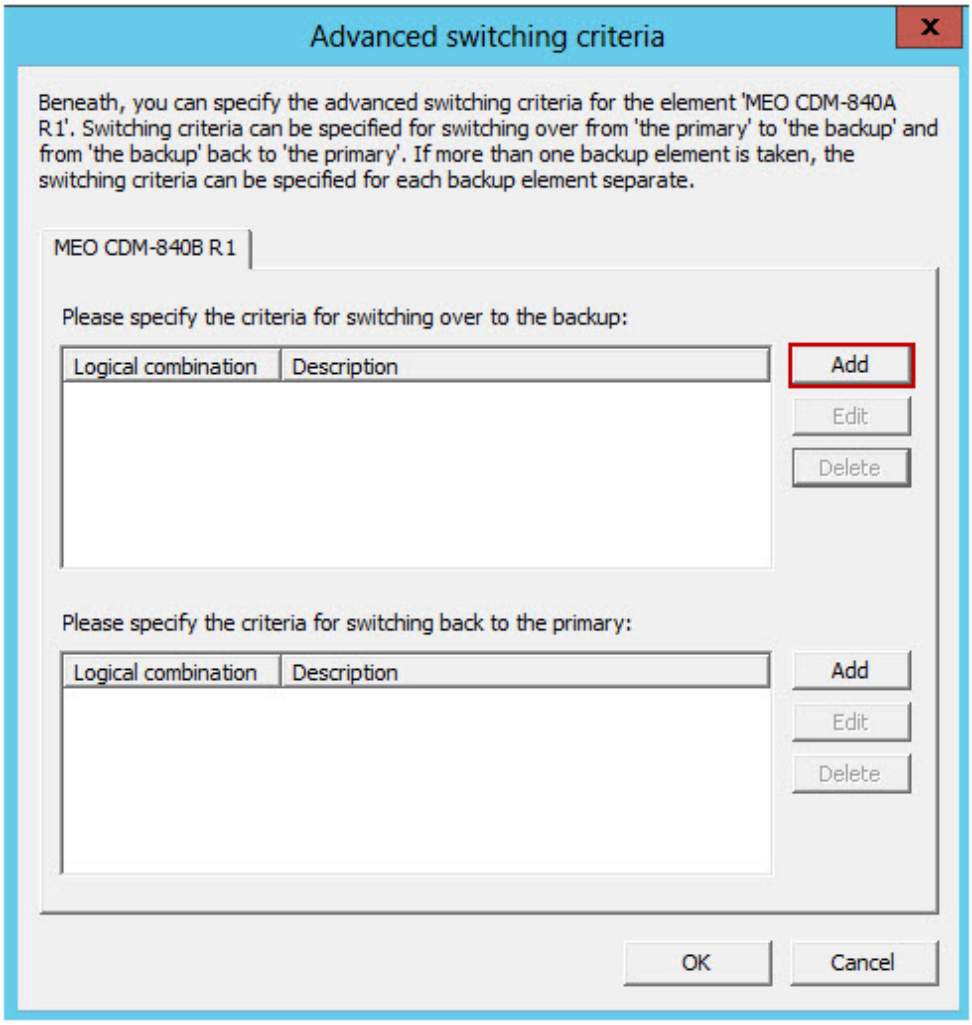


Figure G-20. Back Up Switch Criteria

23. Set up the criteria for switching to a backup element:
    a. Select **Parameter is changing.**
    This is the default setting.
    b. Select the **Element** from the list.
    Choices include <ALL Primary> or the individual Primary Element.
    c. Select **Redundancy State** from the **Parameter** list.
    d. Set **Equal** to **Off Line.**
24. Click **OK.**

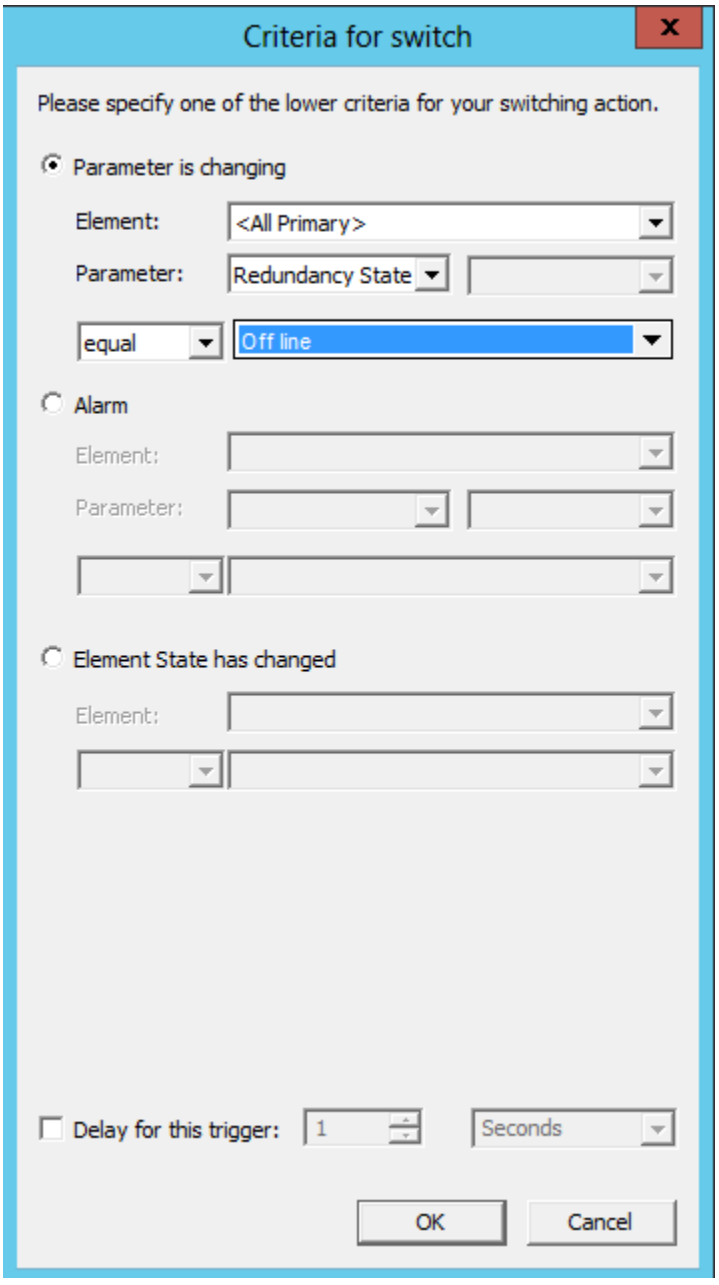


Figure G-21. Redundancy State Offline

25. Click **Add** to specify the criteria for switching to the primary element.

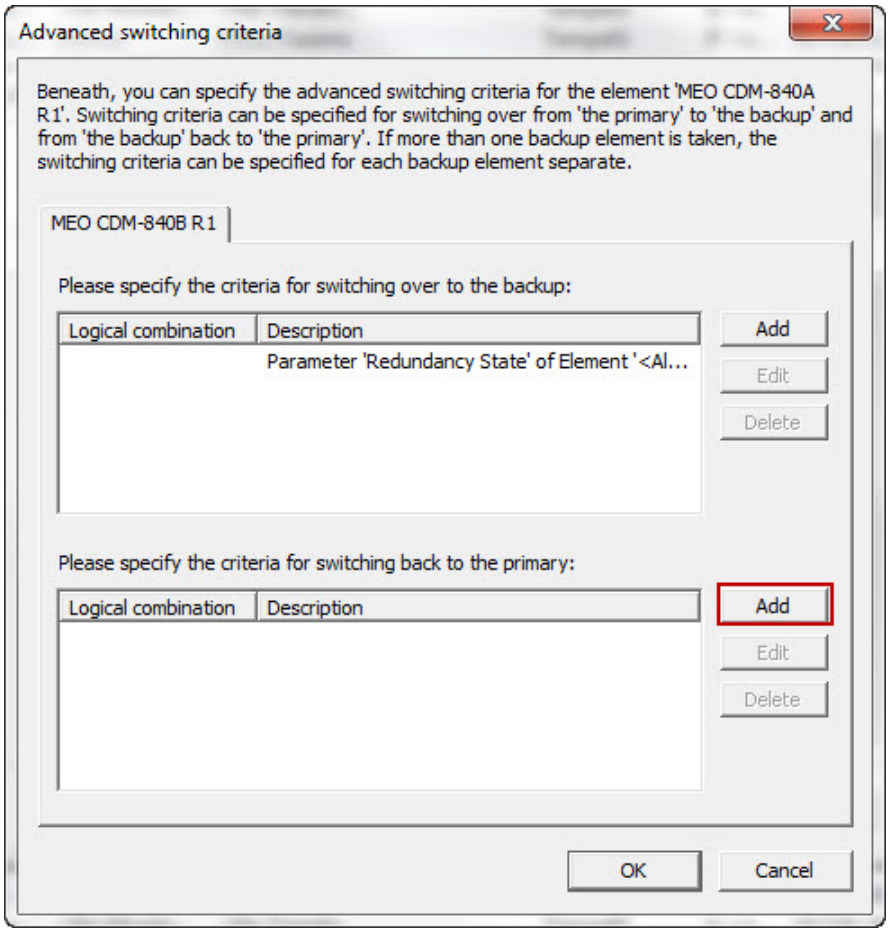


Figure G-22. Switch Back Criteria

26. Set up the criteria for switching to the primary element:
    a. Select **Parameter is changing.**
    b. Select the **Element** from the list.
    Choices include **<ALL Backup>** or the individual Backup Element.
    c. Select **Redundancy State** from the **Parameter** list.
    d. Set **Equal** to **Off Line.**
27. Click **OK.**

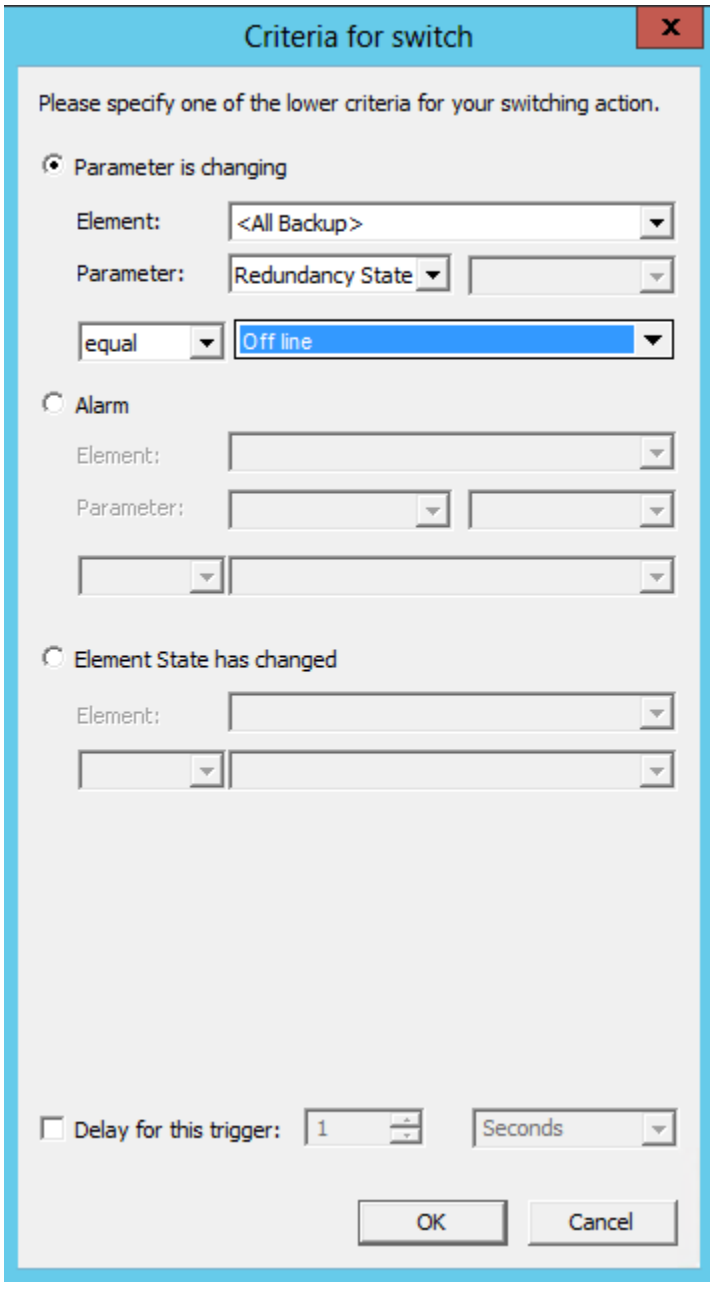


Figure G-23. Redundancy State Offline

28. Make sure that the criteria for both elements are listed and correct.
29. Click **OK.**

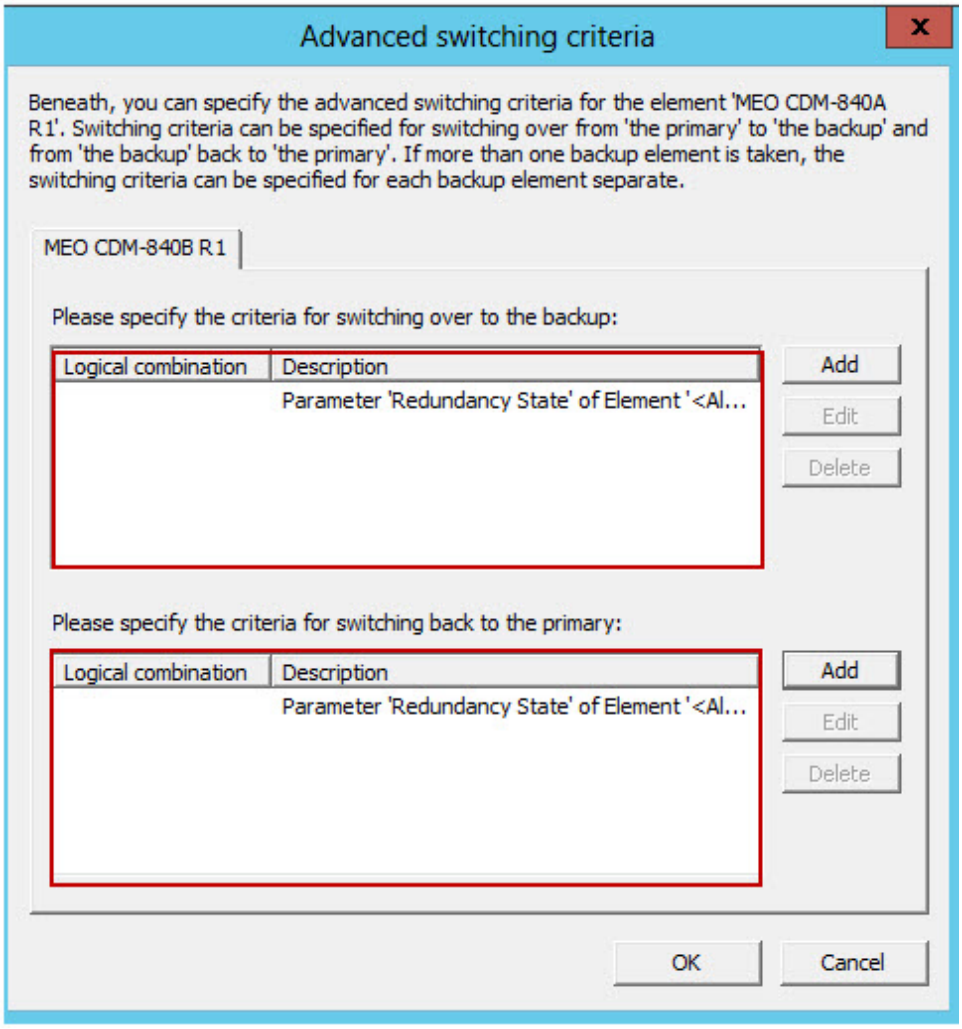


Figure G-24. Criteria Set

30. Click **Next.**

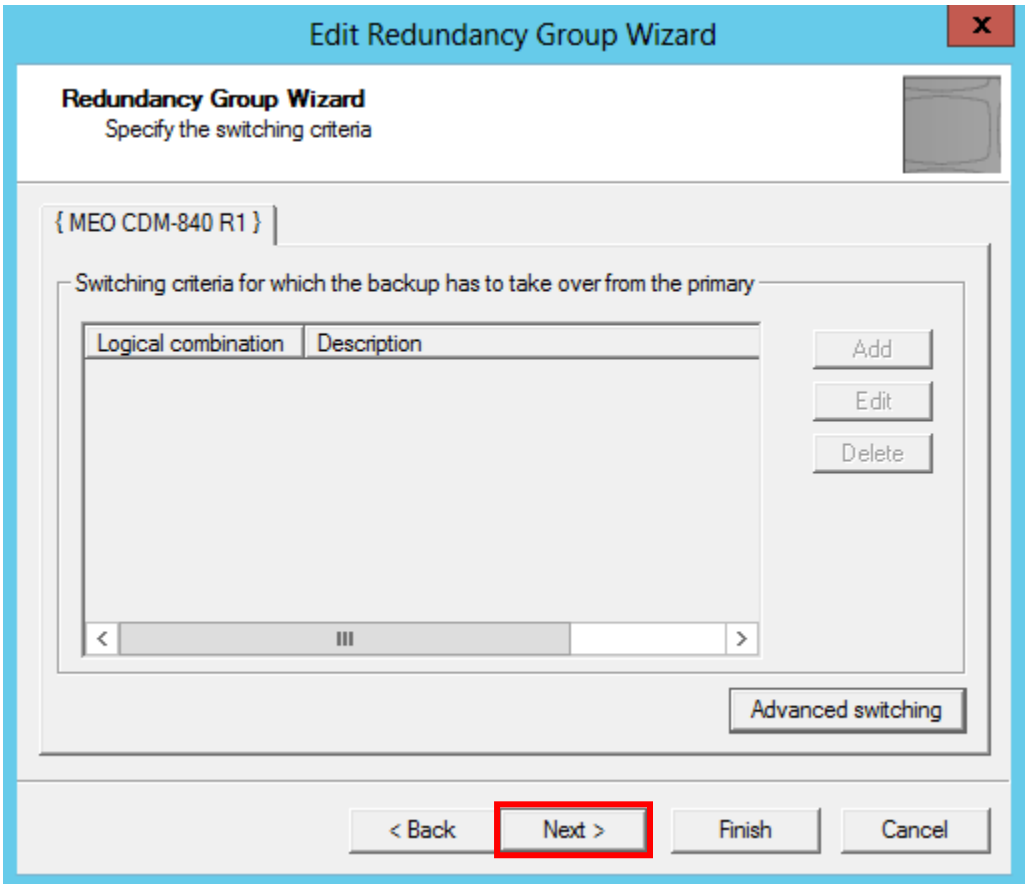


Figure G-25. Advanced Switching Criteria Completed

31. Put the Redundancy Group into the correct view.

If necessary, you can move the redundancy group later.

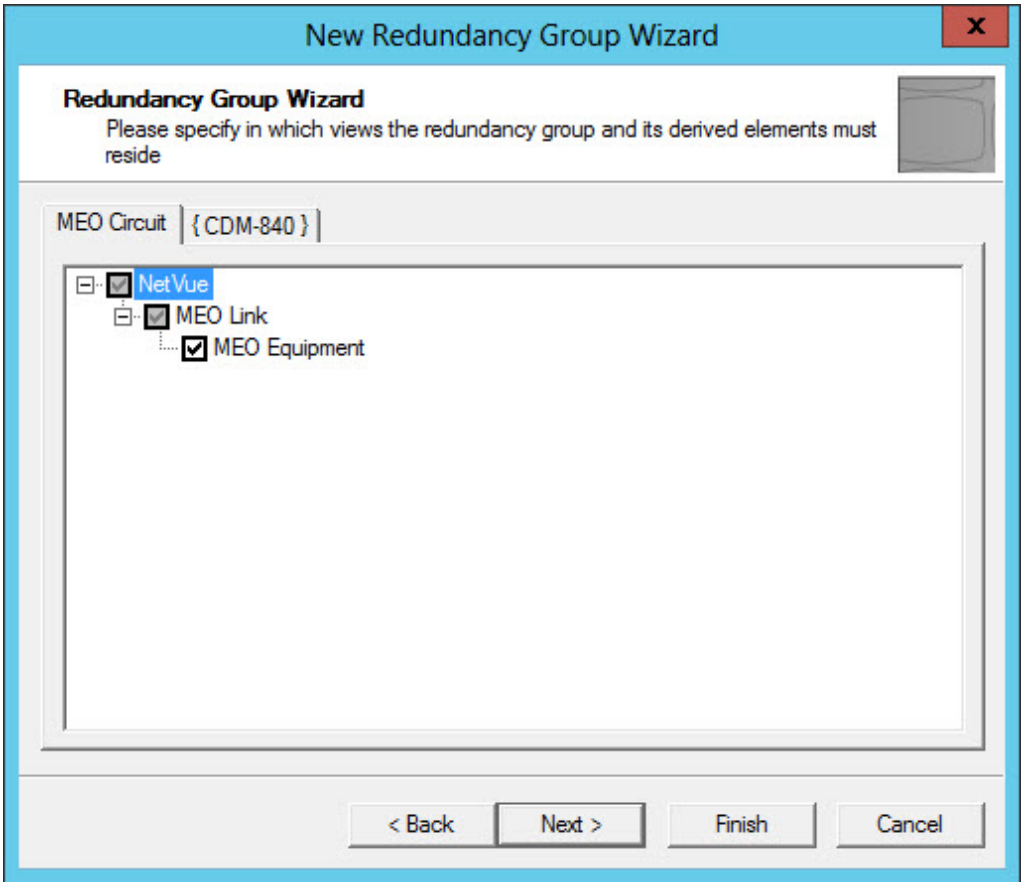


Figure G-26. Redundancy Group Placement

32. Click **Finish.**

G.6 Create a Redundancy Group in System Display for CDD880

1. Log in to system display.
2. Click the **Admin** tab.
3. Select elements.

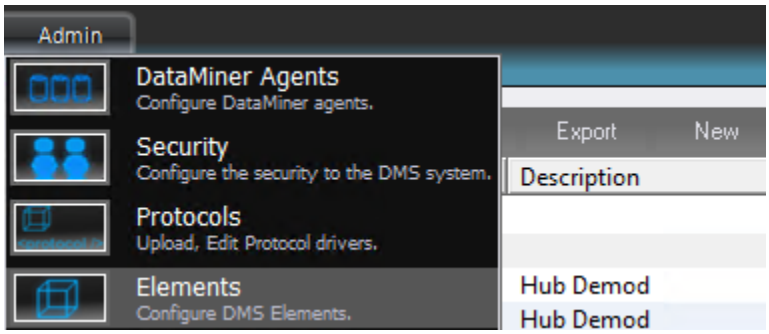


Figure G-27. Admin > Select Elements

4. Click the triangle adjacent to **New.**

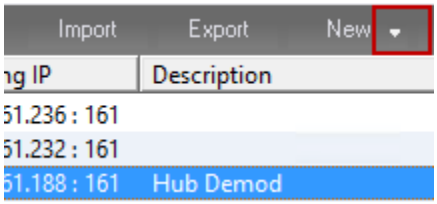


Figure G-28. New Triangle Icon

The New option might not show the triangle. Select an Element in the list to add a triangle. Now, you have the option to create a redundancy group.

5. Select **New Redundancy Group** to start the Redundancy Group Wizard.

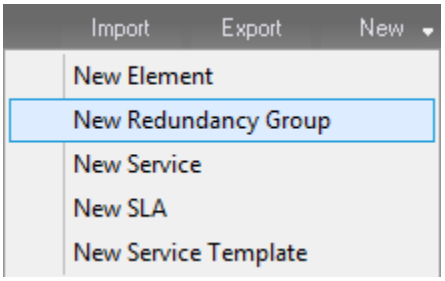


Figure G-29. New Redundancy Group

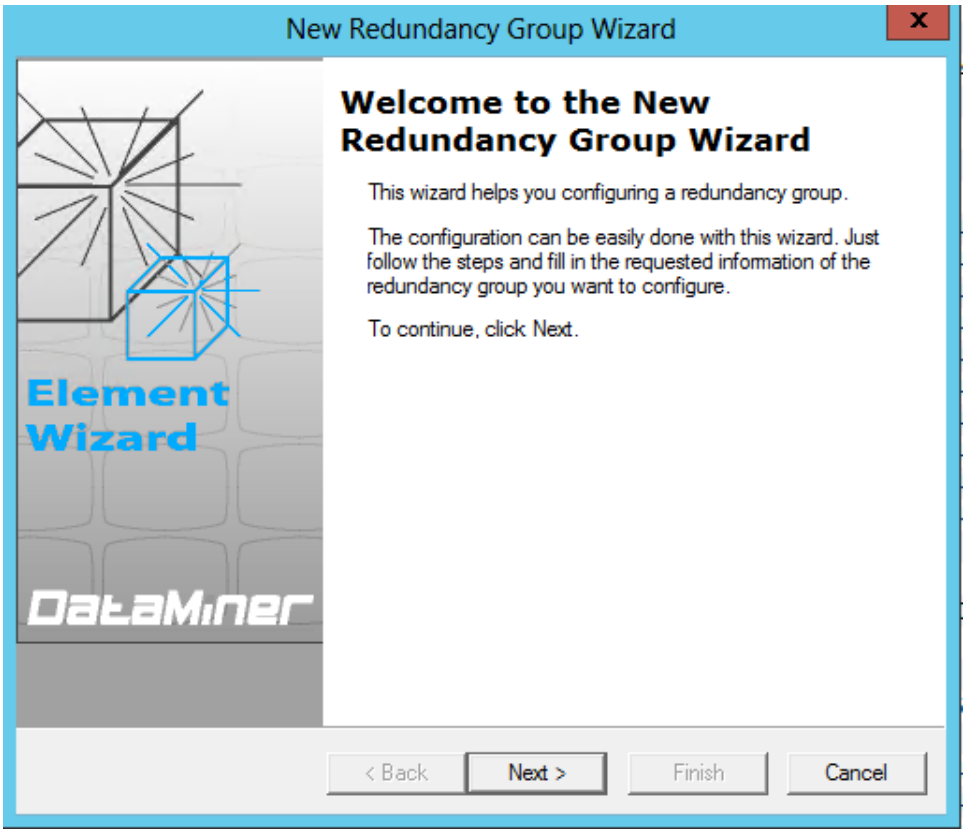


Figure G-30. New Redundancy Group Wizard Welcome

6. Enter a unique **Name** for the Redundancy Group.
7. Optionally, enter a **Description.**
8. Click **Next.**

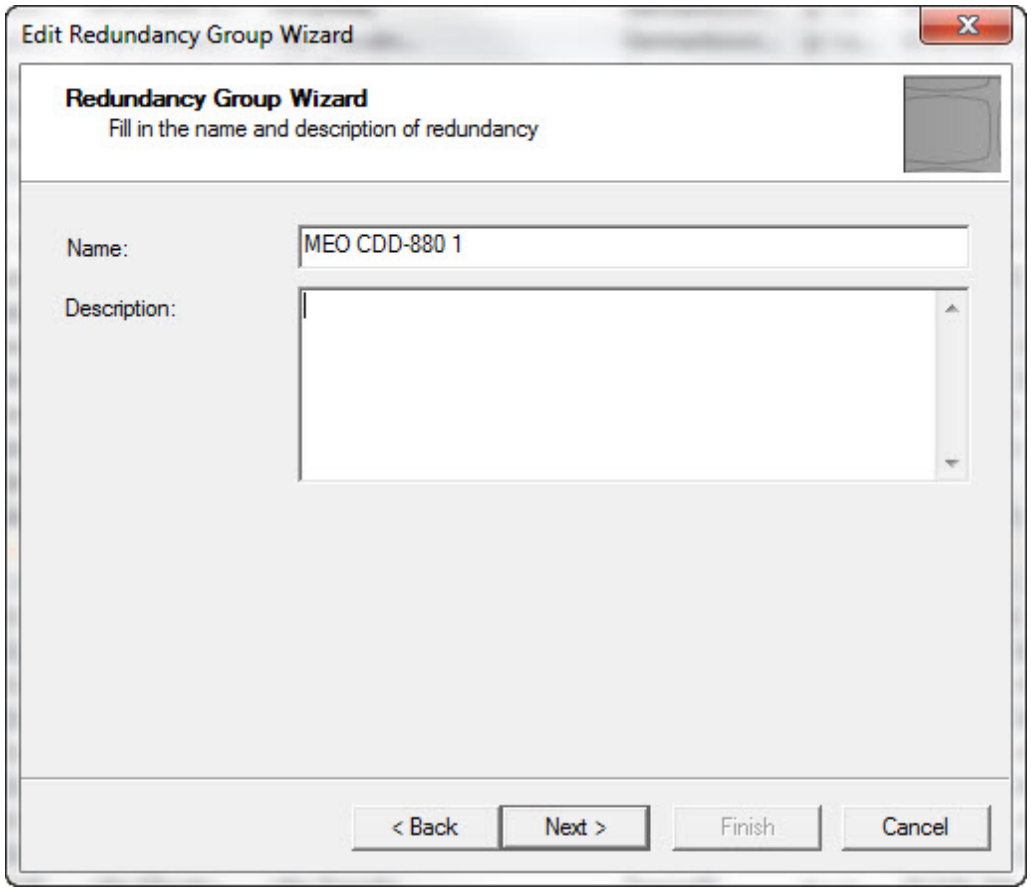


Figure G-31. Redundancy Group Name

9. Make sure that **Configure the masking for all elements at once** is not selected.
10. Click **Add Primary Element.**

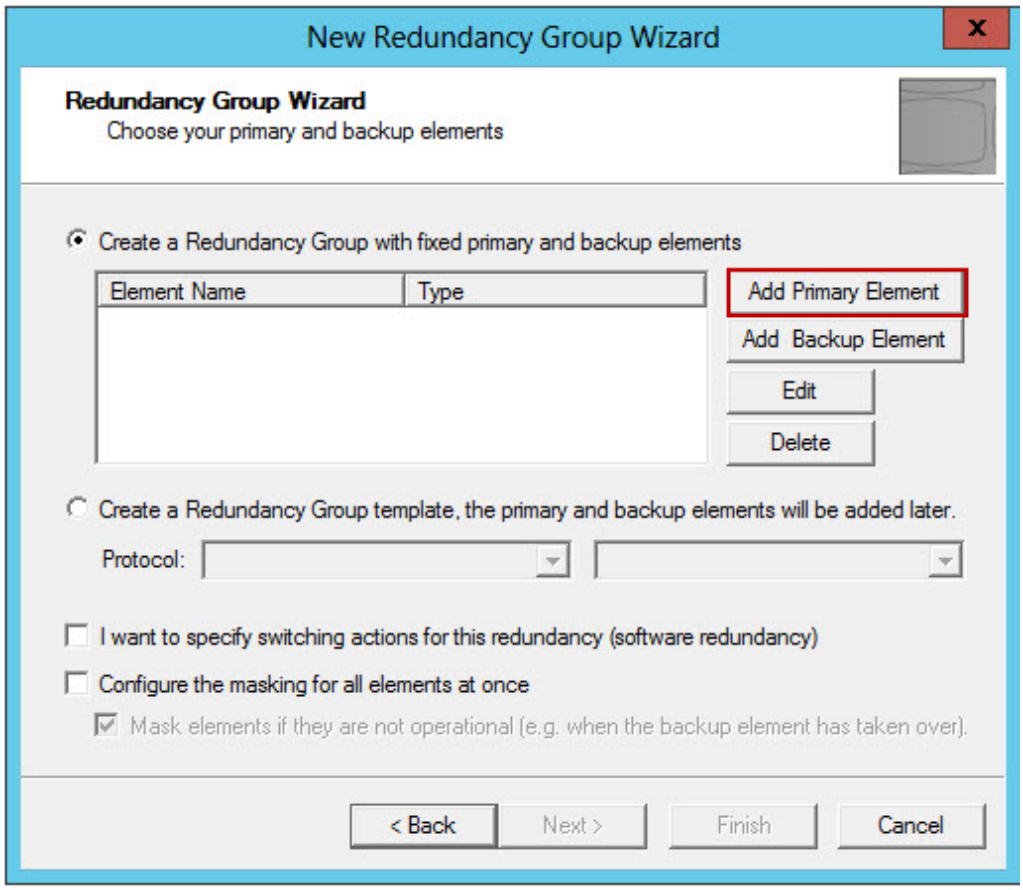


Figure G-32. Add Primary Element

11. Select the **Element** from the drop down list.
12. The **Derived Name** is the **Element** name of the active unit.

At first, the Element name is that of the primary device. Change this so that the VNO cannot distinguish which device it is choosing. For example, delete the A or B and keep only the Unique Identifier, such as the Circuit ID.

13. Make sure **Mask this element if it is not operational** is not selected.
14. Select **Custom Templates after switching.**
15. Set the **Alarm** and **Trending Templates** for when the unit is operational and non operational.

The templates can always be changed later.

16. Click **OK**.

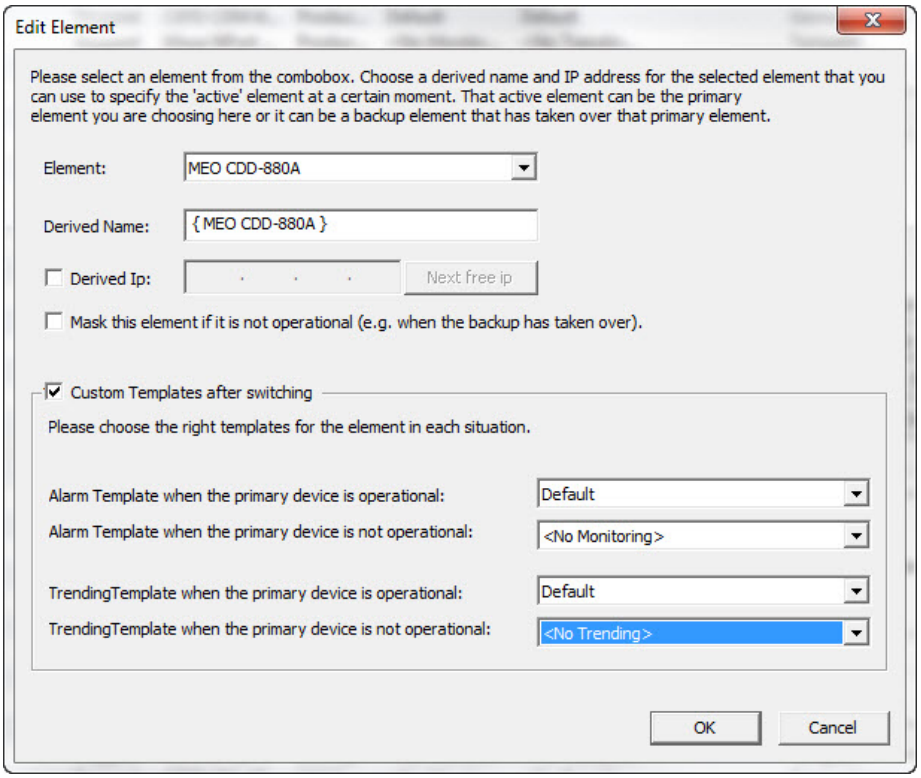


Figure G-33. Custom Templates

17. Click **Add Backup Element.**

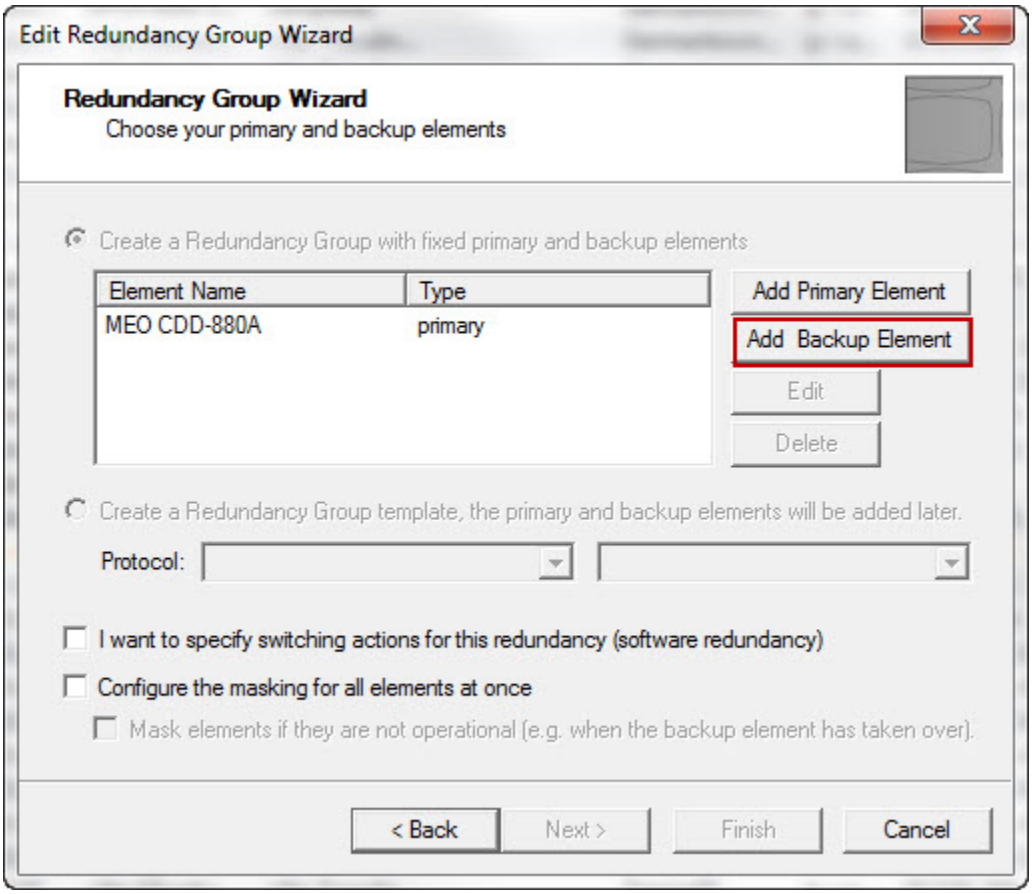


Figure G-34. Backup Element

18. Choose the **Backup Element** from the drop down Menu.

The drop down list shows only the same type of element as the primary element.

Choose the **Alarm Template** and the **Trend Template** for when the device is not operating. This must be the offline template that you set up in the previous section.

19. Click **OK**.

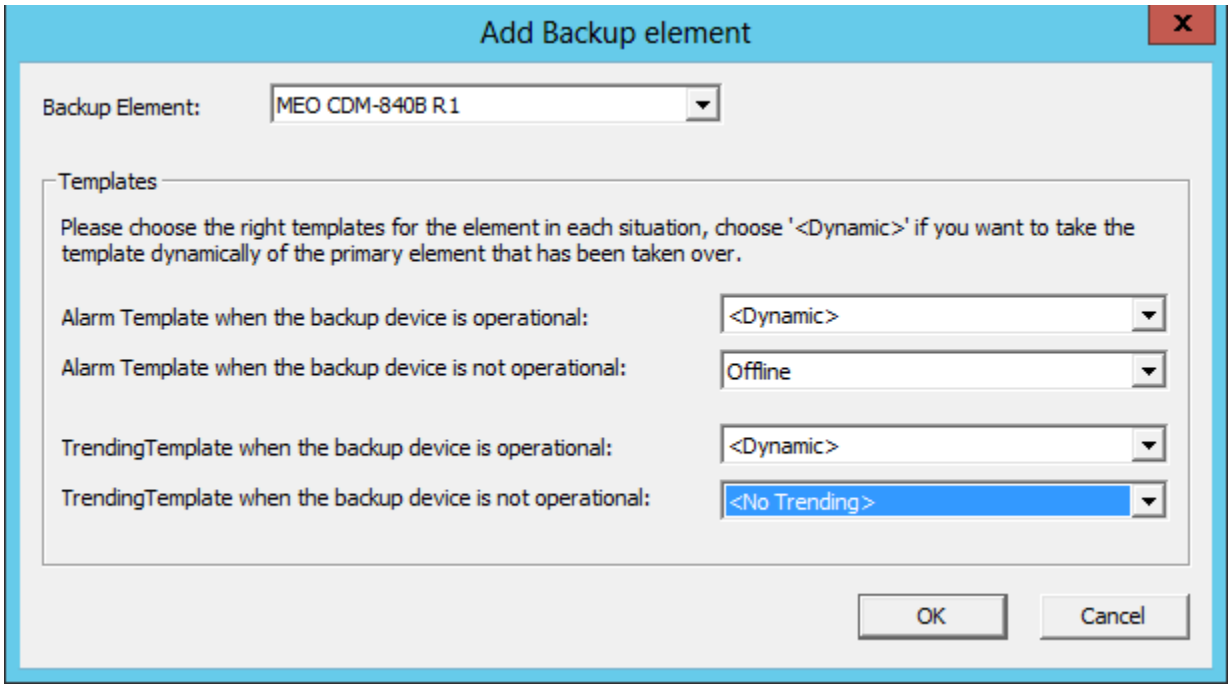


Figure G-35. Backup Element Templates

20. Make sure both Primary and Backup elements are defined.
21. Click **Next**.

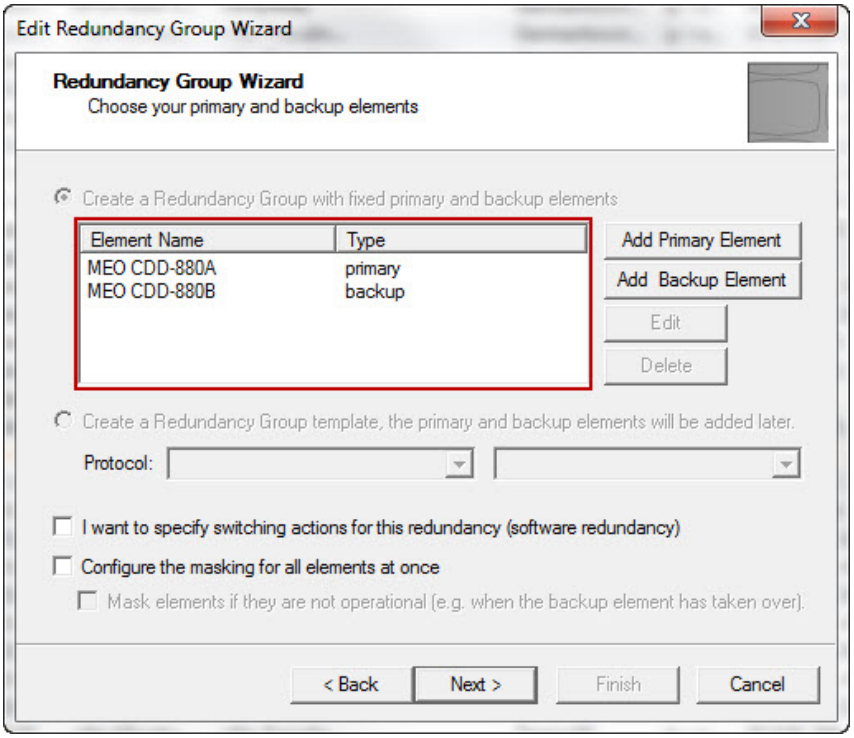


Figure G-36. Define Both Primary and Backup Elements

22. The switching criteria must be set for when the offline has to take over from the online and vice versa.
23. Click **Advanced Switching**.

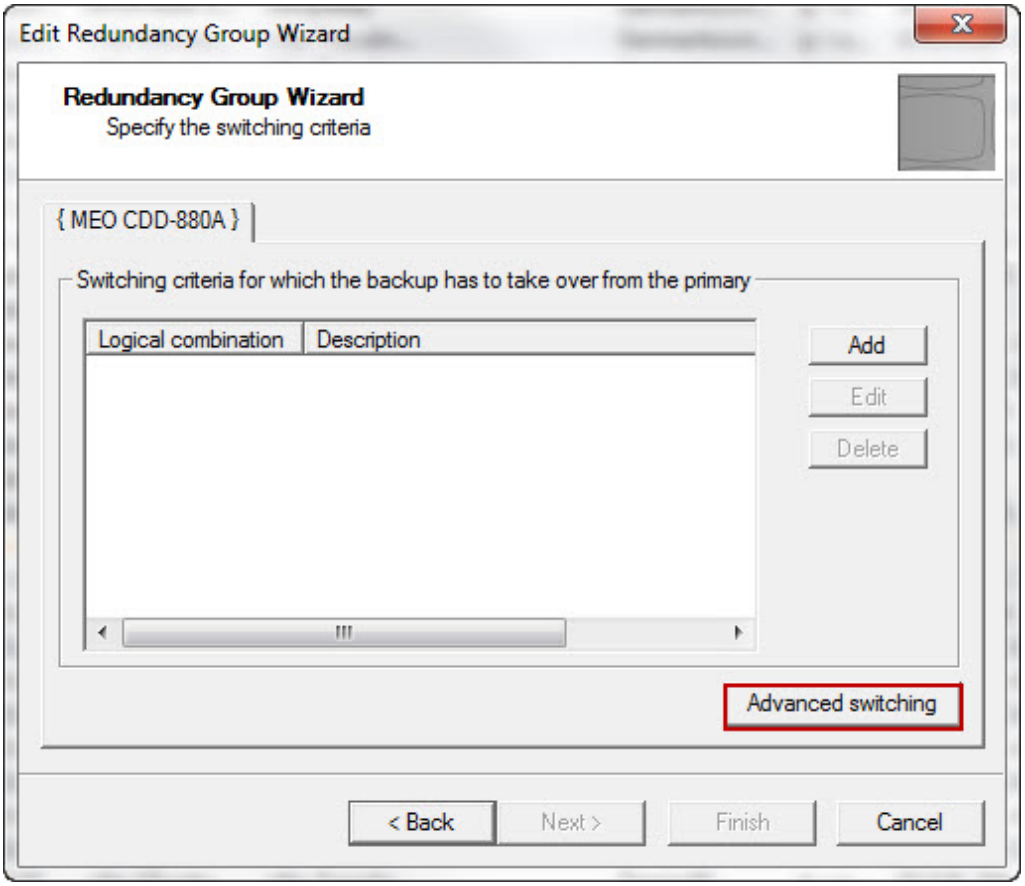


Figure G-37. Redundancy Group Wizard Advanced Switching

24. Click **Add** to set the criteria for switching to the backup.

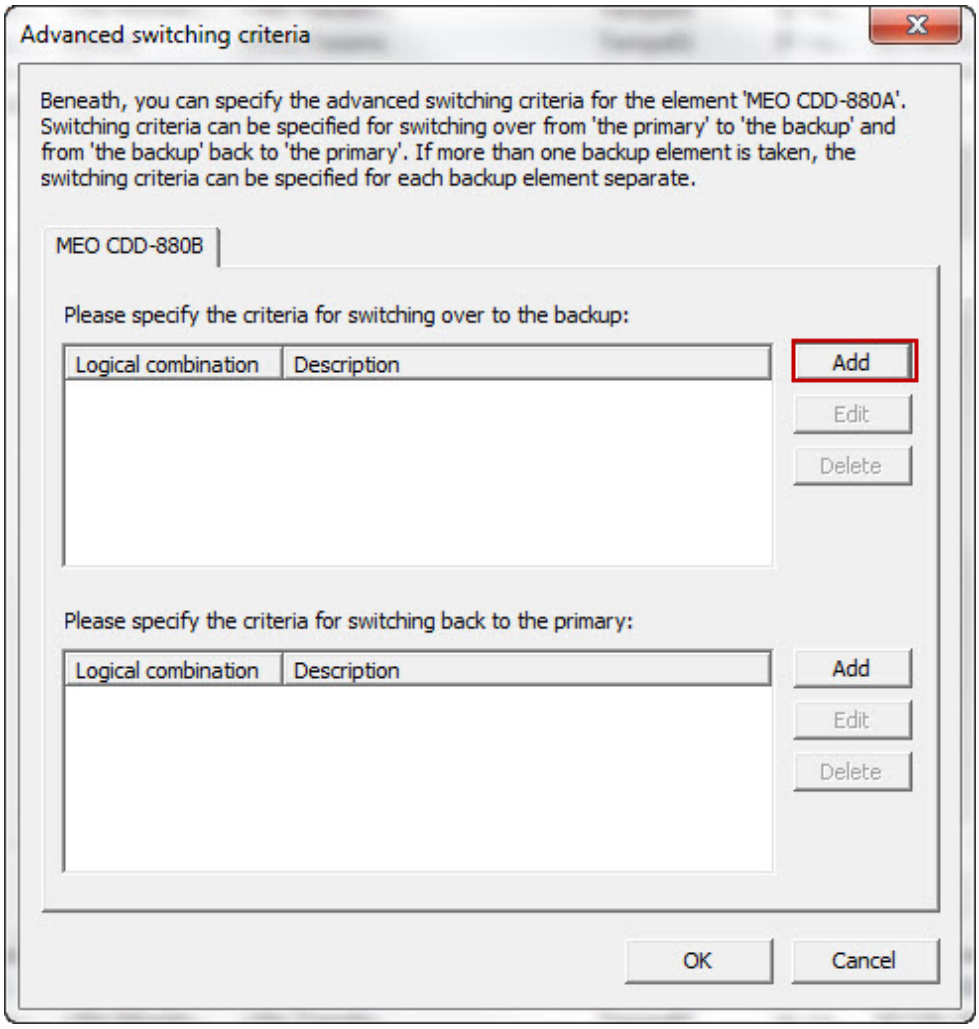


Figure G-38. Advanced Switching Criteria

25. Set up the criteria for switching to a backup element:
    a. Select **Parameter is changing.**
    b. Select <**ALL Primary**> from the **Element** list.
    c. Select **Rx1** from the **Parameter** list.
    d. Set **Equal** to **Demod Unlock.**
26. Click **OK.**

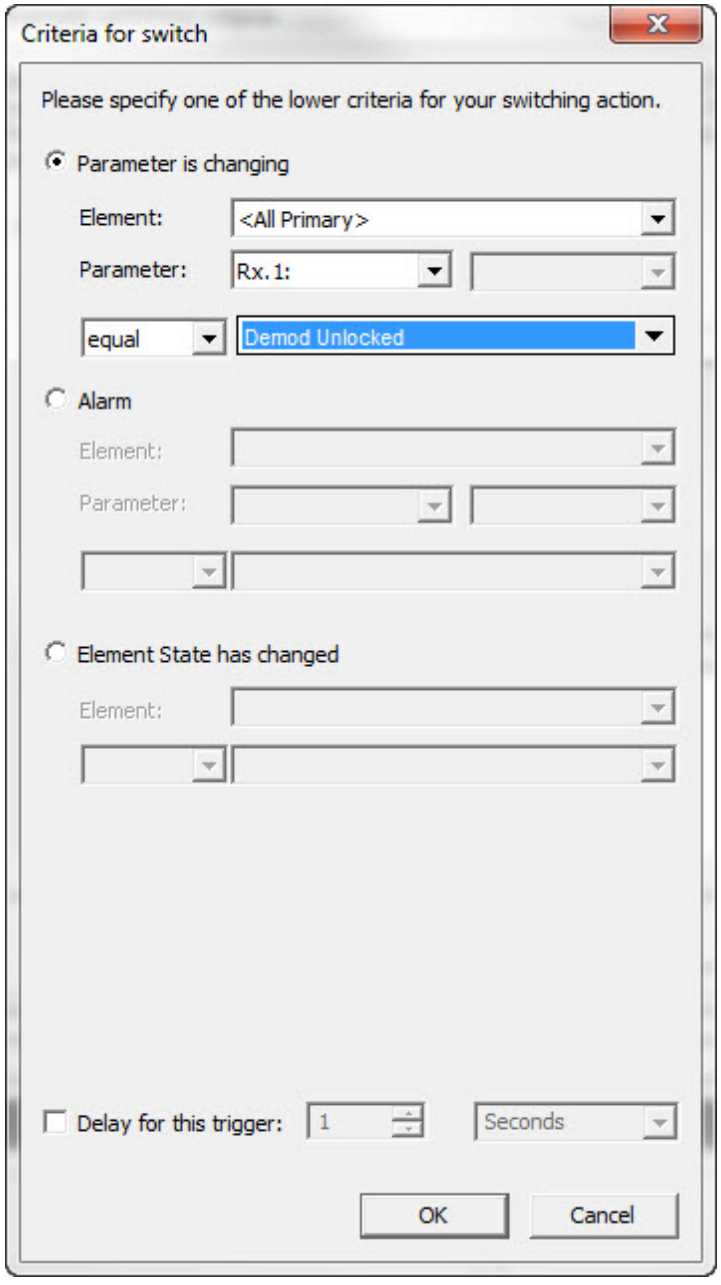


Figure G-39. Set Criteria for Switching to a Backup Element

27. Repeat these steps for all of the demods in use.

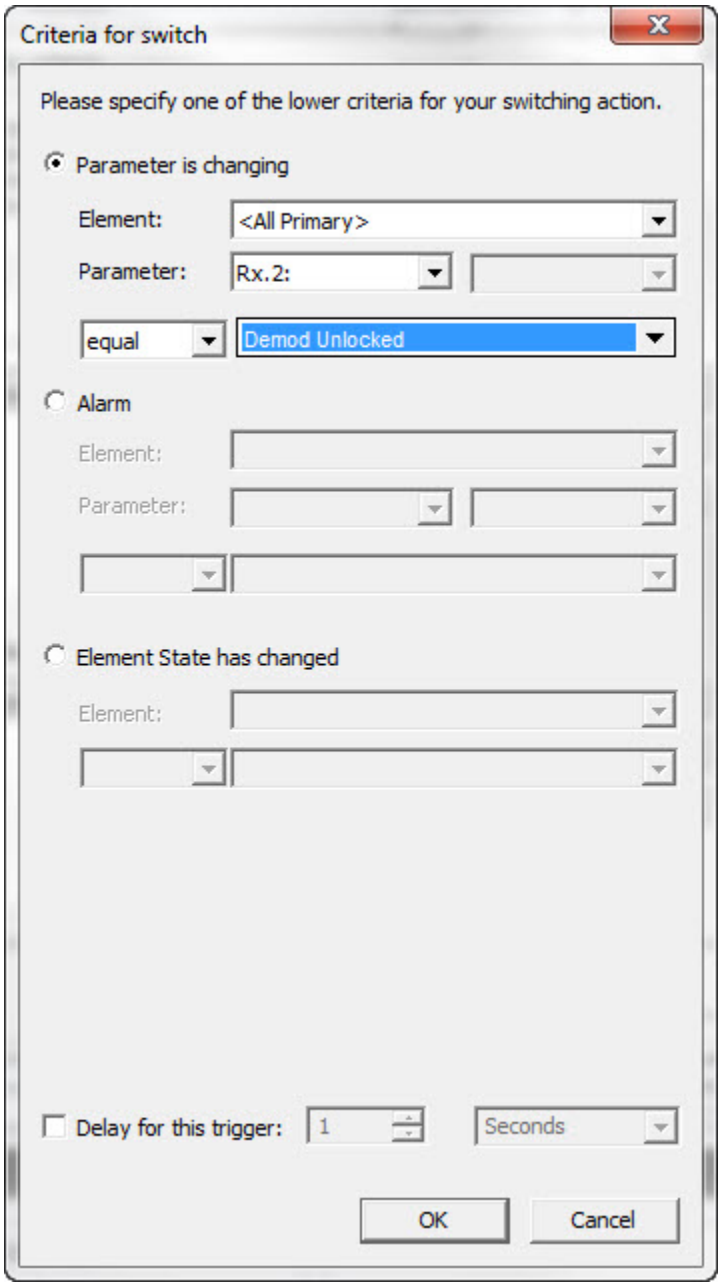


Figure G-40. Set Criteria for Switching (continued)

Set the parameters only for the demodulators actually used by the CDD880.

28. After all the criteria for switching to back up have been added, make sure to add a logical operator of **AND**.

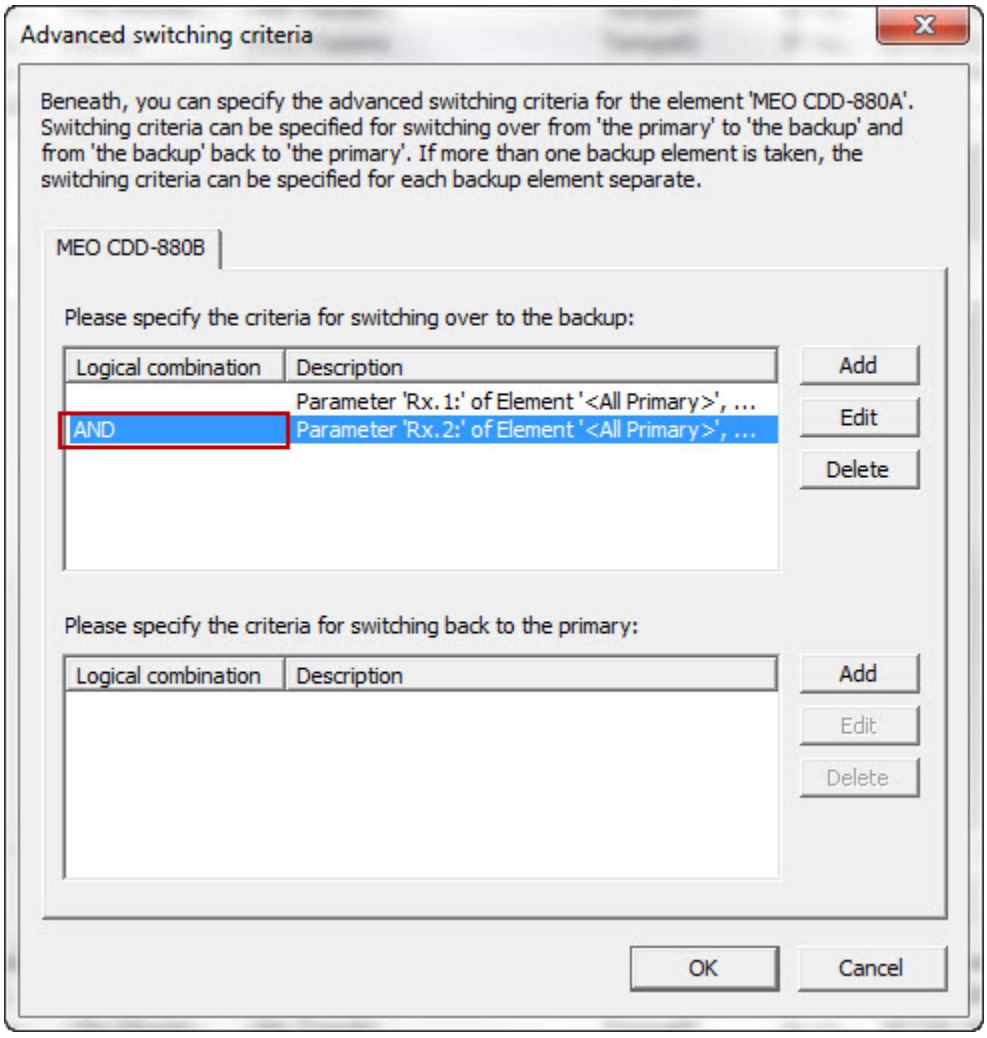


Figure G-41. Add Logical Operator AND

29. Specify the criteria for switching back to the primary.
30. Click **Add** next to that table.

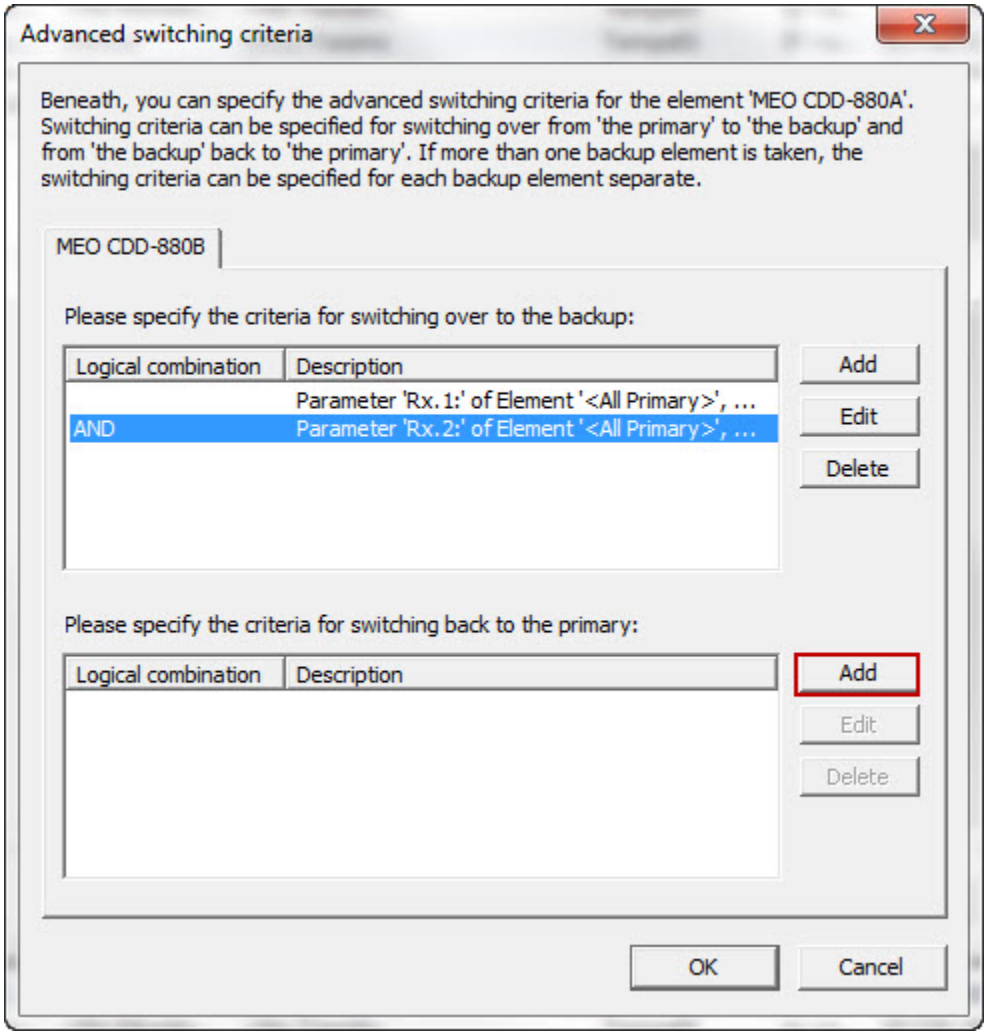


Figure G-42. Add the Criteria for Switching Back to the Primary

31. Set up the criteria for switching back to the primary element:
    a. Select **Parameter is changing.**
    b. Select <**ALL Backup**> from the **Element** list.
    c. Select **Rx1** from the **Parameter** list.
    d. Set **Equal** to **Demod Unlock.**
32. Click **OK.**

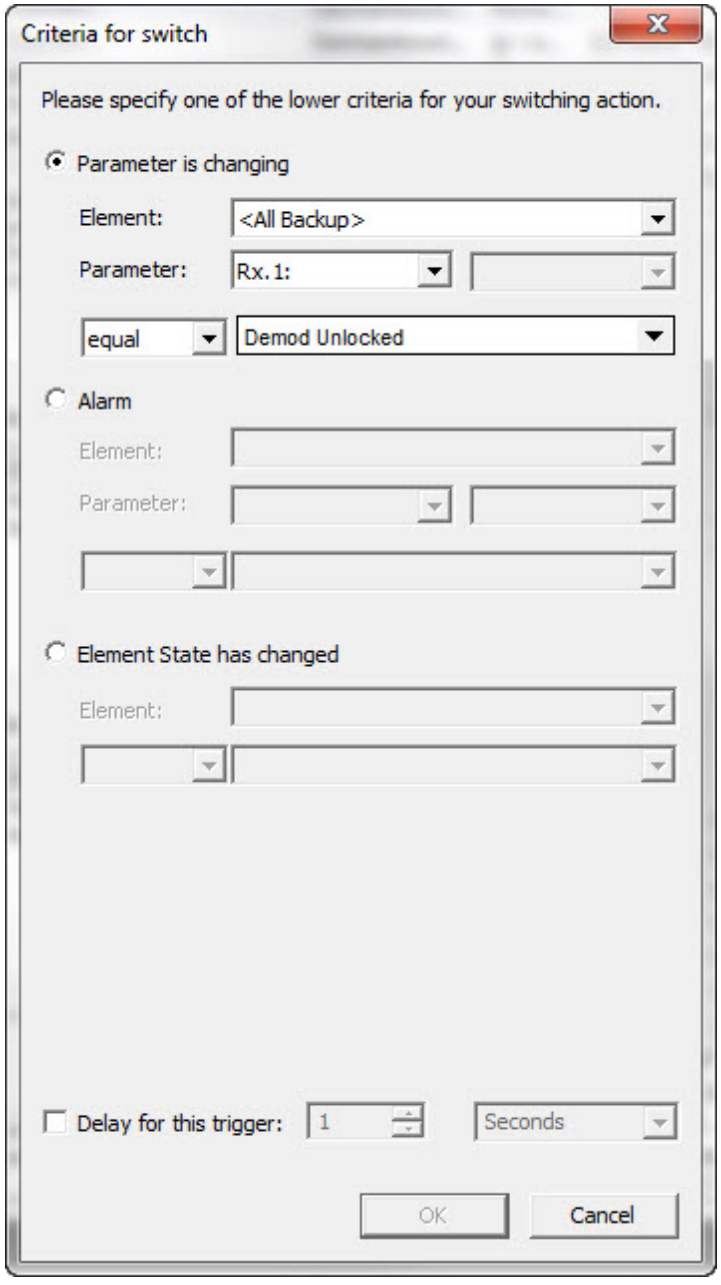


Figure G-43. Specify the Criteria for Switching Back to the Primary

33. Repeat these steps for all of the demods in use.

Set the parameters only for the demodulators actually used by the CDD880.

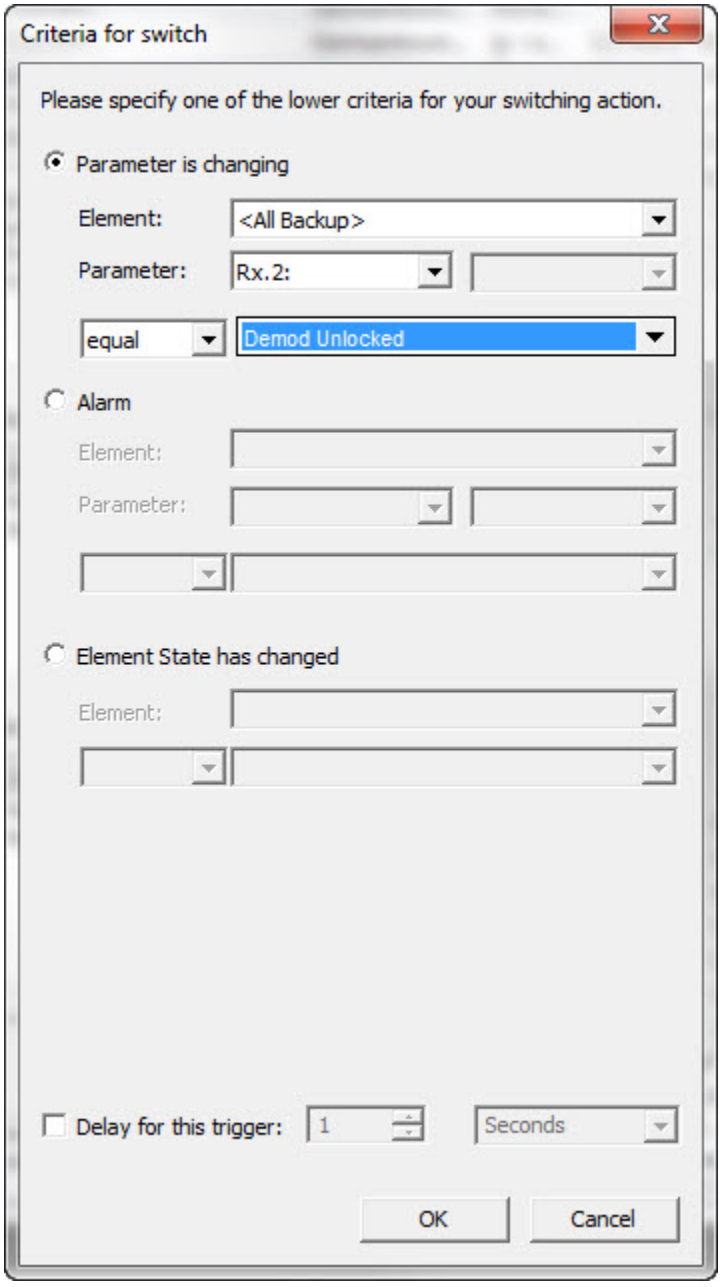


Figure G-44. Set Criteria for Switching to Primary (continued)

34. After all the criteria for switching back to the primary element have been added, make sure to add a logical operator of **AND**.

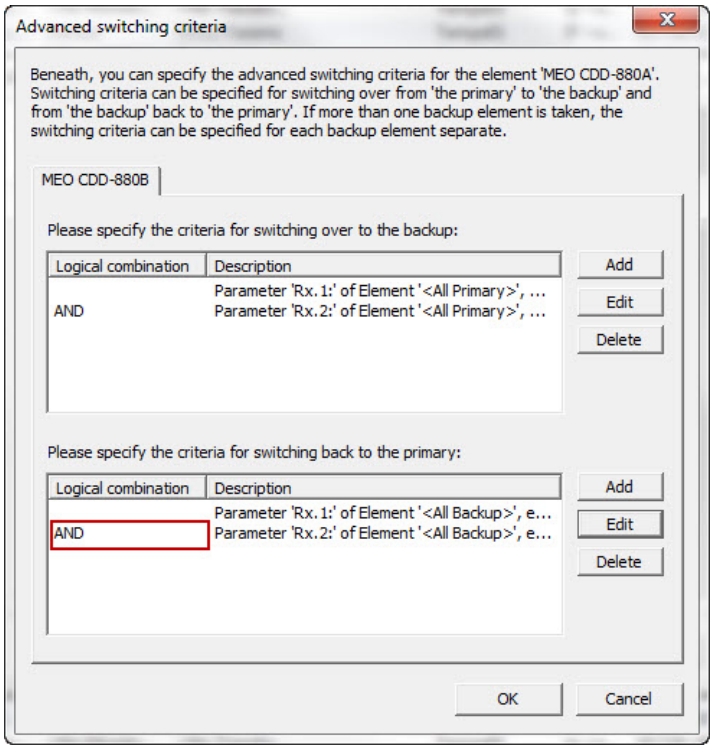


Figure G-45. Add Logical Operator AND

35. Click **Next.**

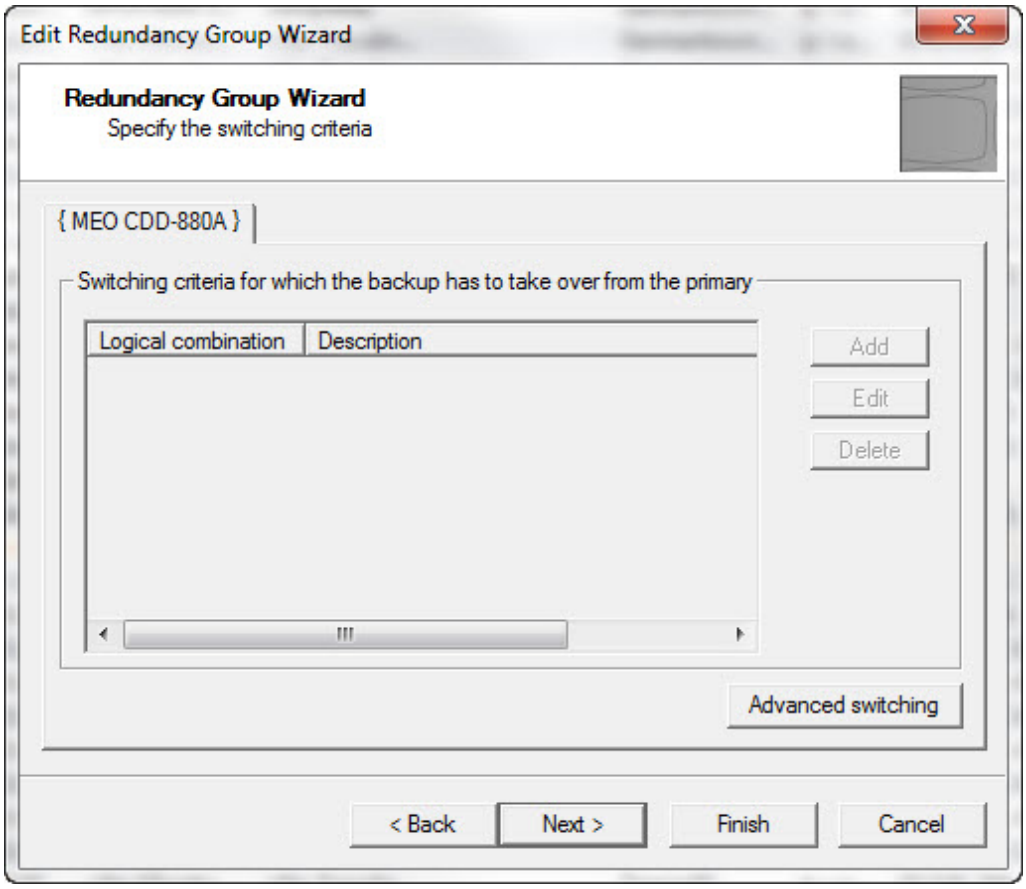


Figure G-46. Advanced Switching Criteria (continued)

36. Put the Redundancy Group into the correct view.

If necessary, you can move the redundancy group later.

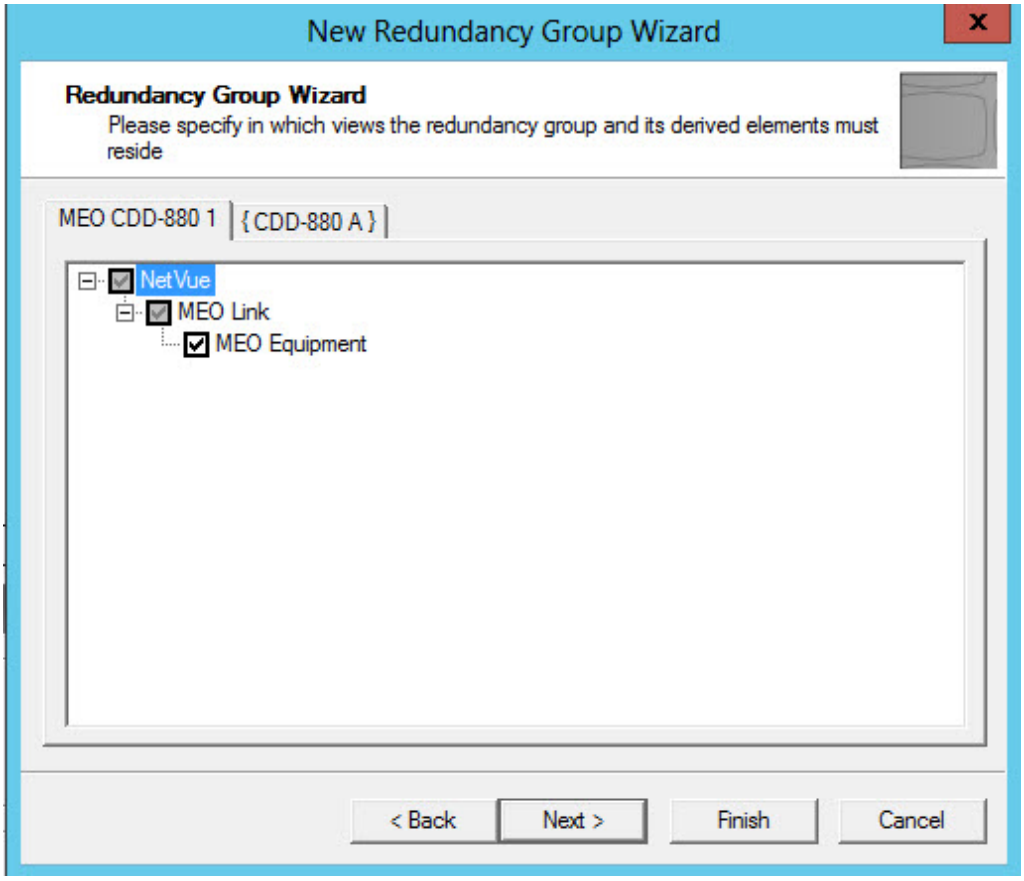


Figure G-47. Redundancy Group Placement

37. Click **Finish.**

G.7 Link Elements to Circuit View

As with an HNO, a VNO can request access to see the overall health and status of the unit.

However, a method of linking the redundancy groups to the circuit view is not included during provisioning a circuit. This section explains how to link the derived elements created in earlier steps to a circuit, so that the VNO is able to see only the active online unit. This prevents the VNO from making changes to the offline units, and possibly causing a service interruption.

The HNO can see the health of all units, including those that are offline. Access is given per View. Create a new view if a CTOG is occupied by multiple tenants.

G.8 Link Elements

1. Log in to NetVue Cube with an account that has the rights to modify the surveyor tree.

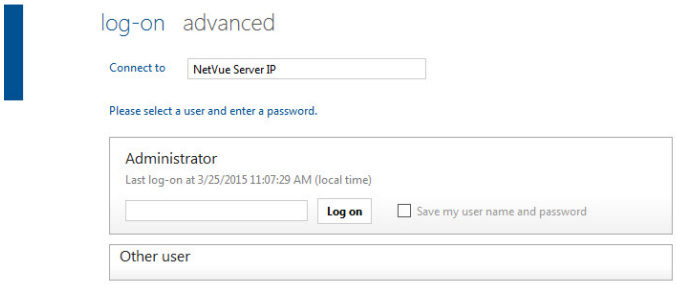


Figure G-48. Log-on Tab

2. Find the derived elements for the CDD880 and CDM840s in the Surveyor Tree.

   By default, these are indicated by {Unit Label}. However, during the redundancy group process, you can remove the brackets { }.

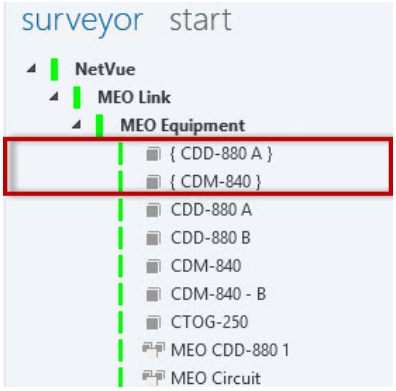


Figure G-49. Find the Derived Elements

3. Right click the **Element** and Click **Properties.**

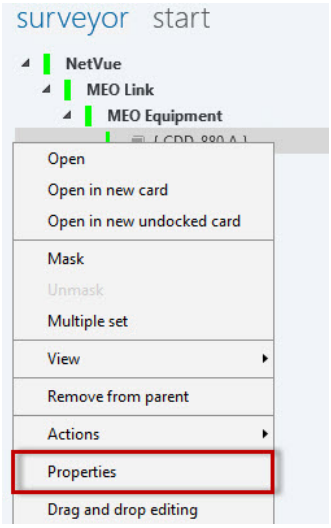


Figure G-50. Select Properties

4. Find the DMA ID/Element **ID.**
5. Highlight the ID and copy it to the clipboard.

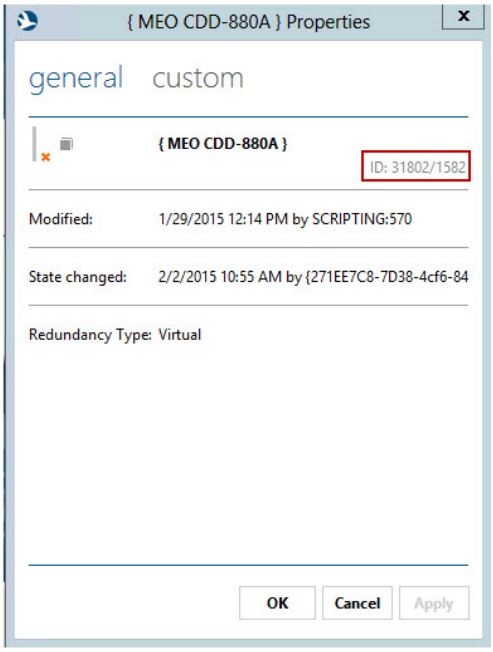


Figure G-51. Copy the ID

6. Right click the **Circuit** (identified by the two cubes interconnected icon).
7. Select **Properties.**

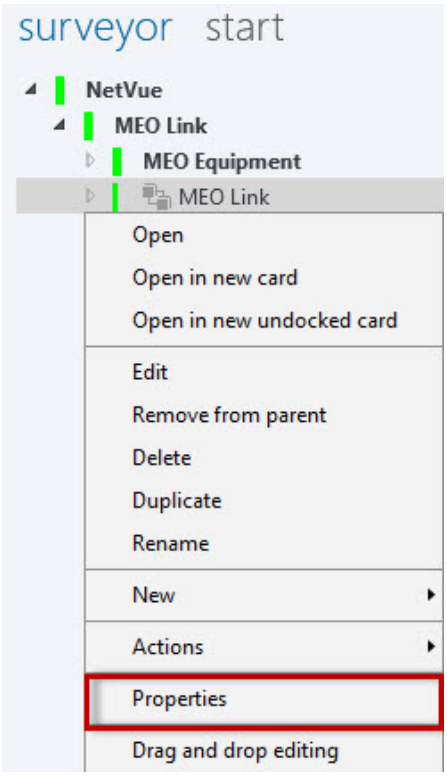


Figure G-52. Select Properties

8. Click the **Custom** tab.

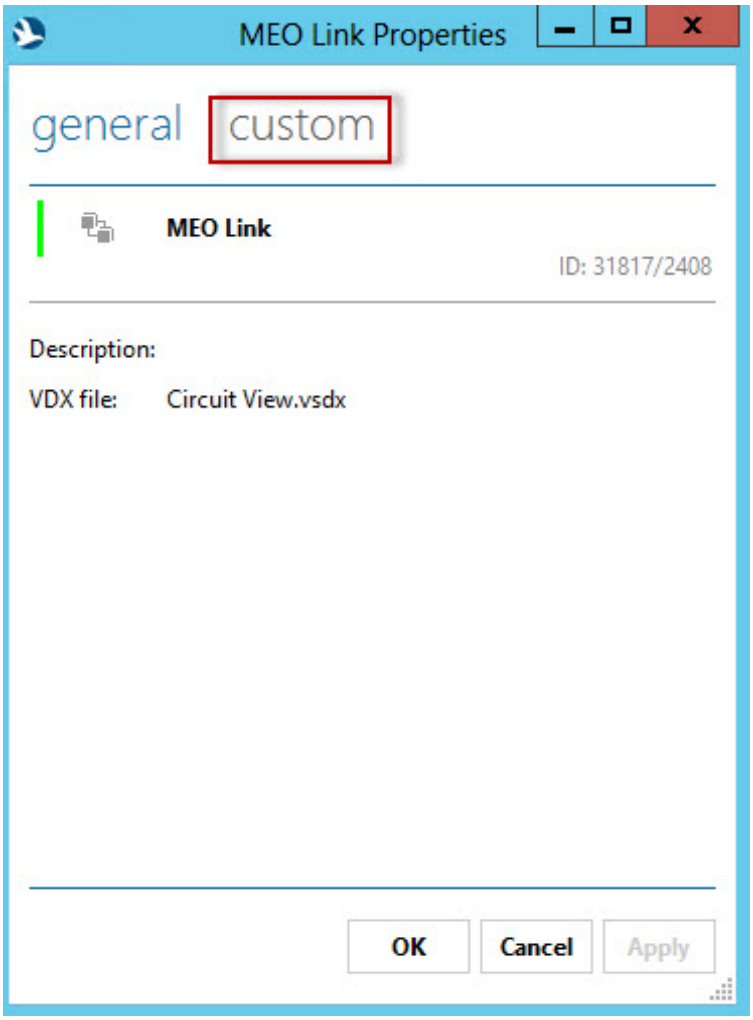


Figure G-53. Custom Tab

9. Find the CEFD CDD-880 SNMP_B and CEFD CDM-840 **Properties.**

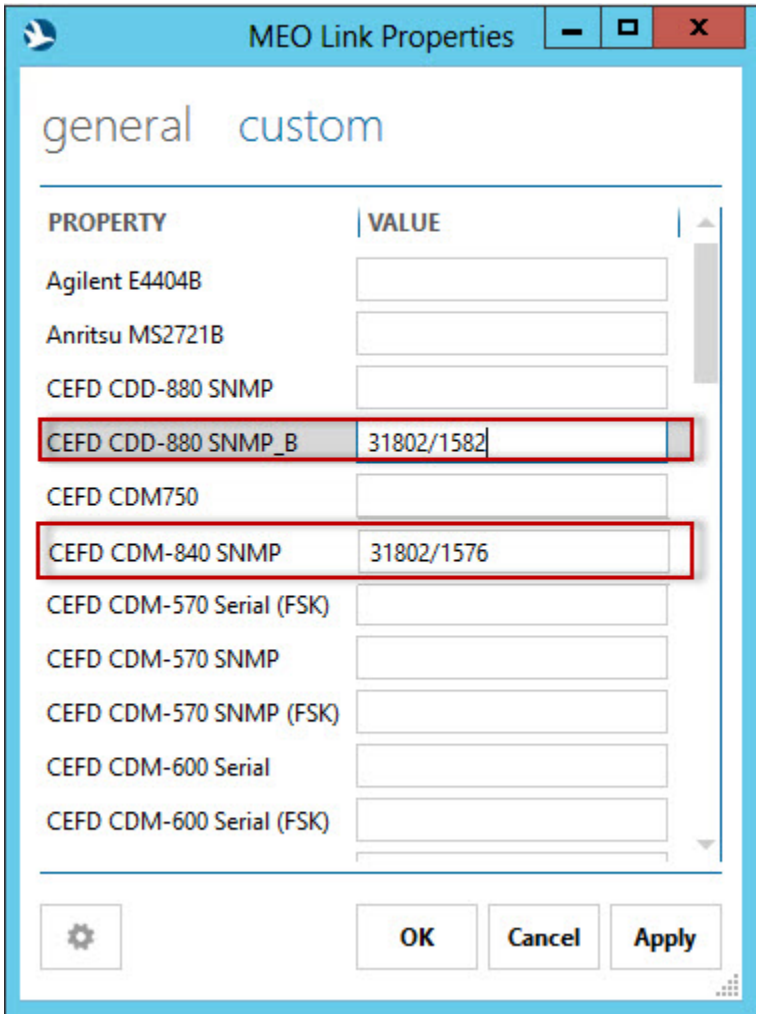


Figure G-54. Find the Properties

10. Replace the existing values with the DMA ID/Element IDs of the derived element.

You must put the CDD-880 Value into CEFD CDD-880 SNMP_B.

If you do not see the property, you must add it by clicking the gear icon:

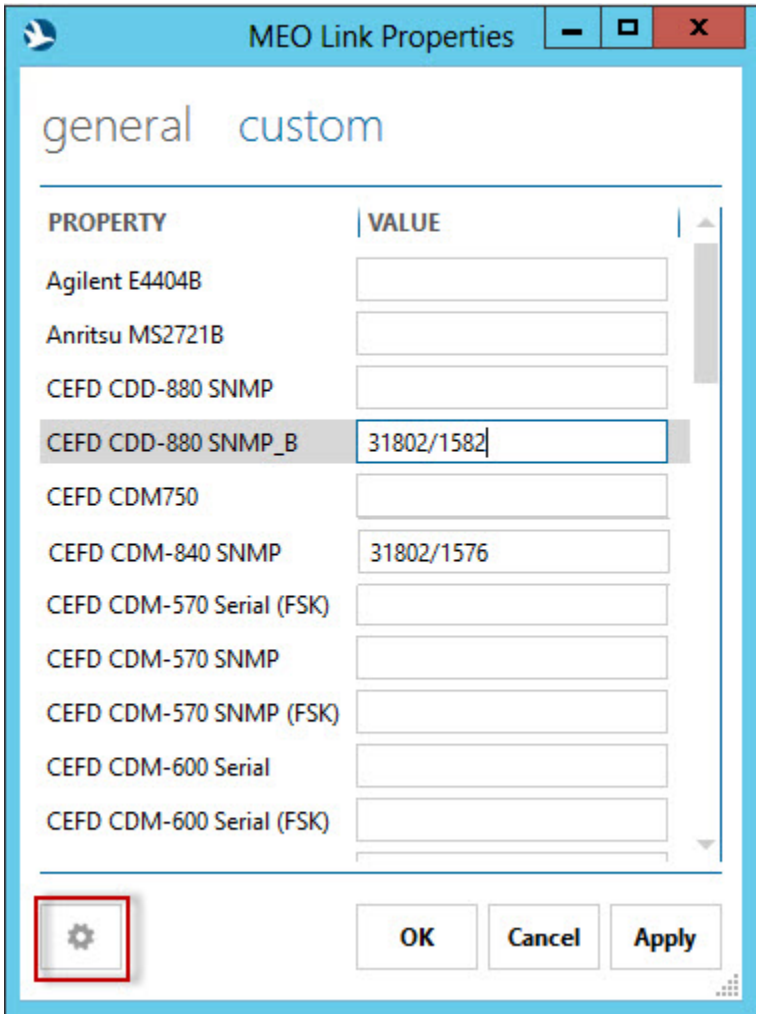


Figure G-55. Gear Icon to Add a Property

11. Click **Add.**

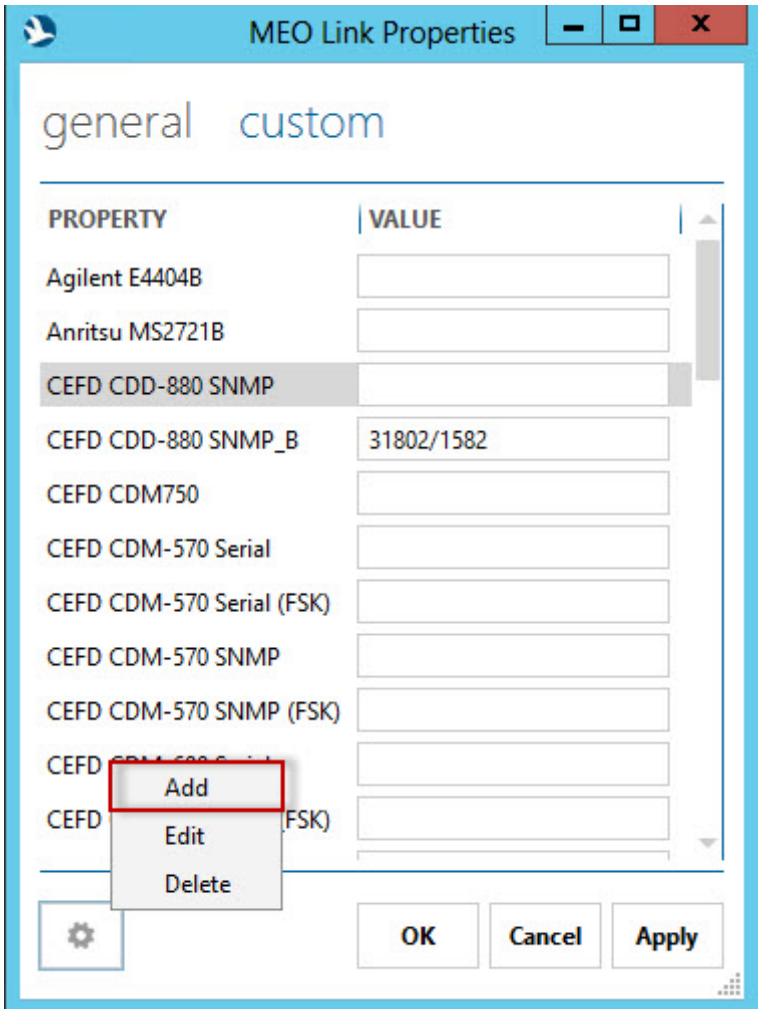


Figure G-56. Add a Property

12. In the **Edit** window, make sure the **Name** is either **CEFD CDM-840 SNMP** or **CEFD CDD-880 SNMP_B.**

    You can leave all other values at their default settings.

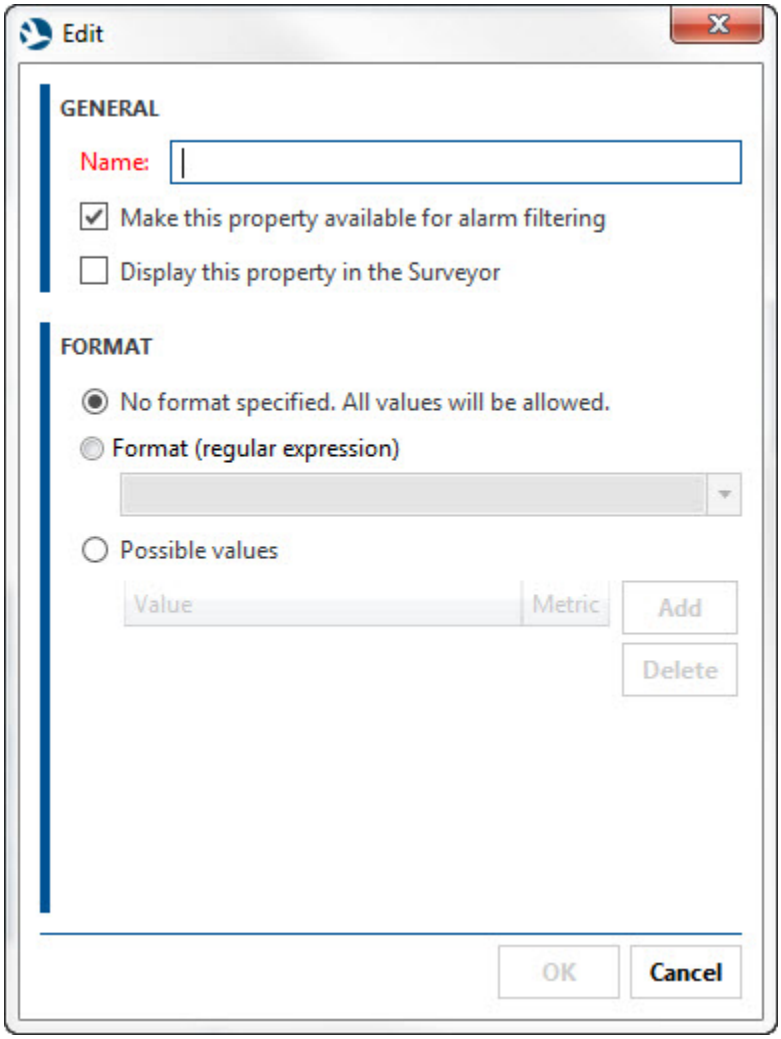


Figure G-57. Edit the Property Name

G.9 Customizing Circuits

This section tells how to customize a circuit so that the VNO can see the health status of the online unit only.

If you want to let the VNO see the health status of both units, skip this section.

1. Log in to NetVue Cube.
2. Find the MEO Circuit in the **surveyor** tab.

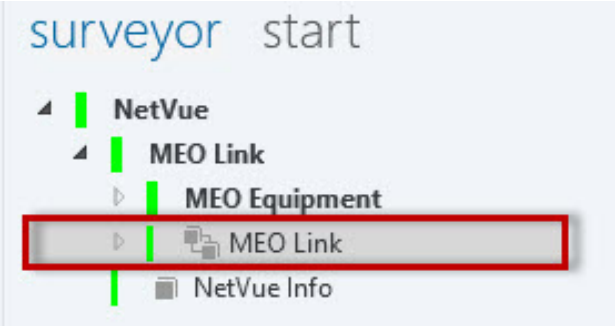


Figure G-58. Find the MEO Circuit

3. Right click the **Circuit**.
4. Select **Edit**.

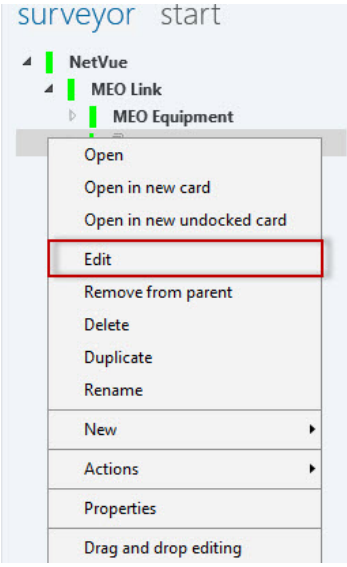


Figure G-59. Edit the Circuit

5. Select the **elements** tab.

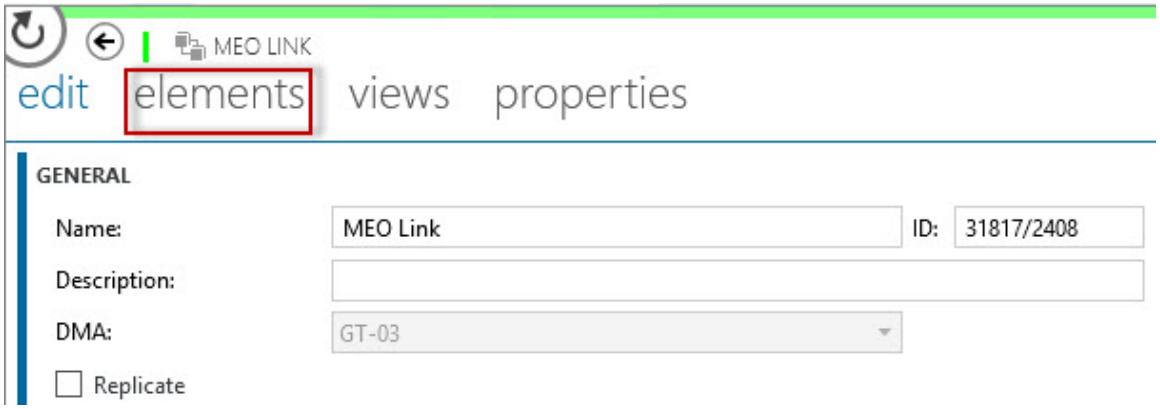


Figure G-60. Elements Tab

6. Find the CDD-880A and B, and the CDM-840 A and B.
7. To delete these elements, click the blue X next to each element.

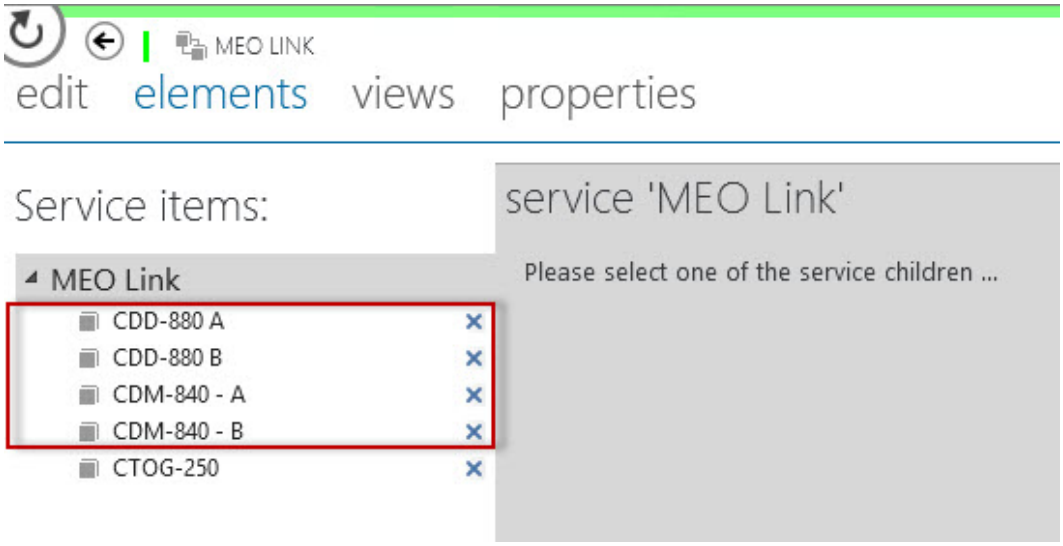


Figure G-61. Find the Elements to be Deleted

8. Click **Add Element**.

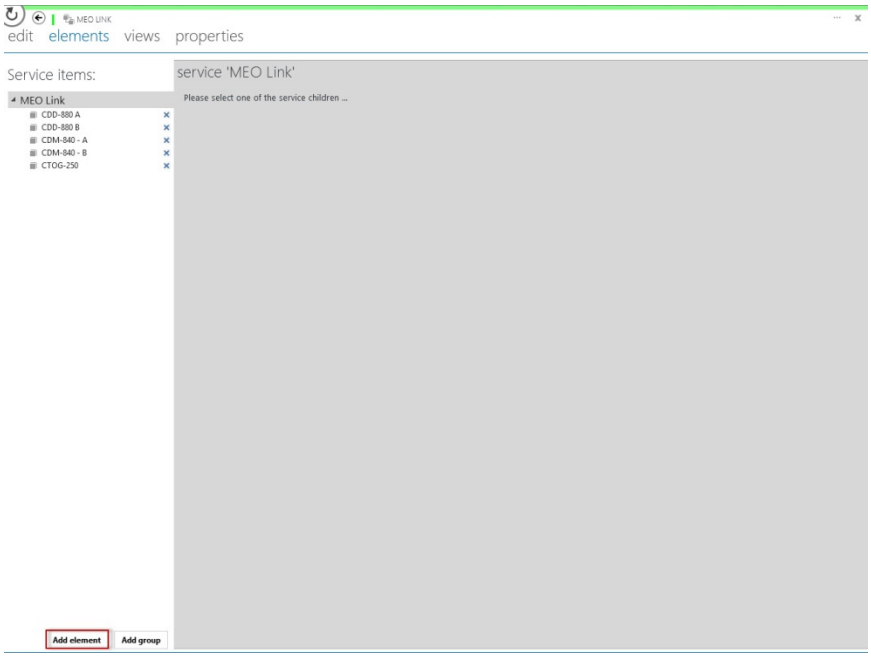


Figure G-62. Add Element Button

9. Select the derived elements.
10. Click **Add.**

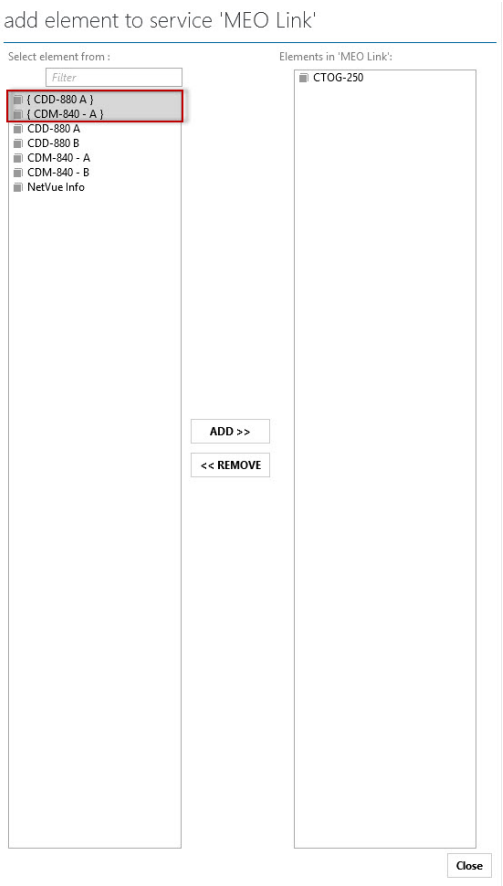


Figure G-63. Add Elements

11. Make sure the elements are included in the Circuit.
12. Click **Close.**

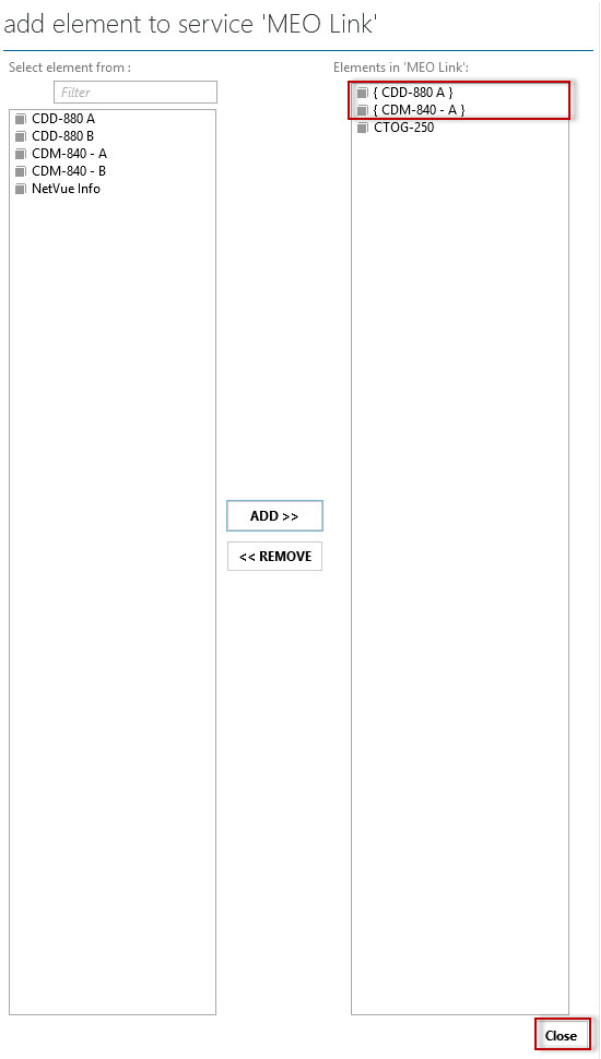


Figure G-64. Verify Elements in Circuit

The MEO link should be set up and polling. It switches dynamically between the online and offline equipment based on the criteria you set up using the steps in the previous sections.

Appendix H. NETVUE NORTHBOUND INTERFACES (NBI)

H.1 Northbound Interfaces

NetVue gives the ability to promote information outside the NetVue operational environment. NetVue can do the command, control and monitoring for Comtech EF Data's product family; however, you can operate NetVue as a slaved device, and have the information gathered by NetVue promoted up to a Manager of Managers (MOM).

To interface with a MOM, a machine interface must provide the common structure between the NetVue and the MOM. The Northbound Interface (NBI) is the interface between the NetVue and the MOM. Figure H-1 shows NetVue's architecture, and the many methods of supporting an NBI. For specifics on the NBI configuration, please contact the Comtech EF Data Engineering Support Center (ESC) or your program manager.

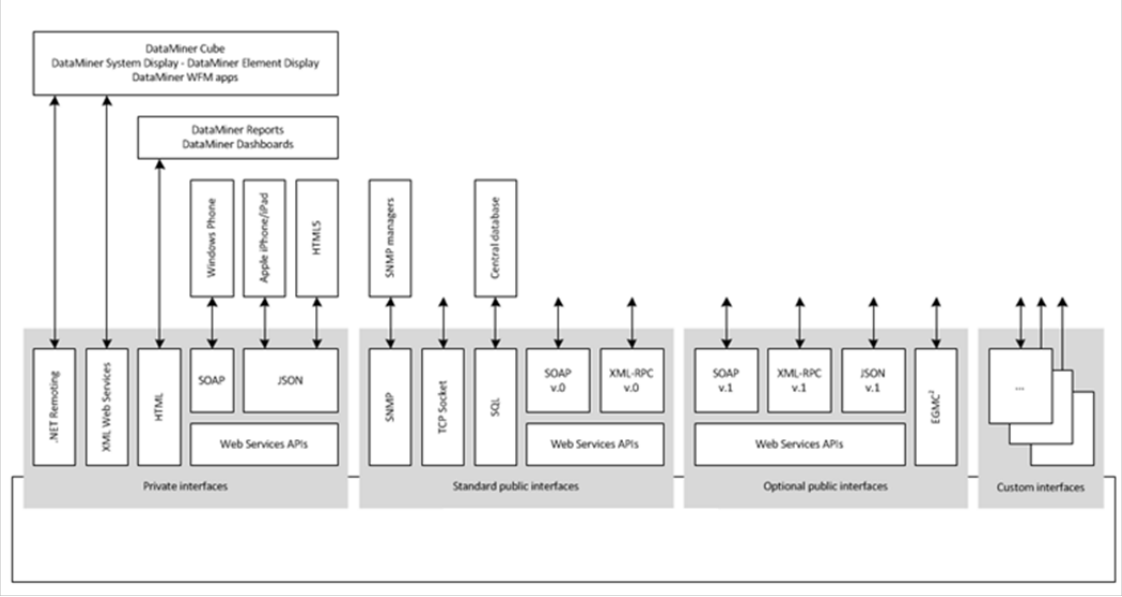


Figure H-1. NetVue Architecture

NetVue NBIs include:

- Private Interfaces
- Standard Public Interfaces
- Optional Public Interfaces
- Custom Interfaces

H.1.1 Private Interfaces

NetVue ships with several private interfaces to connect to the standard NetVue client applications.

Standard NetVue web clients (connecting via .NET Remoting or XML Web Services)

- NetVue Cube
- NetVue System Display
- NetVue Element Display

H.1.2 Standard Public Interfaces

By default, every NetVue System has several standard public interfaces that allow:

- Forwarding of SNMP traps to third-party SNMP managers (HP OpenView and IBM NetCool)
- Performing SNMP Get and SNMP Set requests on individual controls and readings of devices
- Exchange of information via TCP-IP sockets
- Offload of database records via SQL
- Web Services APIs (SOAP XML, XML-RPC)

H.1.3 Optional Public Interfaces

Optionally, a NetVue System can be configured to connect to third-party applications via:

- Web Services APIs (SOAP XML, XML-RPC, JSON)
- EGMC2

H.1.4 Custom Interfaces

In addition to the available private and public interfaces, highly specialized custom interfaces can be developed to allow a NetVue System to integrate seamlessly into an existing infrastructure.

Appendix I. SERVER SOFTWARE UPGRADE AND RECOVERY

I.1 Upgrade NetVue Agent

You can upgrade NetVue Agents from the NetVue Taskbar Utility or from System Center. Both methods use an archive file called a NetVue package to complete upgrades. Depending on the type of upgrade, an Upgrade package or Application package is used during the upgrade operation.

- Upgrade packages (file extension .**dmupgrade**) upgrade a NetVue Agent to a new version.
- Application packages (file extension .**dmapp**) install a NetVue app on an existing NetVue System.

The remainder of this chapter describes instructions for managing upgrades from the NetVue Taskbar Utility and from System Center.

I.1.1 Upgrade Using NetVue Taskbar Utility

This section will guide you through the process of upgrading to a new version using the NetVue Taskbar Utility.

I.1.1.1 Test the User Credentials

Before starting the upgrade, make sure you are using NetVue user credentials with sufficient access to all NetVue Agents in the NetVue System. Do these steps:

1. In one of the NetVue system trays, right-click the NetVue Taskbar Utility icon.
2. Select **Options**.
3. Select the **slnet** tab.
4. Enter the user credentials.
5. Click on **Test & Save Connection**.
   If successful, an information prompt shows this message: **Connection with SLNet was successful**.

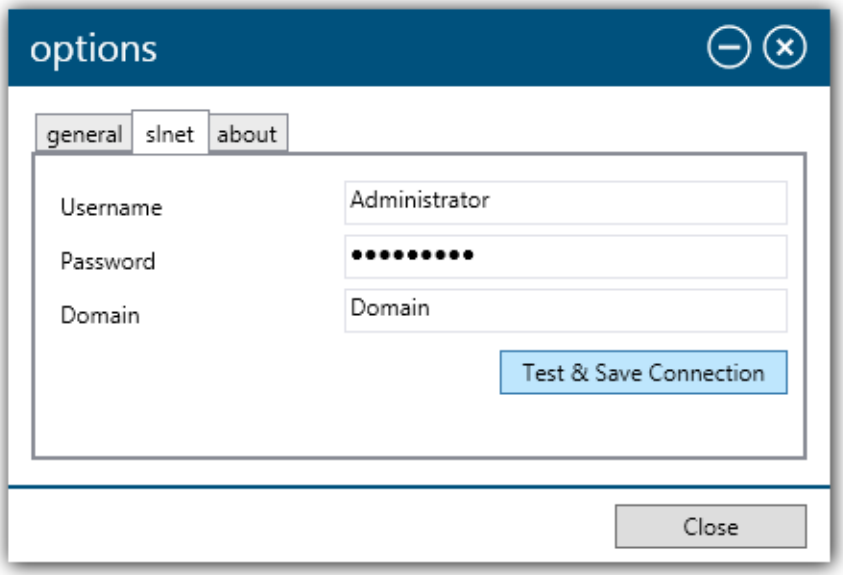


Figure I-1. Credential Entry

I.1.1.2 Upgrade Using the NetVue Taskbar Utility

After you enter the applicable user credentials, upgrade your NetVue Agent(s) to a new version:

1. In the Windows task bar, right-click on the **NetVue Taskbar Utility** icon and click **Upgrade**.
2. To the right of the **Package** box, click the ellipsis button **...**
3. Select the NetVue upgrade package, file extension .**dmupgrade**.
4. To the right of the **Agents to upgrade** box, click **Change**.
5. Select the NetVue Agents to be upgraded.
6. Expand the **Options** section and select the necessary upgrade options.
7. Click **Upgrade** to start the upgrade procedure.
8. Wait until the upgrade has finished. This can take several minutes, depending on the network properties and the type of upgrade.
9. When all NetVue Agents have successfully been upgraded, click **Finished**.

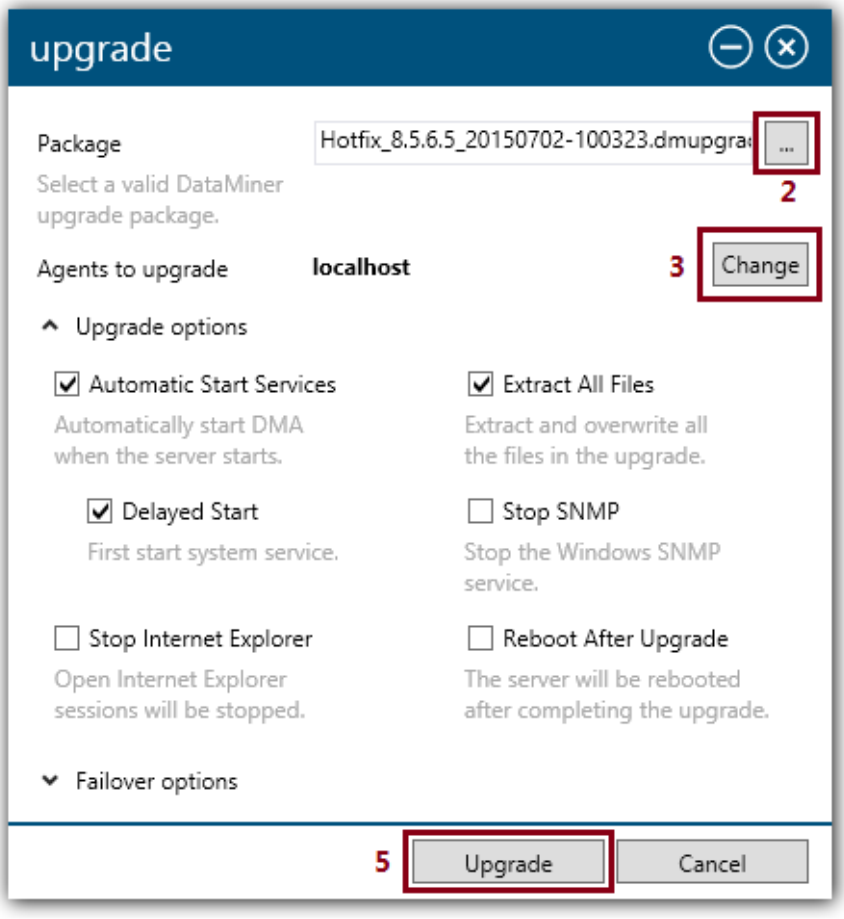


Figure I-2. Taskbar Utility Upgrade

I.1.2 Upgrade in System Center

This section will guide you through the process of upgrading to a new version in System Center.

1. Go to **Start > Apps > System Center > Agents**.
2. In the **Manage** tab, select the DMA you want to upgrade, or a DMA from the cluster you want to upgrade.
3. In the panel on the right, click the **Upgrade** button.
4. In the **Schedule** tab of the **Upgrade** window, under **Upgrade package**, select an upgrade package in one of these two ways:
    - Select **Available packages** and then select one of the available packages in the list.
    - Select **New package** and click the ellipsis button ... to select the NetVue upgrade package, file extension .**dmupgrade**.
5. Under **Upgrade DataMiner Agents**, select which **Agents** to upgrade:
    - To upgrade the entire cluster, select **All Agents in cluster**.
    - To upgrade one or more individual Agents, select **Individual Agents** and expand the **NetVue Agents** section to select the **Agents,** or add them by entering an external IP.
6. Expand the **Advanced upgrade options** section and select the necessary upgrade options.
7. For Agents in a failover setup:
    - Open the section **Advanced failover options**.
    - Select the failover policy, which sets the order in which the DMAs are upgraded.
8. Click **Upgrade** to start the upgrade procedure.

The upgrade process can take several minutes, depending on the network properties and the type of upgrade. You can follow the update's progress in the **Progress** tab.

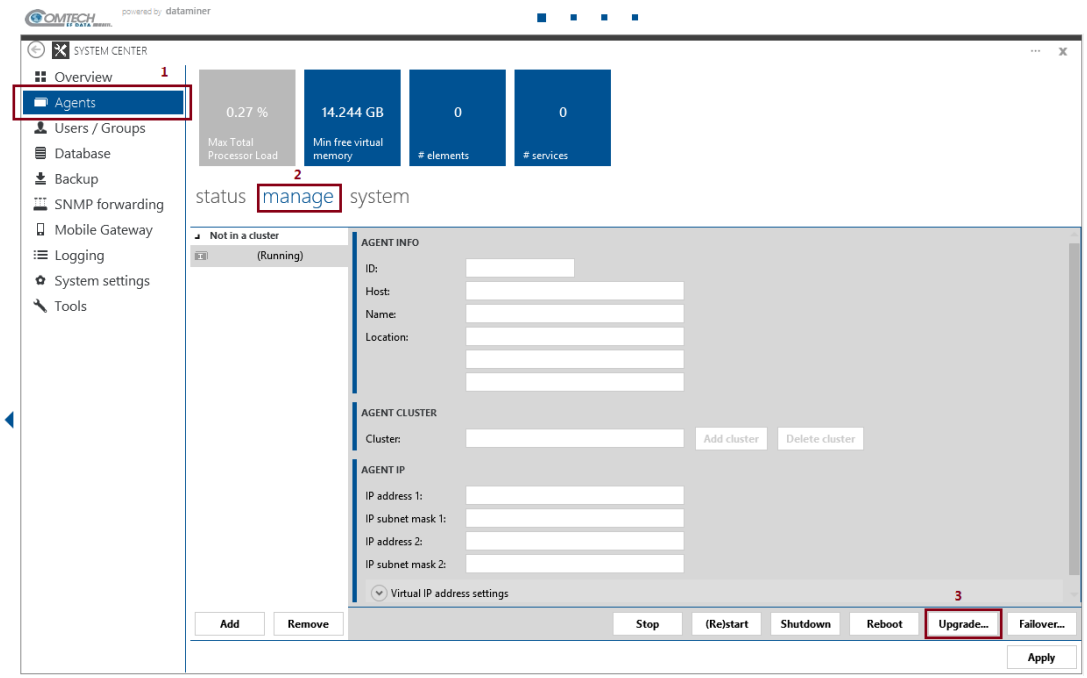


Figure I-3. Open Upgrade Dialog

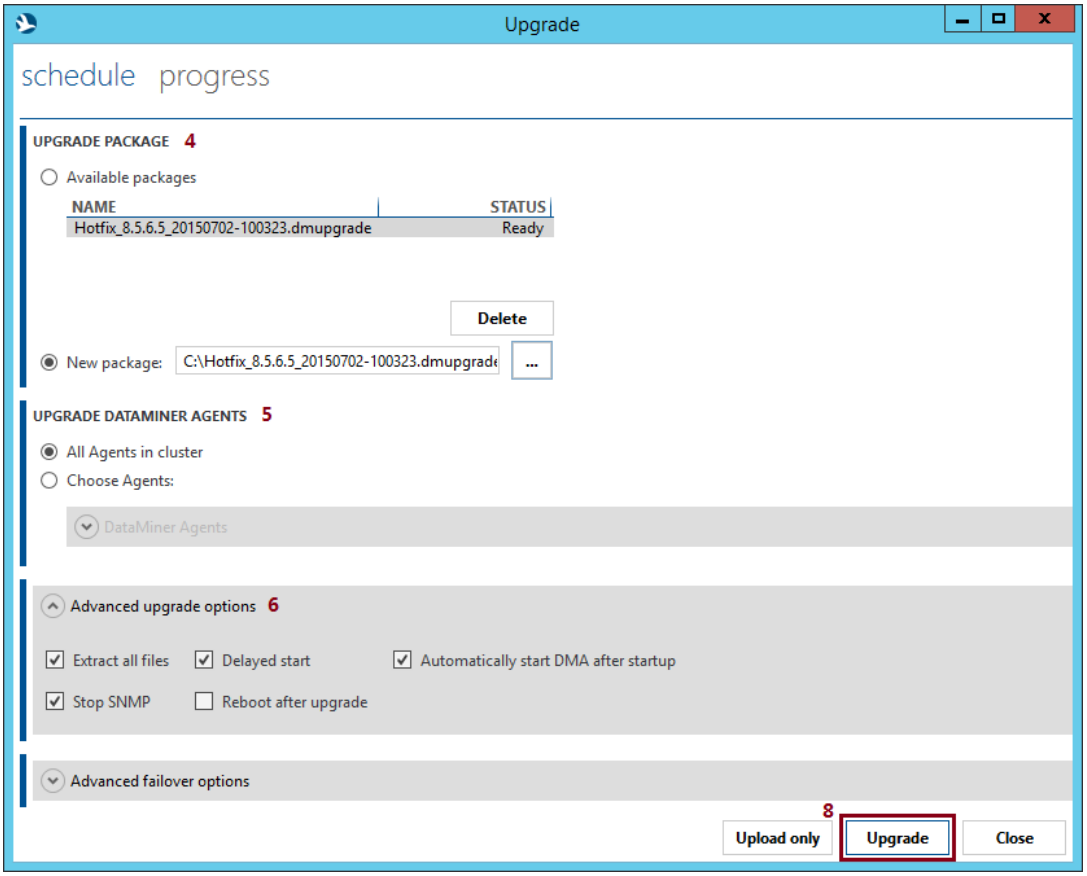


Figure I-4. Upgrade NetVue Agent(s)

I.2 NetVue Agent Recovery

You can restore a NetVue Agent from a Backup package or, roll back an upgrade from a rollback package. These sections will guide you through restoring a NetVue Agent from a Backup package and rolling back a NetVue upgrade.

I.2.1 Restoring from a Backup Package

Backup packages (file extension .**dmbackup**) are created by scheduled processes, or manually created by a user. With an existing Backup package, do these steps to restore a NetVue Agent.

1. In the Windows task bar, right-click the **NetVue Taskbar Utility** icon and click **Backup/Restore** > **Restore**.
2. In the restore window, click the **...** button to select a backup package. A description of the contents of the package shows under **Description**.
3. Click **Restore** to start restoring the DMA.
4. The different steps of the restoration process show in the **restore** window.

During the restoration process, all open Internet Explorer windows are closed.

5. When the restoration is complete, click **Finished**.

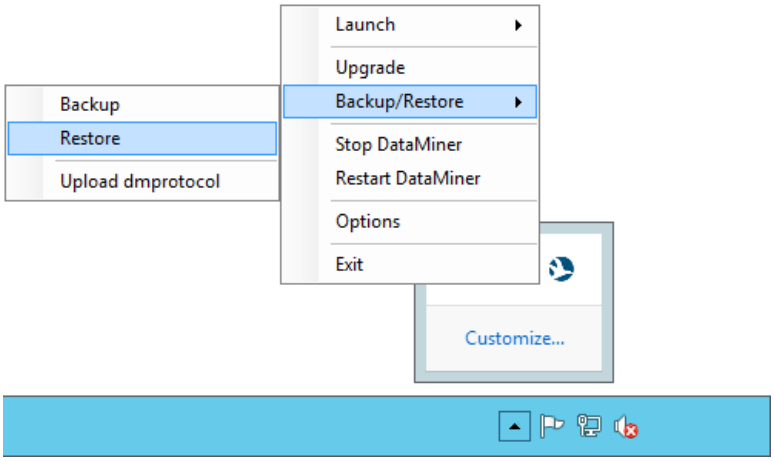


Figure I-5 Select Restore from Taskbar Utility

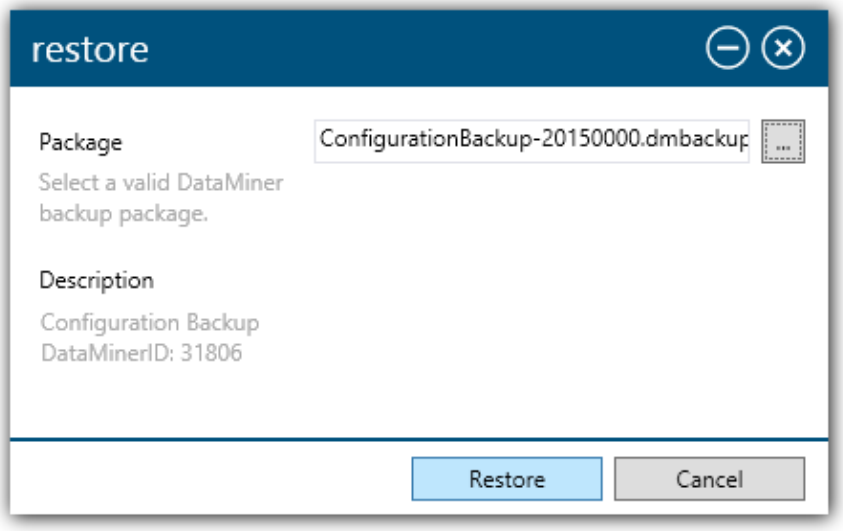


Figure I-6. Restore Backup

I.2.2 NetVue Agent Upgrade Rollback

By default, a rollback package is created when a NetVue upgrade is performed. These rollback packages (file extension .**zip**) contain all files that were replaced during the upgrade. Do these steps to roll back a NetVue upgrade:

1. Stop the NetVue Agent.
2. Unpack the desired rollback package using **StandaloneUpgrde.exe** located in the directory: **C:\Skyline DataMiner\Tools**
3. From the toolbar, go to **File** > **Open** to select the rollback zip file.
4. The most recent rollback package is named **Upgrade_Rollback Most Recent.zip** and is located in the directory: **C:\Skyline DataMiner\Tools**
5. Previous rollback packages are stored in the directory: **C:\Skyline DataMiner\Upgrades**. These files have the name structure of **Rollback_YYYY_MM_DD_HH_MM_SS.zip**.
6. From the toolbar, go to **Upgrade** > **Start…** to start the roll back.

The rollback operation is complete when the terminal shows this message: **Upgrade completed on all specified agents (within cluster)**.

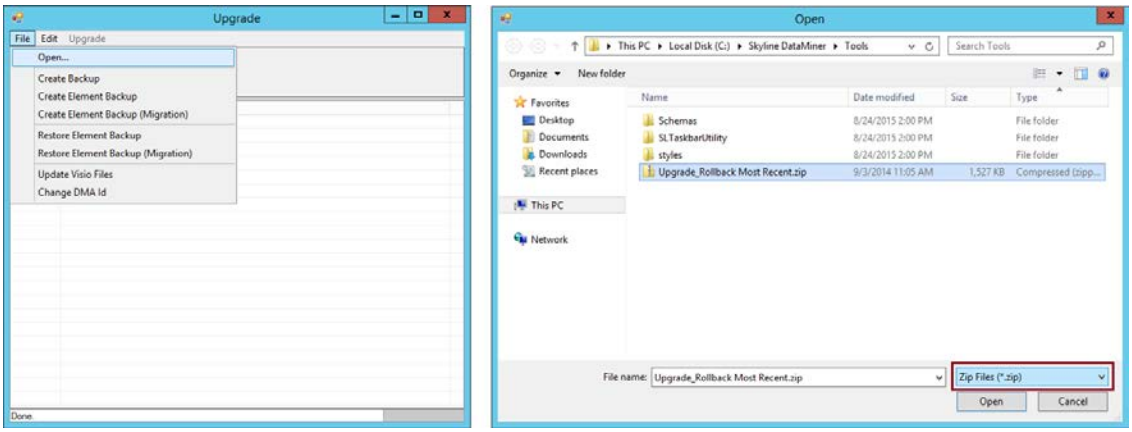


Figure I-7. Open Rollback Zip File

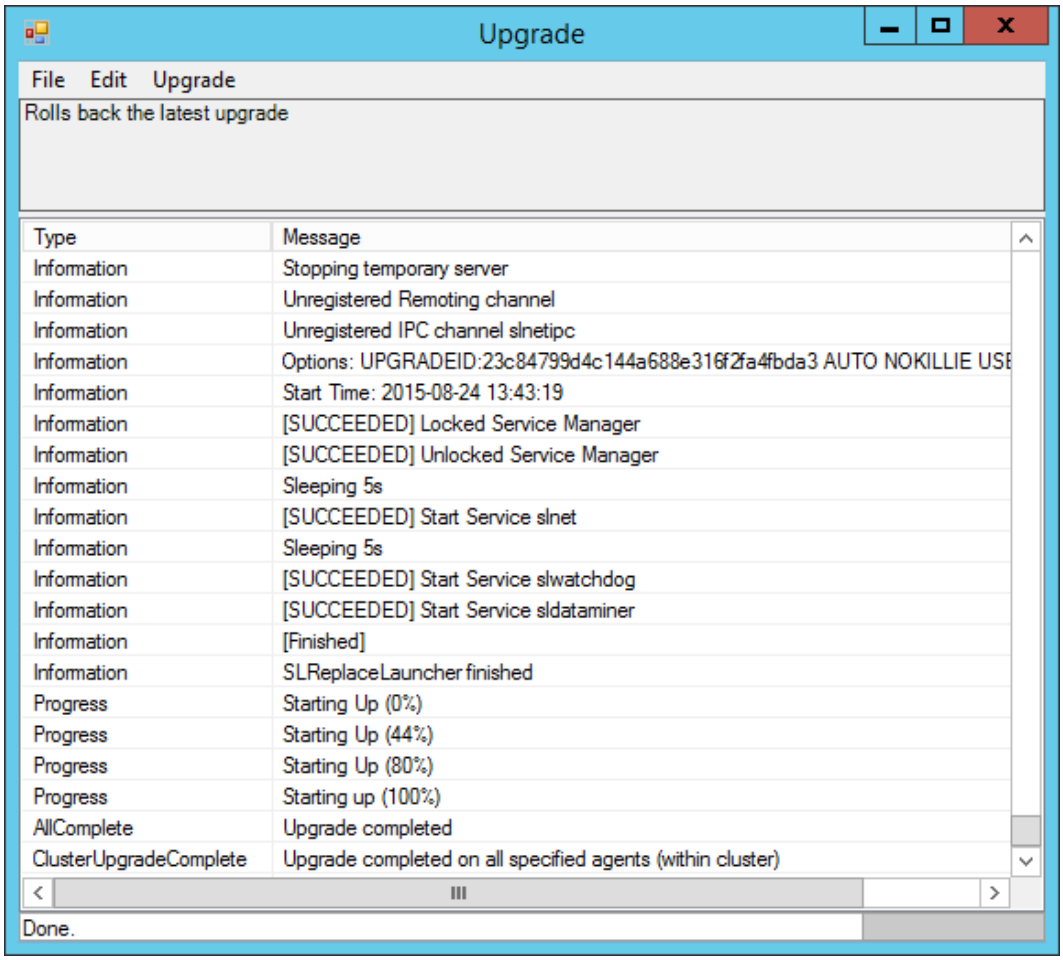


Figure I-8. Rollback Complete

Appendix J. MESH

J.1 Introduction

NetVue supports the configuration and monitoring of Mesh networks for the Heights product-line. To configure a network to use mesh the following steps are required:

- Configure routes in the HRX-16-R(s) for each remote in the mesh network and a route to the Bandwidth Manager.
- Configure the HRX-16-R(s) base Rx Frequency to match the hub HRX base Rx Frequency.
- Configure remote site external subnet(s).
- Assign remote site mesh demodulator(s) to the down-converter and set them allocatable.
- Create remote site distribution(s).

J.2 Configure HRX-16-R Routes

Each HRX-16-R in the Mesh network requires routes to all of the other remotes that are part of the mesh network. The HRX-16-R also requires a route to the NetVue/Bandwidth Manager in order to properly switch demodulators to the correct configurations. These routes use the associated remote's management IP as the next hop IP. And finally, there needs to be a default route created that sends traffic to the associated remote's traffic IP for host that are not on the same subnet as the HRX-16-R. To configure the routes, click on the device element(s) in the Network container and rotate the card and go to **Configuration – Network – Routing View**.

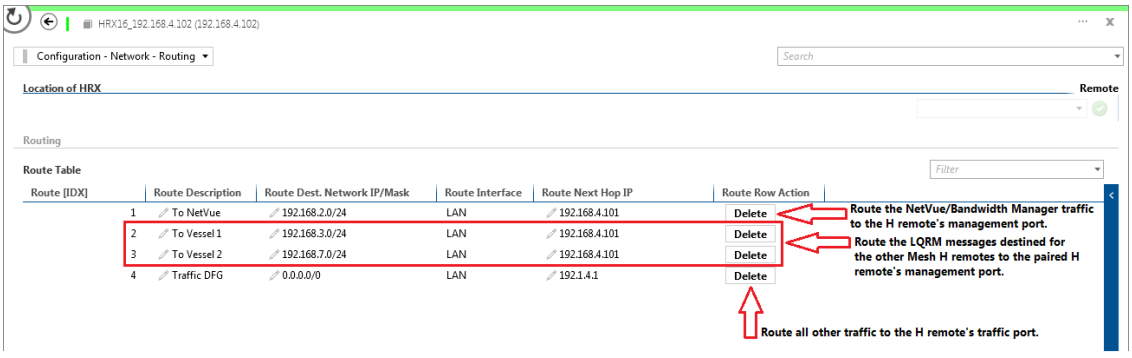


Figure J-1. HRX-16-R Mesh Routes

J.3 Configure HRX-16-R Base Rx Frequency

In order for the HRX-16-R's demodulators to be used in a mesh network, the Rx Frequency range must be compatible with the Hub's Rx Frequency range. The best way to ensure this compatibility is to configure the HRX-16-R's base Rx Frequency to match the Hub HRX's base Rx Frequency. Click on the Hub HRX device element in the Network container and rotate the card and select **Configuration – WAN – Demod View**. Make note of the Rx L-Band Frequency and use that frequency value for each HRX-16-R.

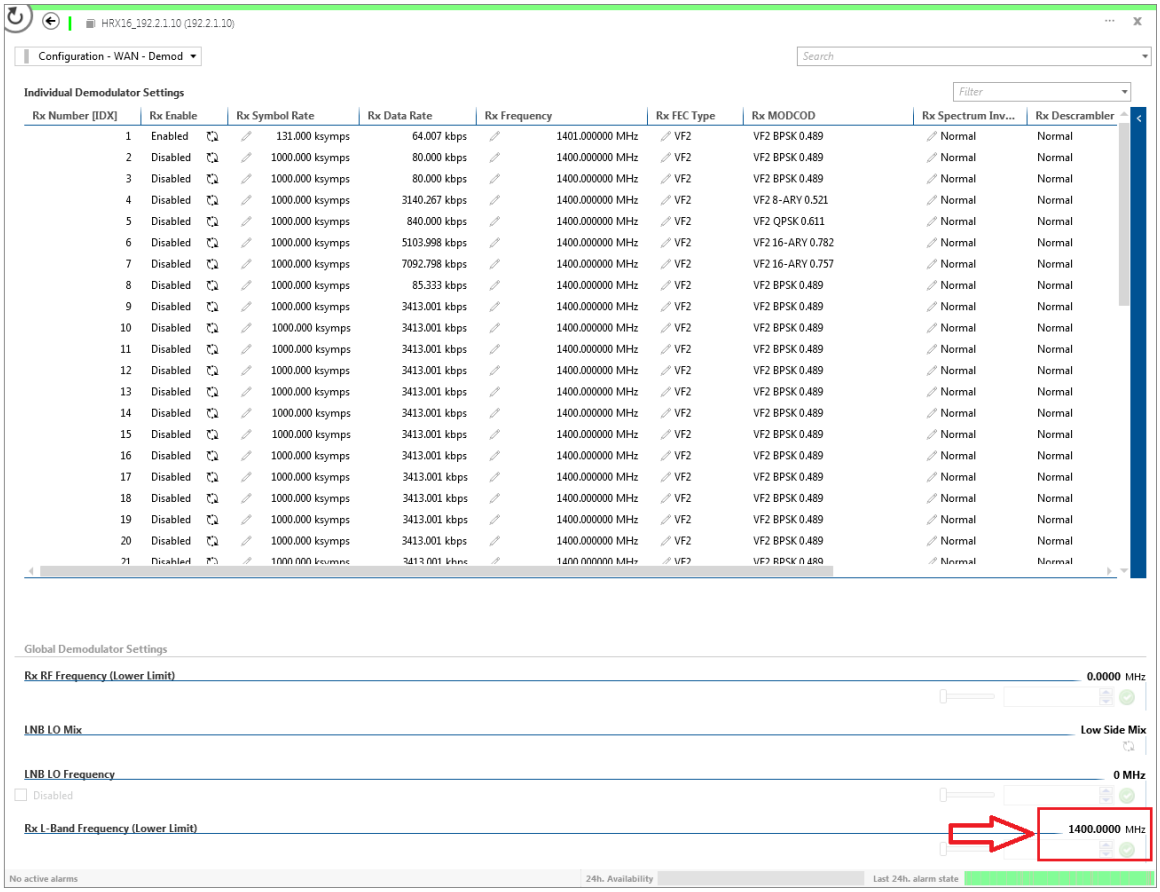


Figure J-2. HRX/HRX-16-R Base Rx Frequency

J.4 Configure Remote Site External Subnet(s)

On the **Service Area->Configuration->Remote Settings->General View**, click on the External Subnets button to add the traffic networks for the remote sites that are to be part of the mesh network. Typically, the only subnet added is the remote's traffic network address.

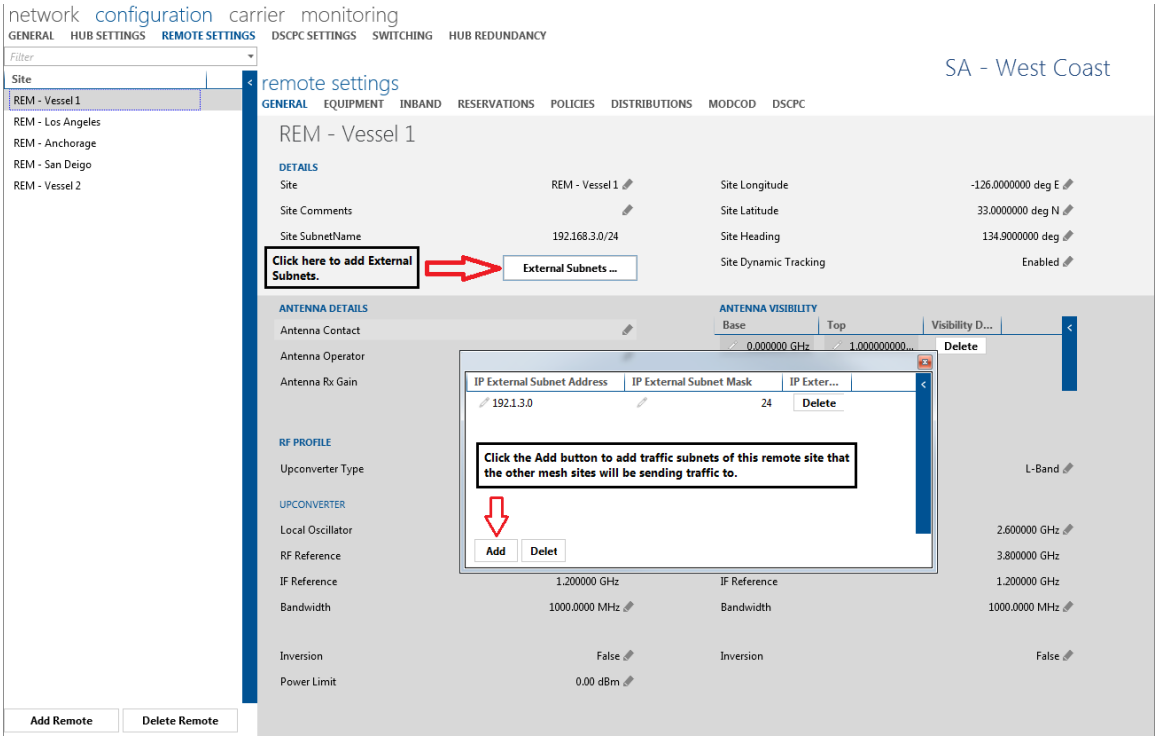


Figure J-3. Mesh Configuring External Subnets

J.5 Configure Remote Site Mesh Demodulator(s)

The remote sites need to have Mesh demodulators assigned and allocated in order for remotes to utilize single hop on demand. For each remote in the mesh network, go to the **Service Area->Configuration->Remote Settings->Equipment View** and select the HRX-16-R demodulator(s) to be used for Mesh and assign them and set the Allocatable state to True.

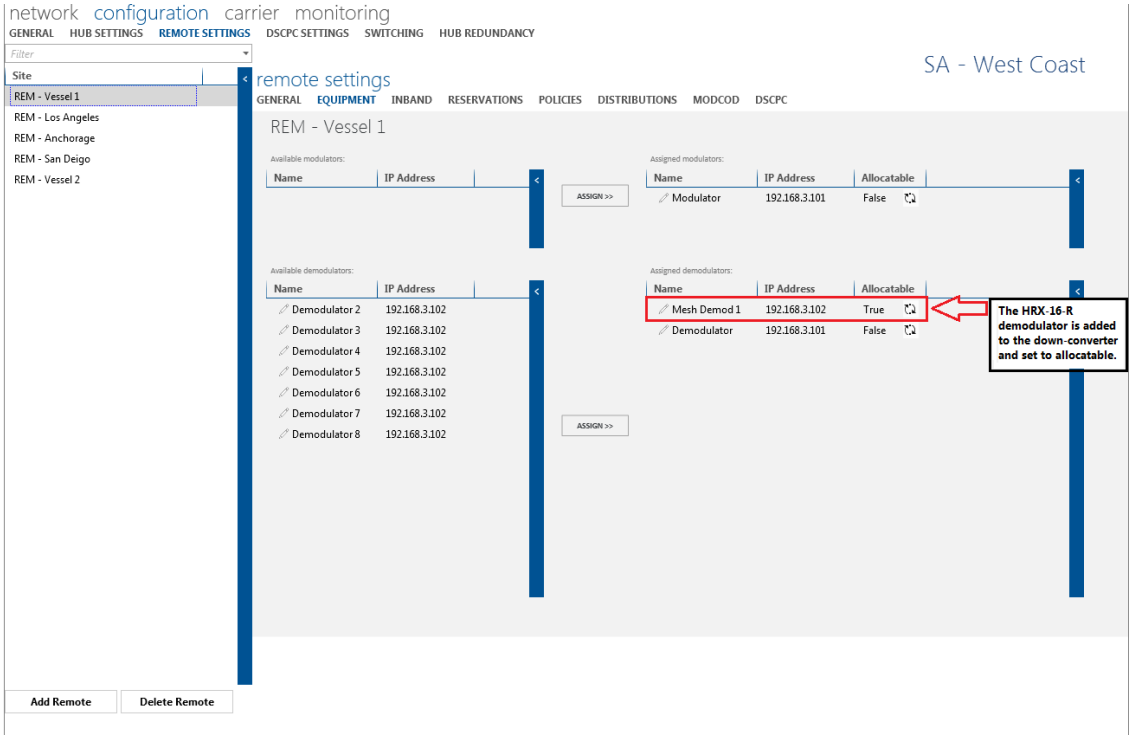


Figure J-4. Adding Remote Site Mesh Demodulator

J.6 Configure Remote Site Distribution(s)

Each remote site in the Mesh network needs to have a distribution list to the other remote sites that make up the mesh network. To configure the remote site distribution, go to the **Service Area->Configuration->Remote Settings->Distributions View** and first add a distribution list and then add the destination remotes as shown below.

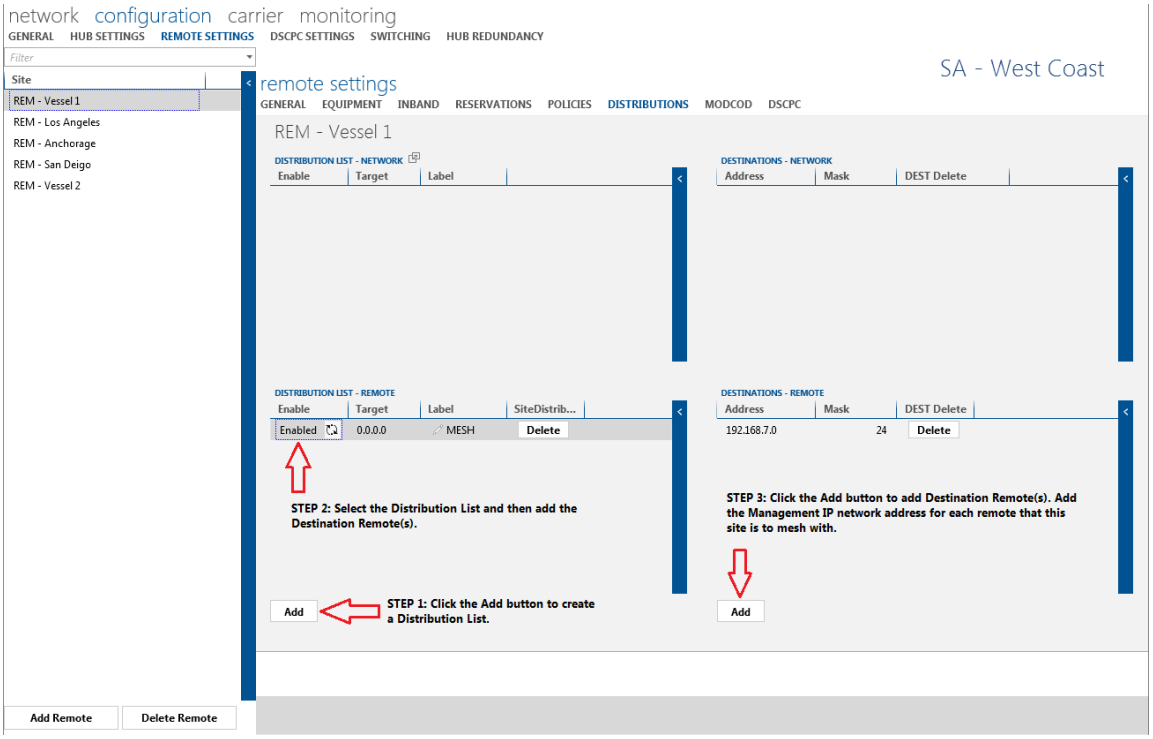


Figure J-5. Adding Destinations for Meshing

J.7 Mesh Switching Reporting

When a remote site is part of a meshed link, the associated demodulators in the **Service Area->Configuration->Switching View** will display all of the Mesh Demodulators that they are linked with.

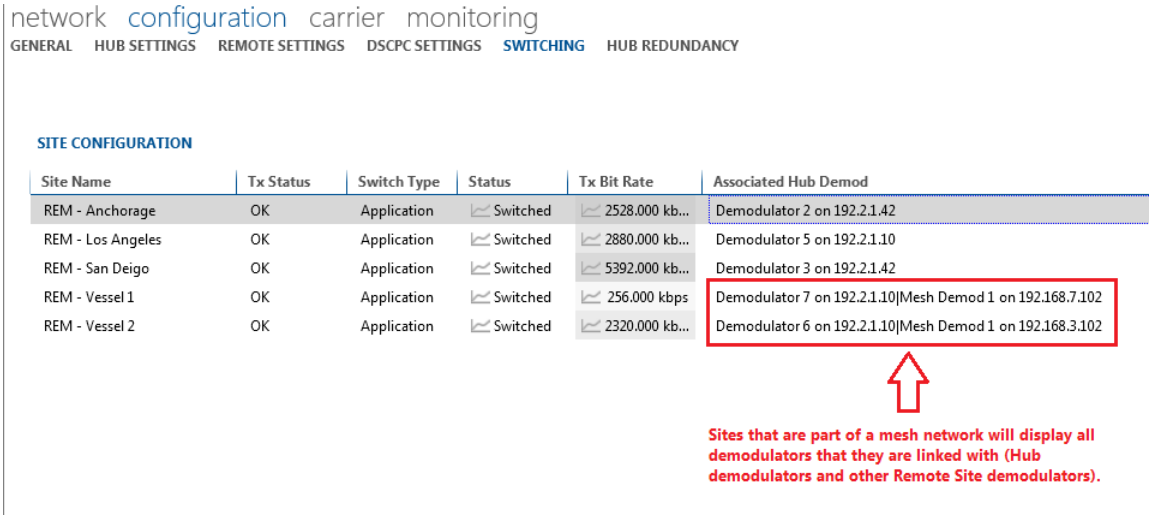


Figure J-6. Mesh Remote Site Associated Demodulators

J.8 Map View with Meshing

The Map View displays the linkage between meshing remote sites.

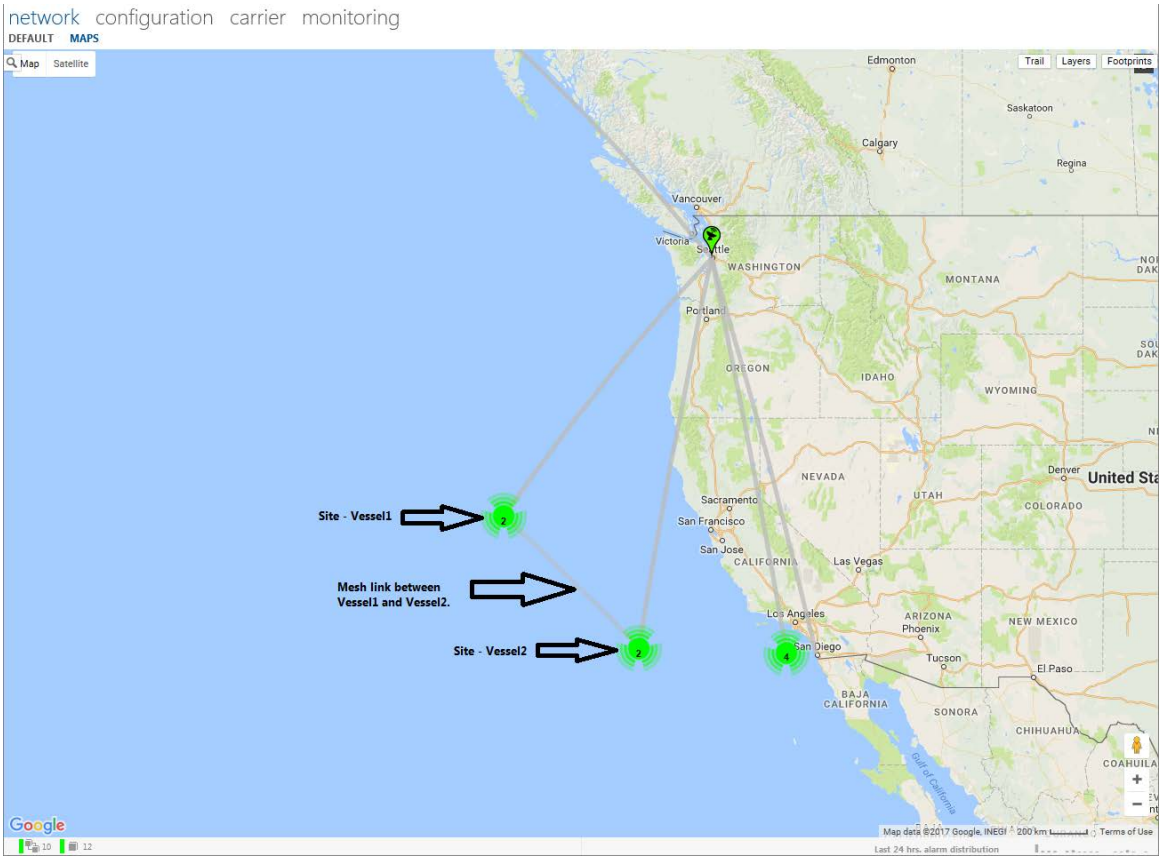


Figure J-7. Map View Showing Mesh Linkage

BLANK PAGE

Appendix K. ROAMING

K.1 Introduction

In release 2.3 and newer versions, NetVue supports Heights roaming using the embedded ROSS feature with Comtech's bandwidth manager. NetVue handles moving the remote device element(s) and the site circuit(s) from one service area to the other in the Surveyor and map views. Using the QoS Group pairing IDs, NetVue can also automatically move remotes into user-defined QoS Groups in the HTO without user intervention. In the Google Map view, NetVue can plot the historical path the site has traveled.

To configure the networks to support roaming, the following settings must be configured:

1. Follow the configuration procedures found in Heights Networking Remote Site manual, Appendix H.
2. Create all of the Service Areas that the remotes will roam to in the same Network container.
3. Enable Dynamic Tracking for each remote that is roaming.
4. Configure Home Modulator for each remote that is roaming.
5. If using user-defined QoS Groups, configure the Pairing IDs in all of the Service Areas in the roaming network.

K.2 Create Roaming Service Areas

All Service Areas and Satellites that are part of the roaming system must be created in the same Network container so that remote devices can properly roam between the Service Areas. Make sure that the Satellite, antennas, and up/down converters are configured to match the ROSS profiles that are loaded into the remotes.

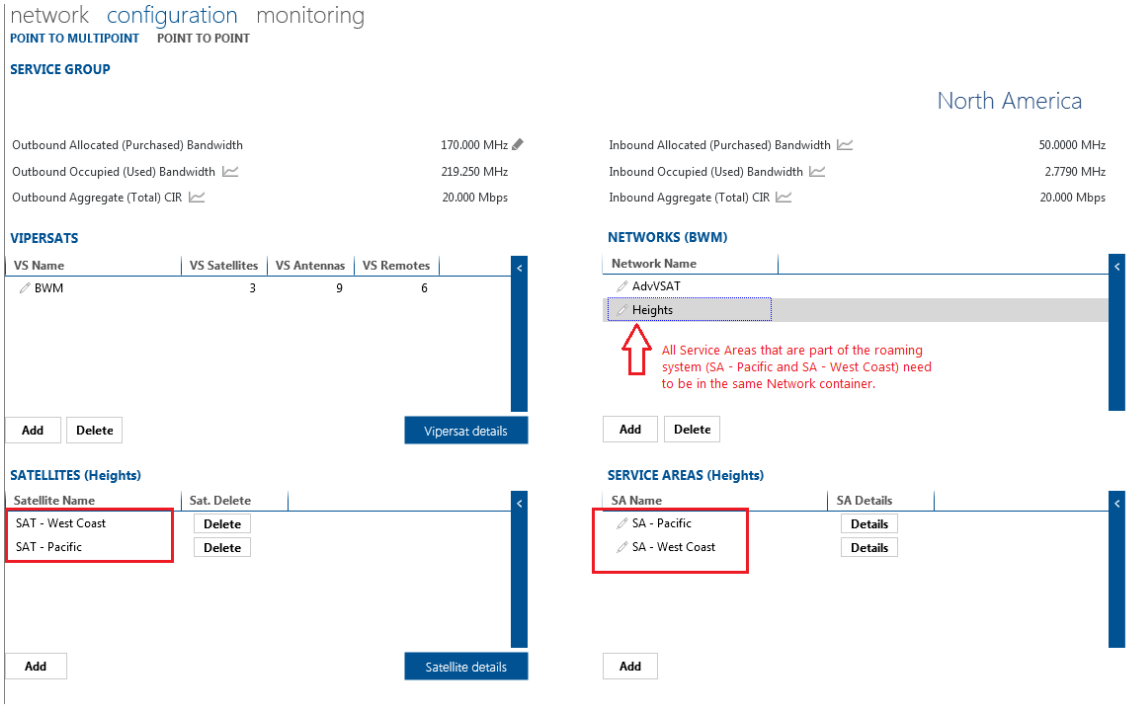


Figure K-1. Create Roaming Service Areas

K.3 Configure Site Dynamic Tracking

The Site Dynamic Tracking field in the **Service Area->Configuration->Remote Settings->General View** needs to be set to Enabled in order for NetVue to properly map the remote as it moves.

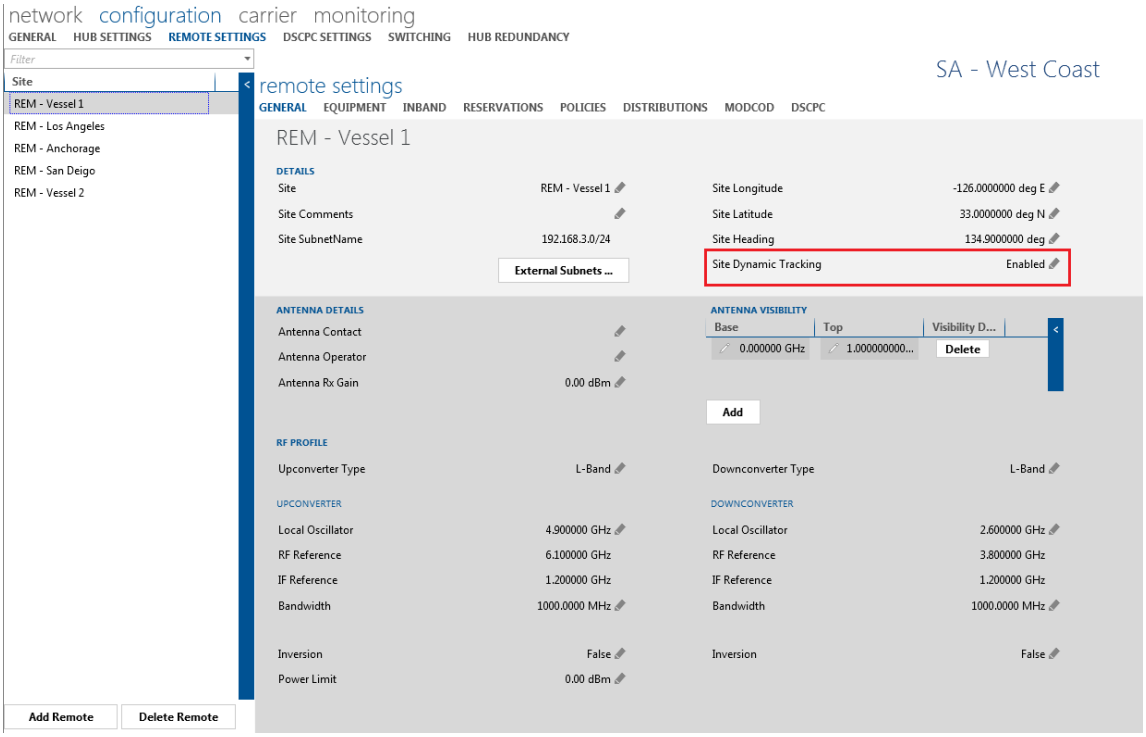


Figure K-2. Enable Site Dynamic Tracking

K.4 Configure Remote Site Home Modulator

The remote site's Home Modulator is used in a roaming environment to tell the site which Service Area it belongs to. This field will automatically change as the remote roams, but it needs to be manually set to a valid hub modulator during initial setup. The field is located in the **Service Area->Configuration->Remote Settings->Inband View**.

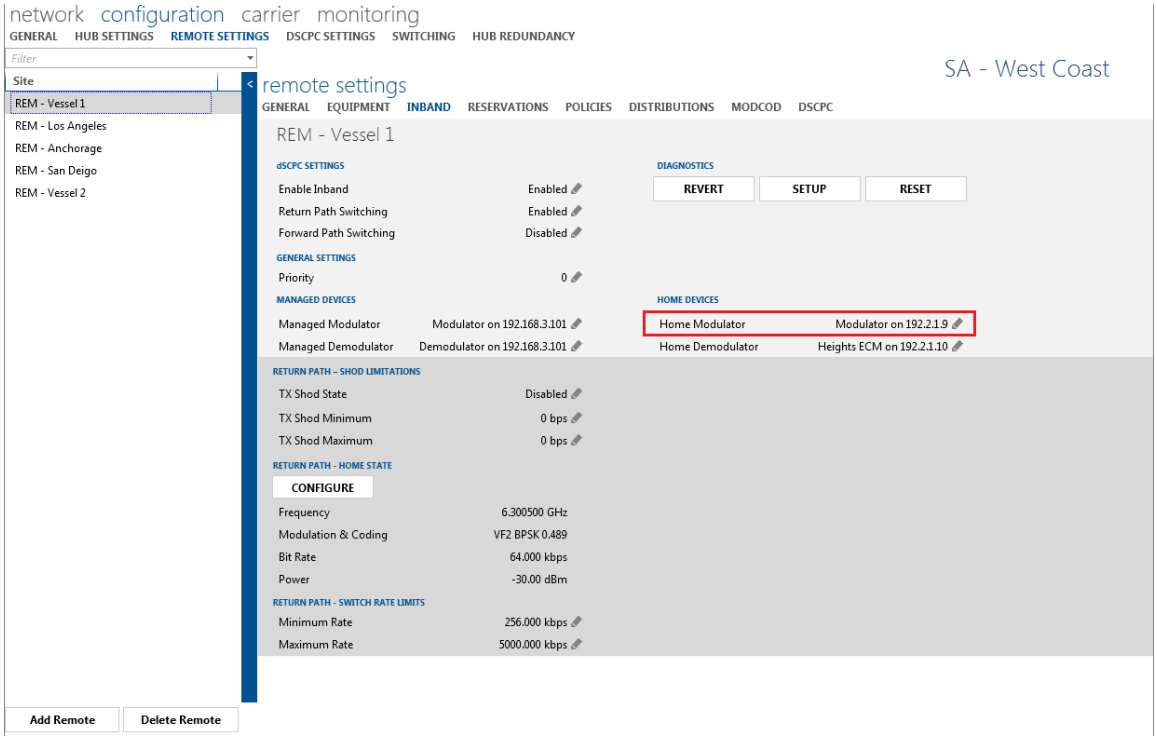


Figure K-3. Configure Remote Home Modulator

K.5 Configure Pairing IDs

If user-defined QoS Groups are used, configure the Pairing ID. If the Outbound QoS Group Pairing ID is configured before adding remotes to the group, the remote QoS Group Pairing ID will automatically be set and the remote's QoS Group is paired. If the remote is already in the QoS Group when the Outbound Pairing ID is configured, then the Pairing ID for each remote will need to be manually configured to match the outbound Pairing ID. See section 9.2 for more information on configuring the remote pairing ID. To configure the outbound pairing ID, go to the **Service Area->Configuration->Capacity Group View** and edit the field(s) in the QoS Group table.

To manually configure the remote site's QoS group pairing ID, go to the **Service Area->Configuration->QoS Group->Inbound View** and edit the pairing ID field.

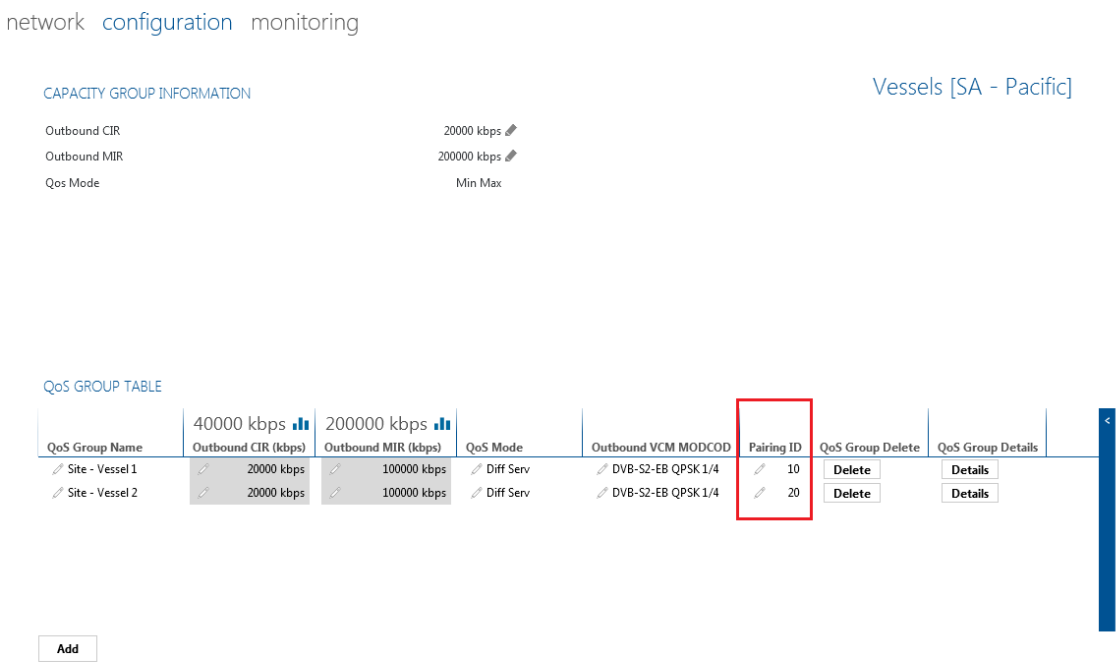


Figure K-4. Configure Outbound QoS Group Pairing ID

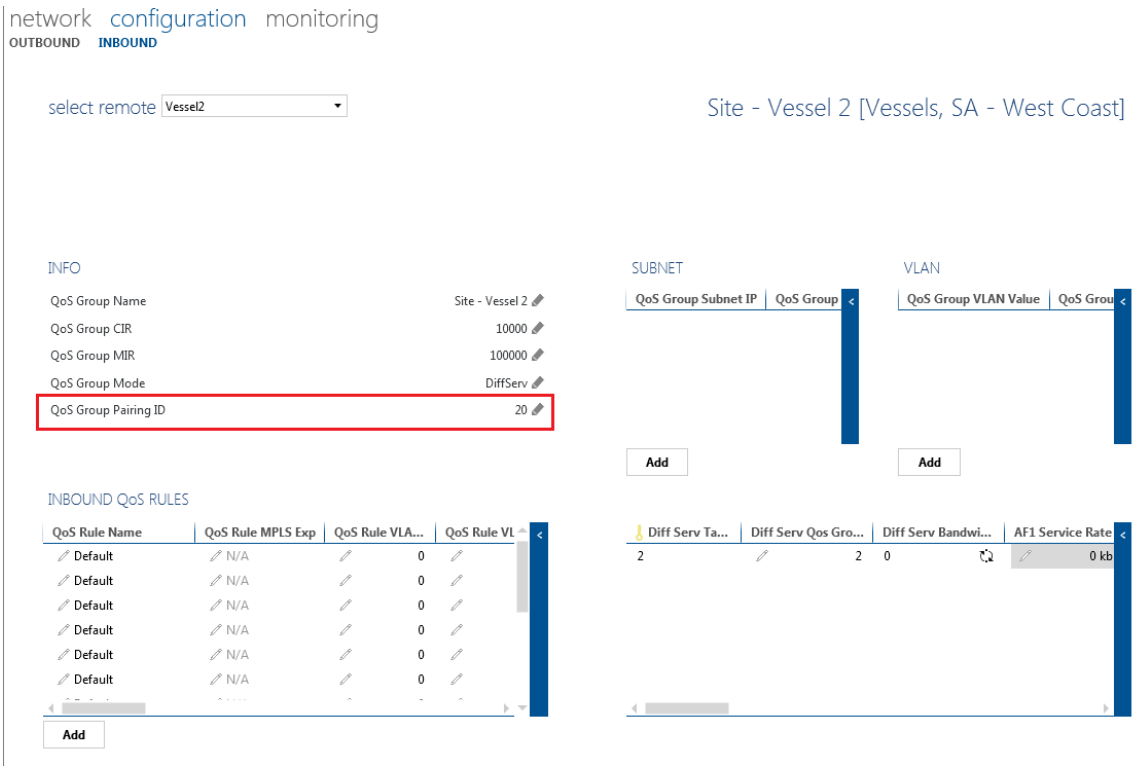


Figure K-5. Remote QoS Group Pairing ID

K.6 Roaming Example

An example of a device roaming between networks: **Site – Vessel2** roaming from **Hub – Pacific (SA1)** to **Hub – West Coast (SA2)**.

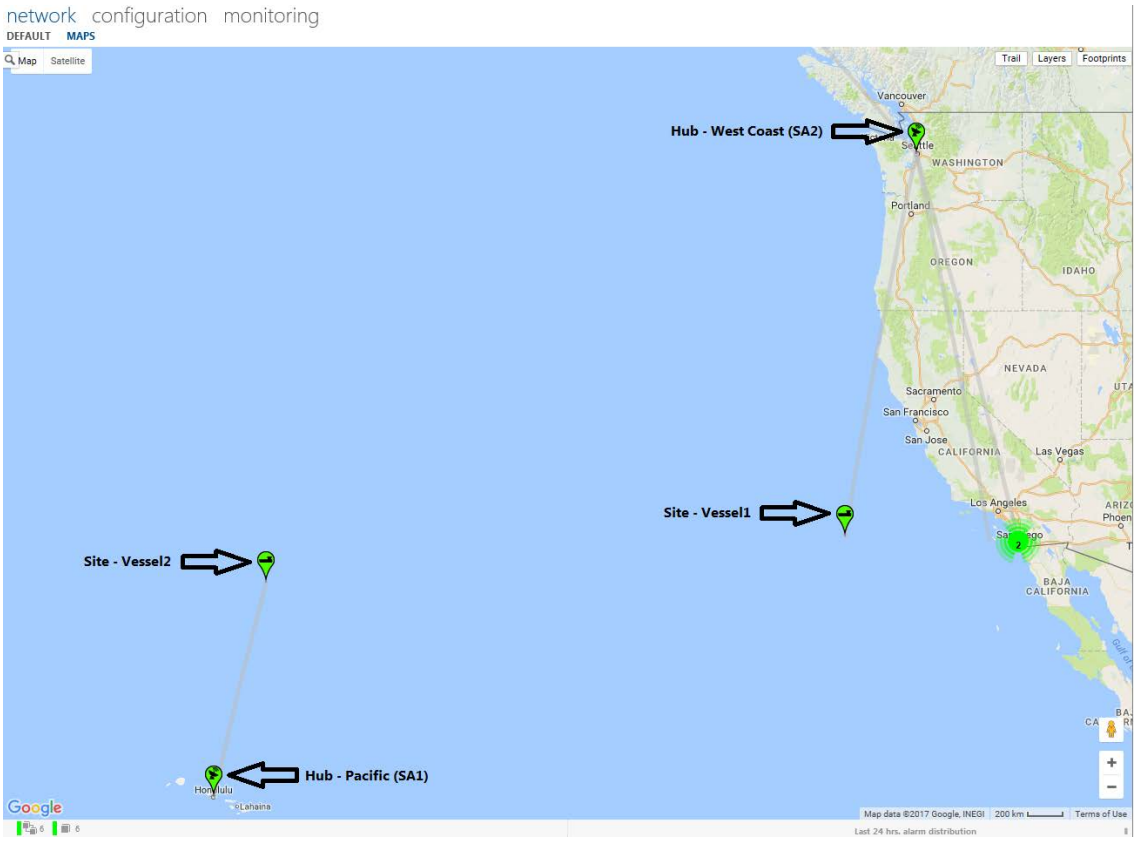


Figure K-6. Roaming Example Map View

As the site leaves Service Area Pacific and enters Service Area West Coast, the bandwidth manager will begin to update the remote's configuration to lock to the new outbound carrier and enter the dSCPC pool in the new Service Area. This configuration change will cause an alarm event in NetVue due to the momentary loss of demodulator lock and loss of communications to the remote device(s).

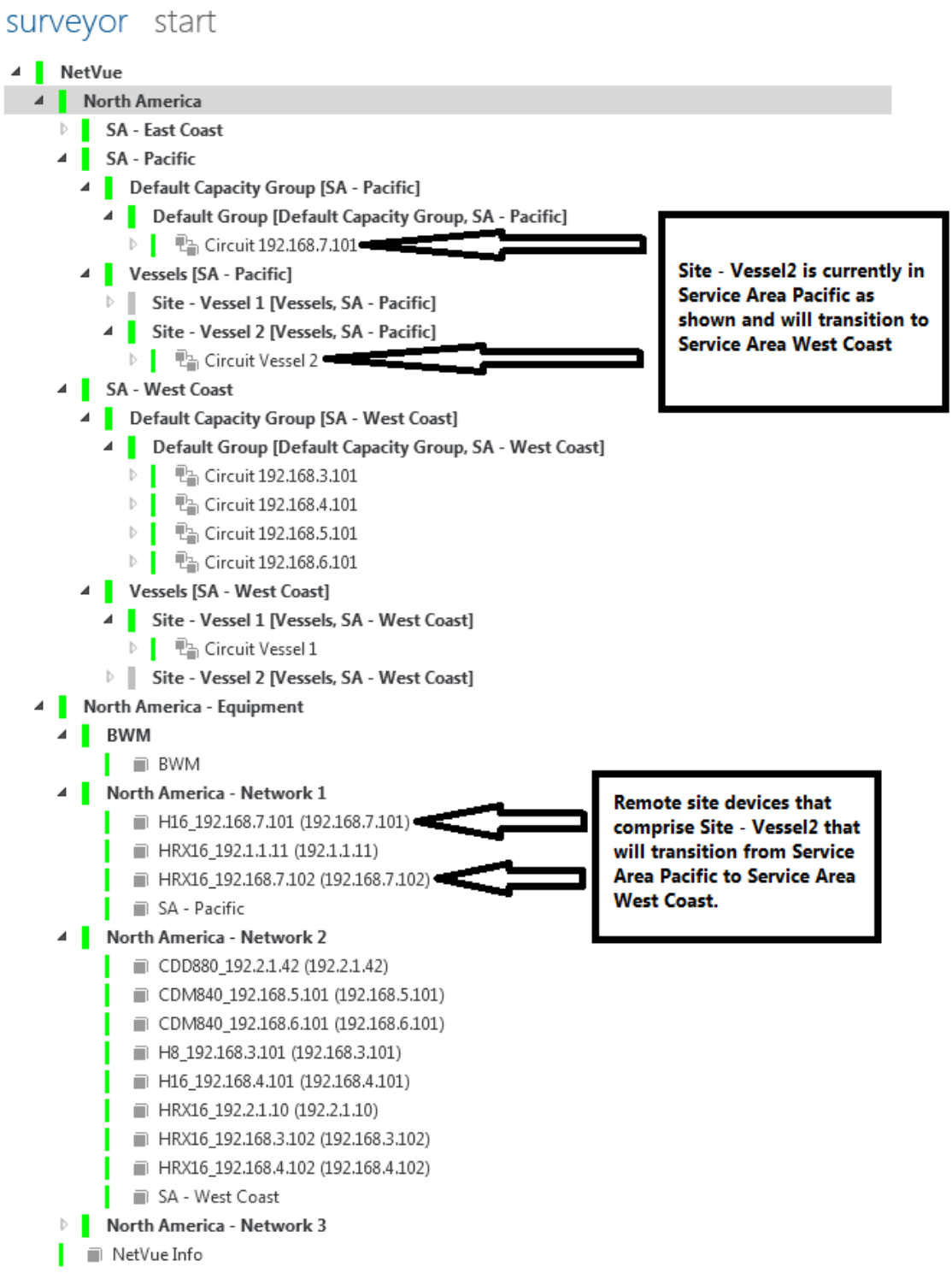


Figure K-7. Roaming Example Surveyor View

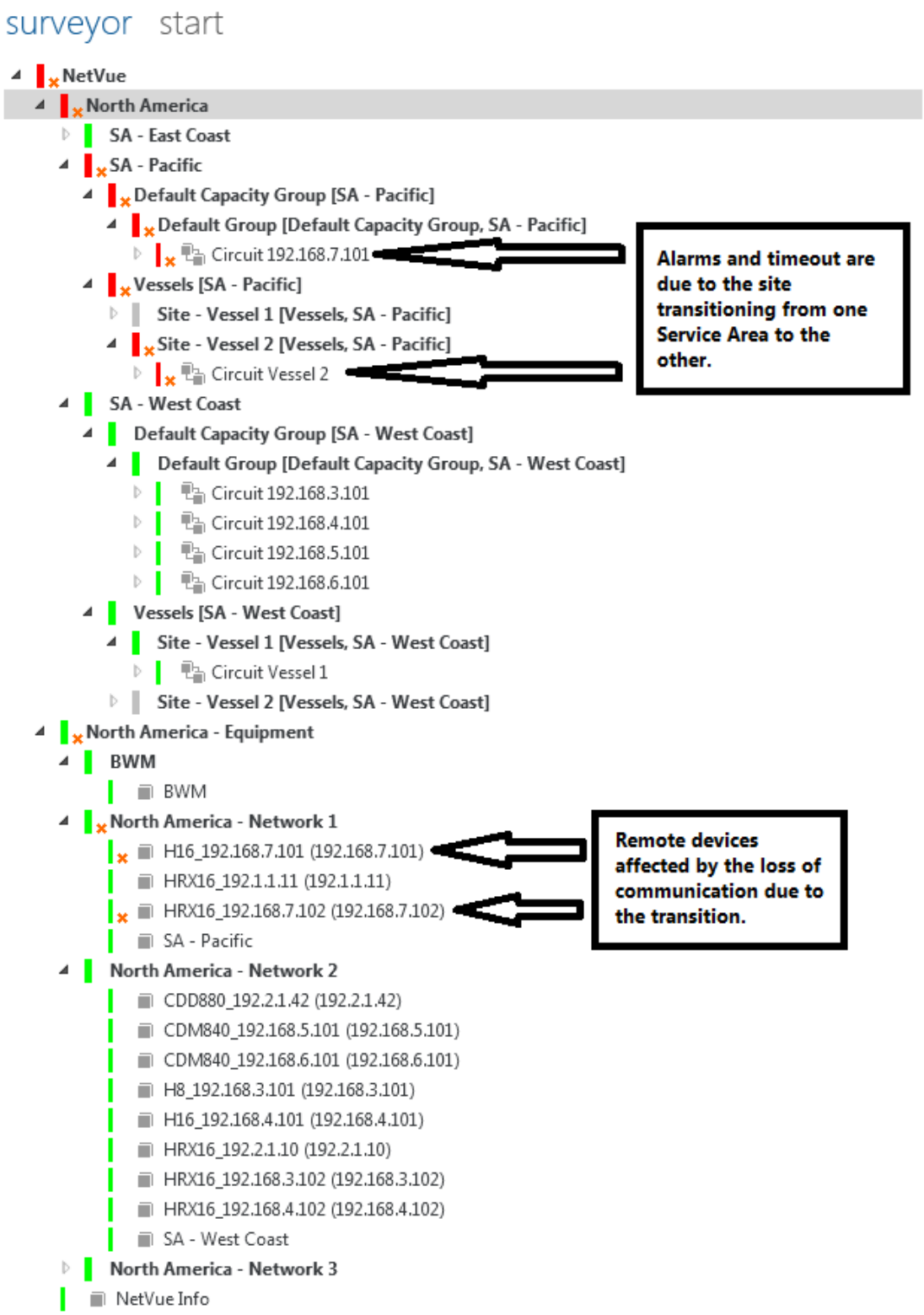


Figure K-8. Roaming Example Device Timeout

Once the remote has completed acquiring lock of the new outbound carrier and has successfully switched into the dSCPC pool, NetVue will update the Surveyor and maps by moving the site from the previous Service Area to the new Service Area.

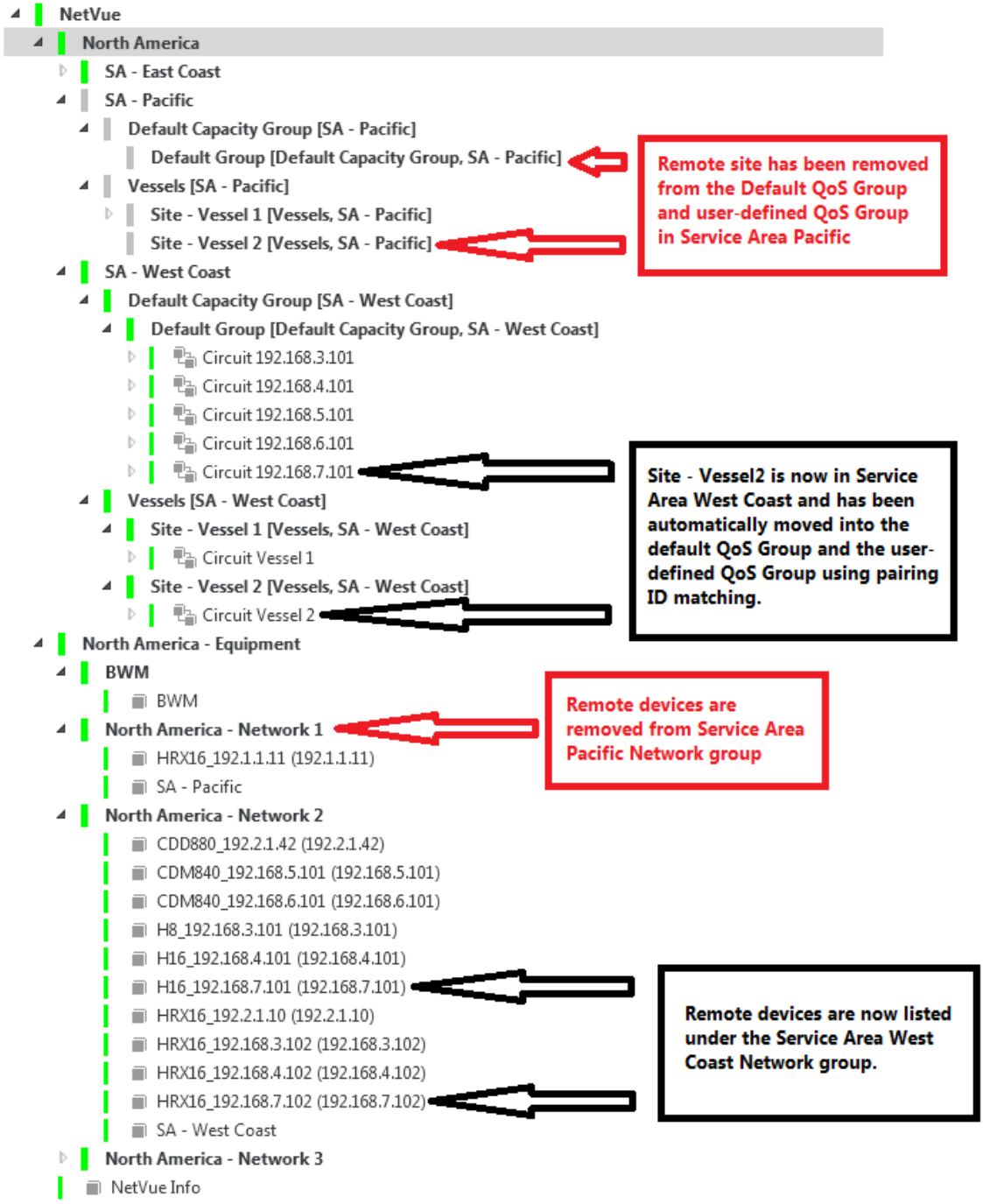


Figure K-9. Roaming Example Surveyor Updated

The map view now shows **Site - Vessel2** is now linked to **Hub - West Coast (SA2)** and no longer linked to **Hub – Pacific (SA1)**.

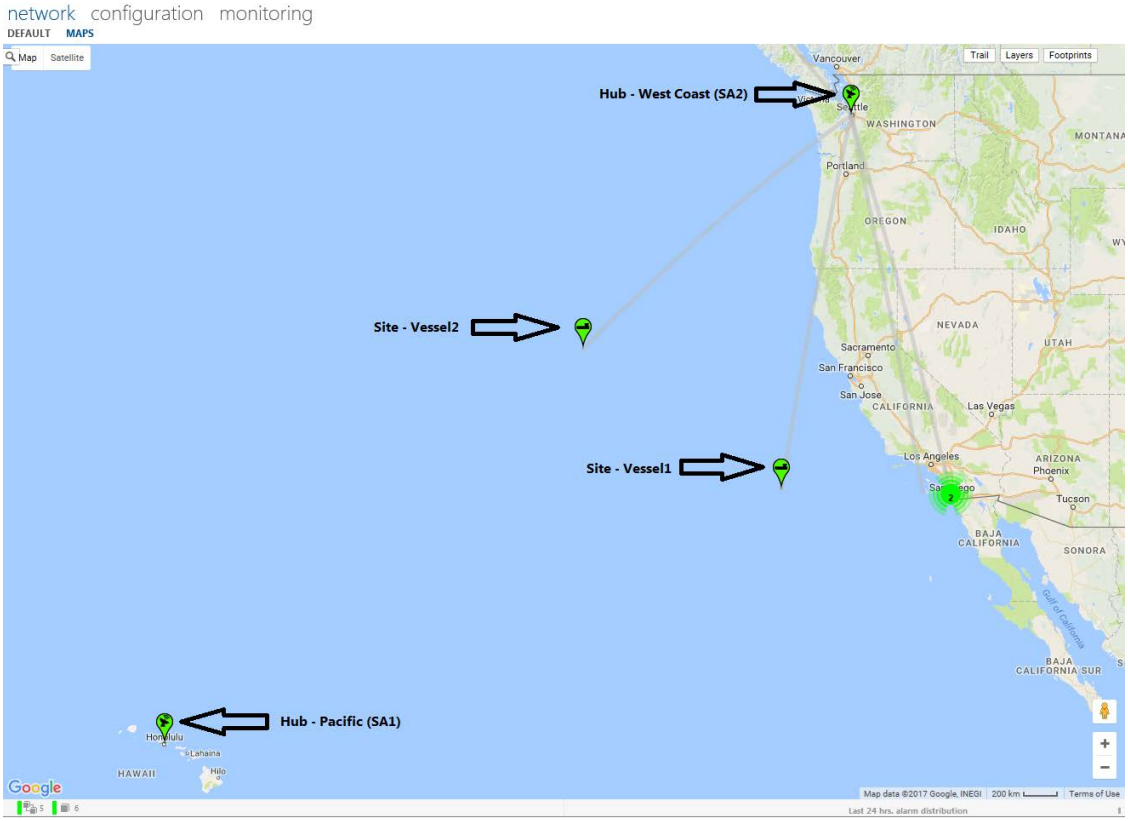


Figure K-10. Roaming Example Map View Updated

Enabling **Route Trace** shows the path that Vessel2 took as it travelled into Service Area West Coast as shown in Figure K-11. The route trace history can be configured based on a start/stop date to focus in on a specific period of time. To select a specific date, click on the Trail button in Google Maps and then click on the Route Trace label. This will bring up a calendar where the user can pick a start and stop date as shown in Figure K-12.

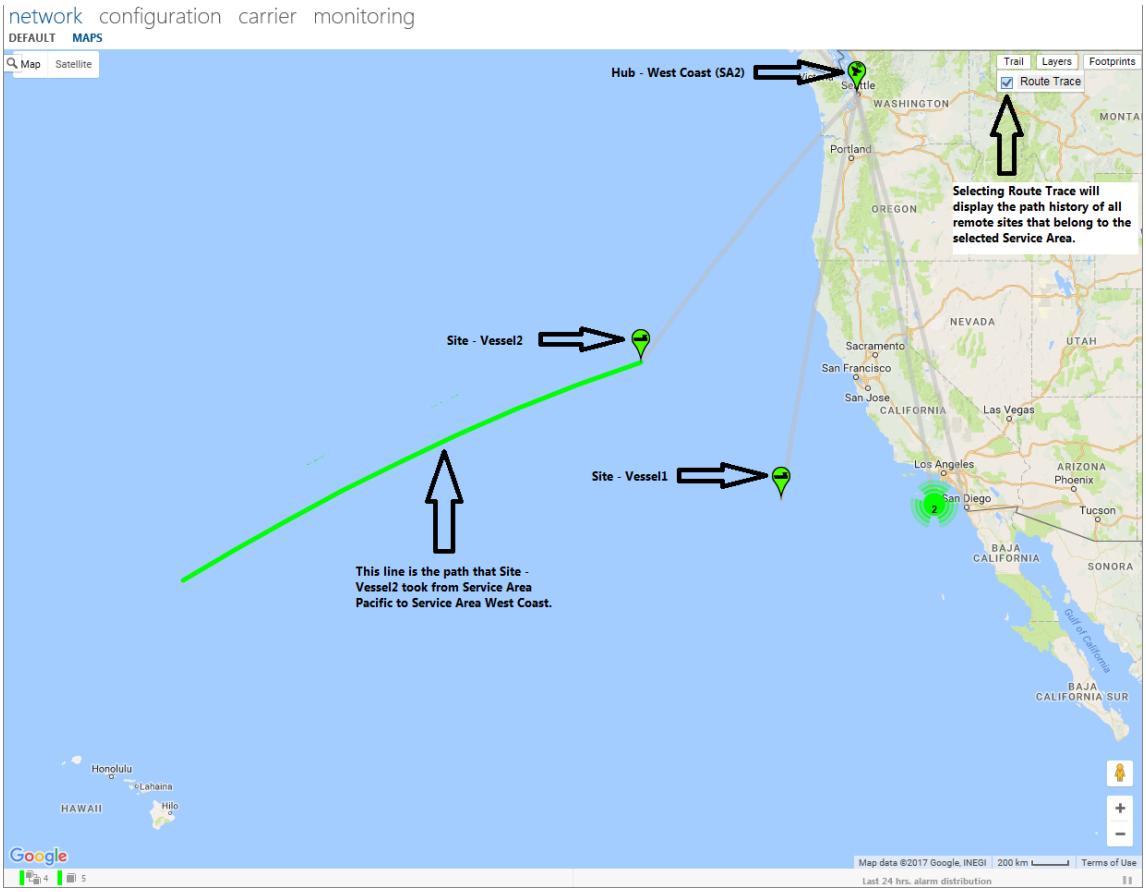


Figure K-11. Roaming Example Site Historical Path

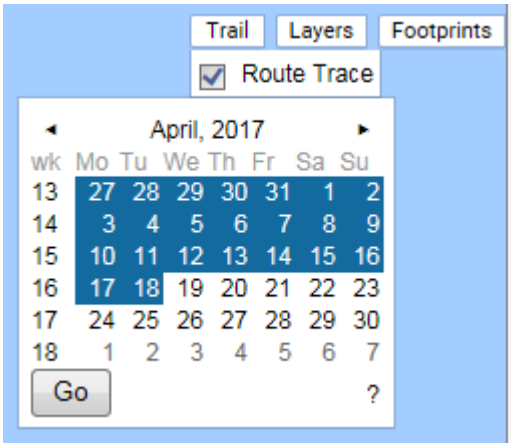


Figure K-12. Configure Route Trace Start/Stop Date Range

Appendix L. TROUBLESHOOTING

L.1 Frequently Asked Questions

L.1.1 When Must I Restart a NetVue Agent?

After an upgrade, the NetVue Agent restarts automatically.

You must restart a NetVue Agent in these cases:

- After you change a DataMiner XML file manually
  - Example: you add a custom command to the Alarm Console shortcut menu in *Hyperlinks.xml*
- After you change the IP address of the server hosting the NetVue Agent
- After you change the time zone on the NetVue Agent

L.1.2 How Do I Synchronize Time Settings in a NetVue System?

In a NetVue System, the time settings on the different NetVue Agents must be synchronized. Otherwise, it is impossible to correlate events, or to have an accurate view of what occurs in the NetVue System.

L.1.2.1 Time Synchronization Options

The most common way to make sure that time is synchronized among all NetVue Agents is to make them all members of the same domain.

If this is not possible, you can set up a time synchronization mechanism among the NetVue Agents based on Simple Network Time Protocol (SNTP). This mechanism causes one computer to be the Time Server, and all other computers in the system to be Time Clients.

L.1.2.2 Set the Time Server

The Time Server gives the correct time settings to all NetVue Agents. To cause a computer to be a Time Server, whether it is a NetVue Agent or not, do these steps:

1. Log on locally to the machine that will be a Time Server, or start a remote desktop session with it.
2. Open Registry Editor: **Start > Run… > regedit**

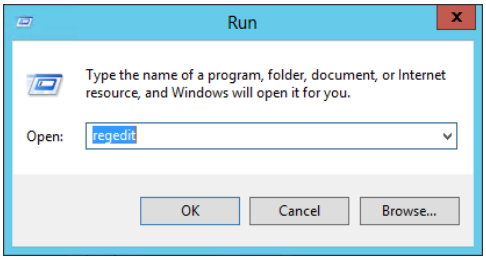


Figure L-1. Regedit

3. Go to this key:
   HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/W32Time/Parameters
4. Change the value of **LocalNTP** from 0 to 1.
   0 = No Time Server except when a domain controller
   1 = Always a Time Server

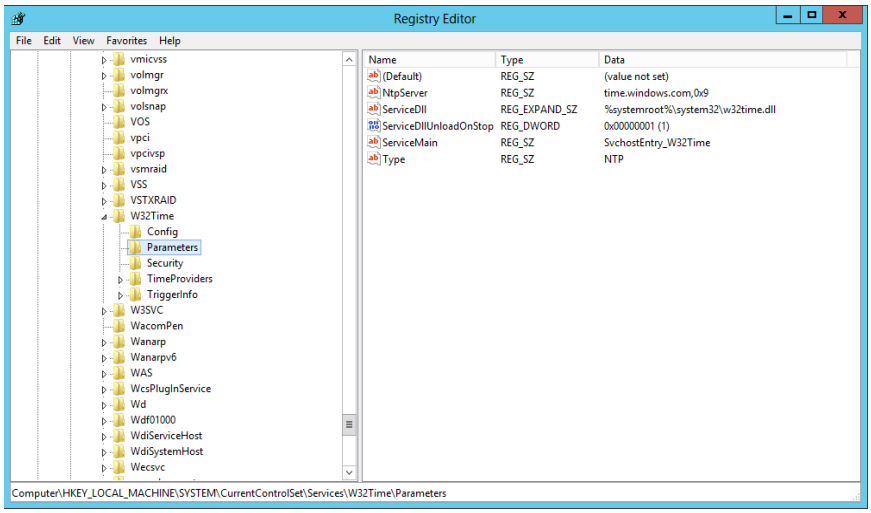


Figure L-2. Registry Parameters

L.1.2.3 Set the Time Client(s)

In the NetVue System, all NetVue Agents must become Time Clients, to synchronize their time settings with those of the Time Server.

To cause a NetVue Agent to be a Time Client:

1. Log on locally to the NetVue Agent, or start a remote desktop session with it.
2. Open the Services dialog box: **Start > Settings > Control Panel > Administrative Tools > Services.**
3. Select the **Windows Time** service.
4. Right-click the service.
5. Select **Properties.**
6. Change **Startup type** to **Automatic.**
7. Click **OK.**

   This setting causes Windows Time service to start automatically when the NetVue Agent is started.

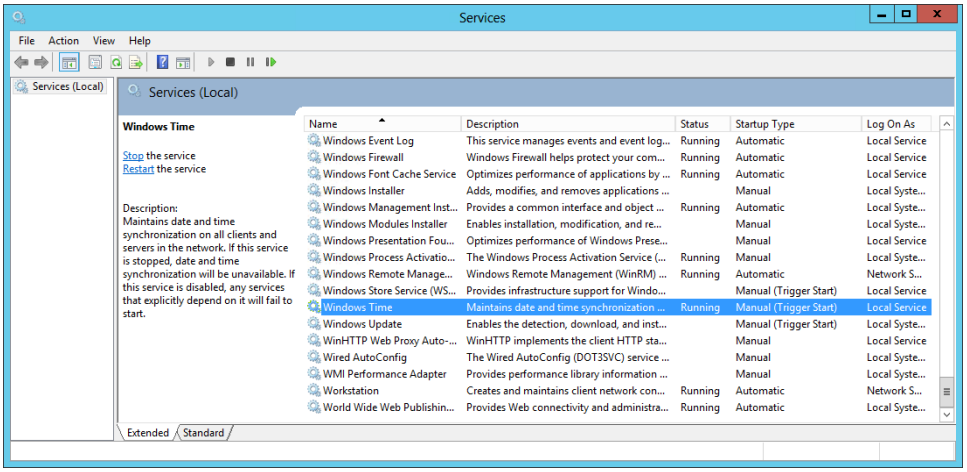


Figure L-3. Windows Time Services

8. Right-click the **Windows Time** service.
9. Select **Start.**
10. Make sure the service is running, and then close the **Properties** dialog box.
11. Open a command prompt window: **Start > Run… > cmd.**
12. Enter **net time /set**, followed by the **IP address** of the Time Server.
13. Press **Enter.**

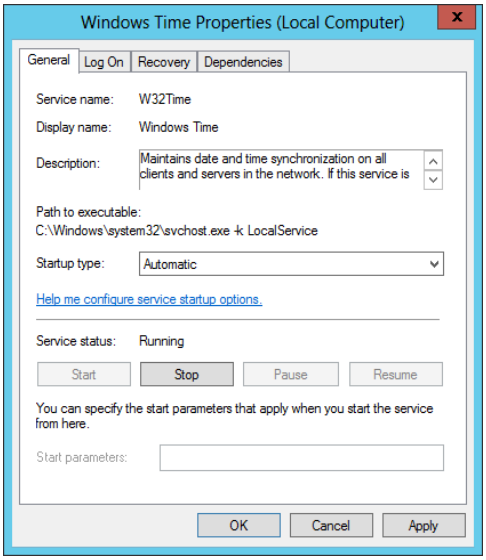


Figure L-4. Windows Time Properties

L.1.3 How Do I Keep My NetVue Client Session from Disconnecting Automatically?

By default, a NetVue client session disconnects after a period of time during which no user activity occurs. This prevents users from leaving sessions open on unattended workstations.

However, it is sometimes necessary to keep a session open indefinitely.

L.1.3.1 Prevent NetVue Cube from Disconnecting Automatically

1. Go to the NetVue Cube user settings.
2. Go to the **Connection** tab.
3. Clear the option: **Time before automatic disconnect.**

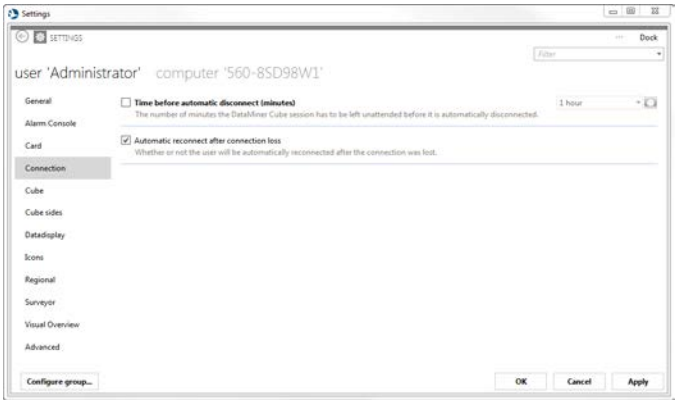


Figure L-5. Connection Settings

L.1.4 How Do I Find the ID of a View?

In NetVue Cube:

1. Right-click the view in the Surveyor.
2. Select **Properties**
3. The view ID shows in the **general** tab, to the right of the view name.

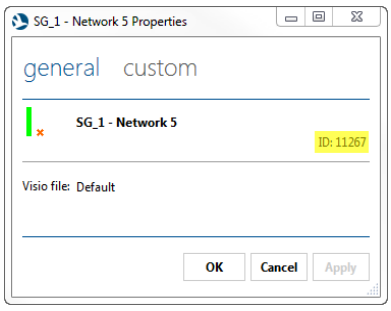


Figure L-6. View ID

L.1.5 How Do I Find the ID of an Element, Service or Redundancy Group?

The ID of an element, service or redundancy group always has two parts separated by a forward slash:

- The ID of the NetVue Agent where the element, service or redundancy group was created

  /

- The ID of the actual element, service or redundancy group

In NetVue Cube:

1. Open the view that contains the element, service or redundancy group.
2. On the view card, go to the data side.
3. Click the **details** tab.
   The IDs of all items in the view show in the **ID** column.

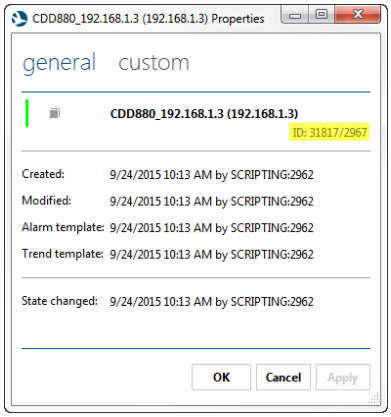


Figure L-7. Element ID

Alternatively, for an element or service:

1. Right-click the item in the Surveyor.
2. Select **Properties**
   The ID shows in the **general** tab, to the right of the name view.

L.1.6 How Do I Find the ID of a Parameter?

In NetVue Cube:

1. On the element card containing the parameter, double-click the parameter.
2. The parameter ID shows to the right of the parameter.

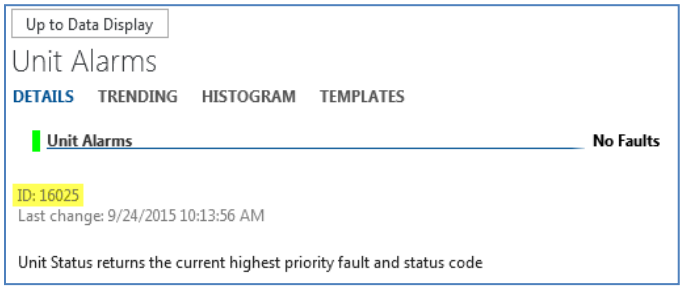


Figure L-8. Parameter ID

L.1.7 What Happens if a Central Database …

L.1.7.1 …Is Activated?

Data from the NetVue System is offloaded from the moment of activation.

Data that dates from before the activation is not offloaded.

L.1.7.2 …Is Deactivated for a Few Days?

There will be a gap in the data stored on that central database.

L.1.7.3 …Cannot be Reached for a While?

The offload files are stored for as long as the central database cannot be reached. The files are then processed from the moment the connection is established again.

L.1.8 How Do I Send Information about my NetVue Client to Technical Support?

In case of problems, the Comtech ESC may ask you for version and/or debug information. Read on to learn how to gather the requested information.

L.1.8.1 Send Version Information to Technical Support

In NetVue Cube:

1. Select **Start > Apps > About.**
2. In the **About** box, click the **Versions** tab.
3. At the bottom of the dialog box, click **Copy Versions Information.**
4. Paste the text in a new email message, and send the information to esc@comtechefata.com.

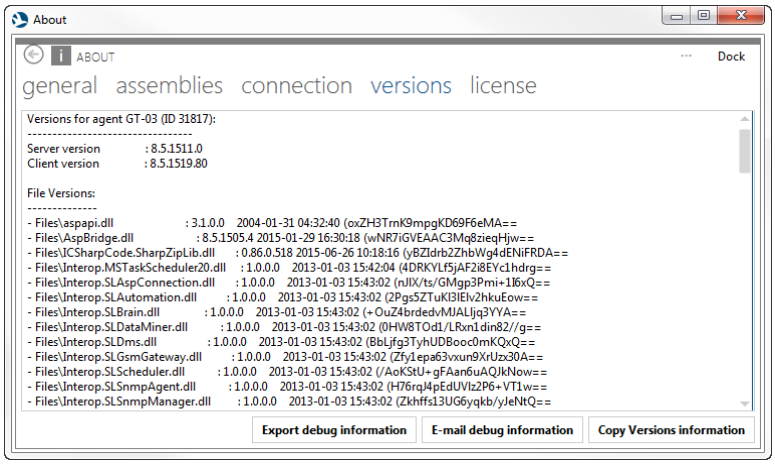


Figure L-9. Versions Information

L.1.8.2 Send Debug Information to Technical Support

In NetVue Cube:

1. Select **Start > Apps > About.**
2. At the bottom of the **About** box, click **E-mail Debug Information**
   A new email opens that contains the debug information.

   You may see a warning that an application (NetVue Cube) is trying to send an email message from your computer.

3. Send the information to esc@comtechefdata.com.
4.

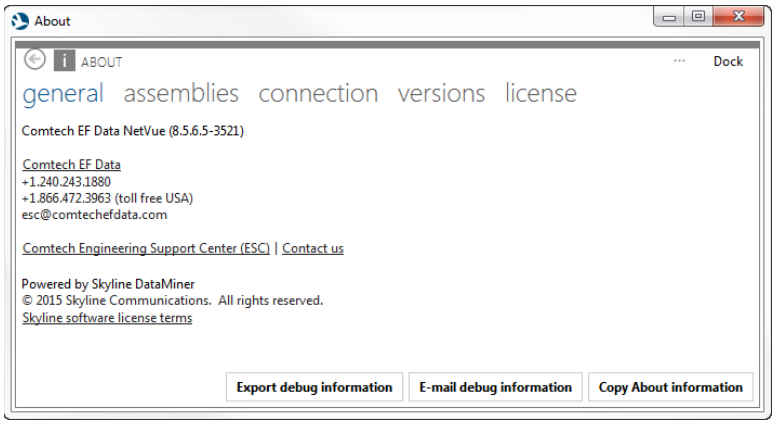


Figure L-10. Debug Information

L.1.9 How Do I Reinstall the NetVue Client Software?

If the security policy of your company or computer allows it, NetVue Cube is downloaded and installed onto your computer automatically, the first time you try to open the user interface in a web browser.

If it is necessary to reinstall the application, you must first clean the XBAP cache (NetVue Cube).

If your NetVue client application was installed using the msi **file, do not use these steps.**

L.1.9.1 Reinstall NetVue Cube

During these steps, replace [NetVue IP] with the IP address or host name of the NetVue Agent to which you want to connect.

1. Open Microsoft Internet Explorer.
2. Depending on your setup, go to one of these addresses:

   https://[NetVue IP]**/Tools**
   http://[NetVue IP]**/Tools**

3. In the DataMiner Tools section, click **Clean DataMiner Cube XBAP Cache**, and then click **Run.**
4. Open Microsoft Internet Explorer.
5. Depending on your setup, go to one of these addresses:

   https://[NetVue IP]**/dataminercube**
   http://[NetVue IP]**/dataminercube**

L.2 Error Messages

L.2.1 An Error Occurred in the Application You Were Using

L.2.1.1 Symptom

When you open NetVue Cube in Microsoft Internet Explorer, you get this error message:

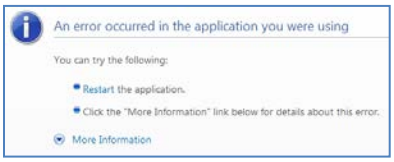


Figure L-11. Error Occurred

If you click **More Information**, you see this notice:

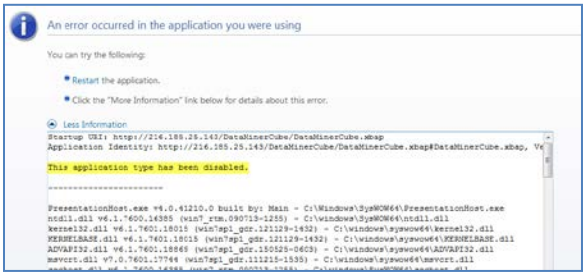


Figure L-12. More Information

L.2.1.2 Cause

In the security settings of Microsoft Internet Explorer, XAML browser applications (XBAPs) have been disabled for the security zone in which you are working (Internet, Local intranet, Trusted sites, etc.).

L.2.1.3 Solution

Do one of these tasks:

1. Add the address of the NetVue client application to the list of **Local intranet** sites.

   - or -

2. In the security settings of the zone in which you are working, set **XAML browser applications** to **Enable**:

   - In Microsoft Internet Explorer, go to **Internet Options > Security**
   - Click **Custom** level.
   - Go to the **XAML browser applications** setting in the **.NET Framework** section.
   - Select **Enable**

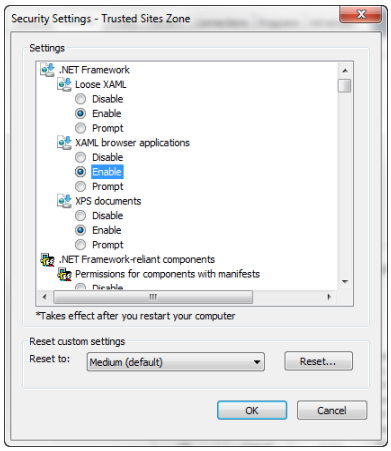


Figure L-13. Enable XAML

L.2.2 Trust Not Granted

L.2.2.1 Symptom

While working with NetVue Cube, you see a **Trust not granted** error.

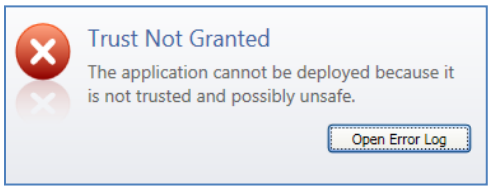


Figure L-14. Trust Not Granted Error

L.2.2.2 Cause

The Skyline certificates are not installed on your computer.

L.2.2.3 Solution

1. Install the Skyline certificates:

   During these steps, replace [NetVue IP] with the IP address or host name of the NetVue Agent to which you want to connect.

   a. Open Microsoft Internet Explorer.

   b. Depending on your setup, go to one of these addresses:
      https://[NetVue IP]**/Tools**
      http://[NetVue IP]**/Tools**

   c. In the **Certificate** section, click the link to install the certificate.

   d. Click **Run.**

   e. When prompted with a security warning about adding the certificate, select **Yes**.

   f. Open Microsoft Internet Explorer.

   g. Depending on your setup, go to one of these addresses:
      https://[NetVue IP]**/dataminercube**
      http://[NetVue IP]**/dataminercube**

L.2.3 Unknown Error

L.2.3.1 Symptom

You see this error:

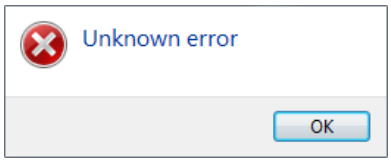


Figure L-15. Unknown Error

L.2.3.2 Cause

The XBAP cache has a problem.

L.2.3.3 Solution

Do these steps:

1. Open Microsoft Internet Explorer.
2. Go to **http:/[NetVue IP]/tools.**
3. In the **DataMiner Tools** section, click **Clean XBAP Cache.**
4. In the **File Download** dialog box, click **Run.**

If you restart NetVue Cube after these steps are completed, a fresh copy of the NetVue Cube application downloads.

L.2.4 Cannot Connect with local SLNet

L.2.4.1 Symptom

When running a driver update package on the NetVue server, you see this Information message:

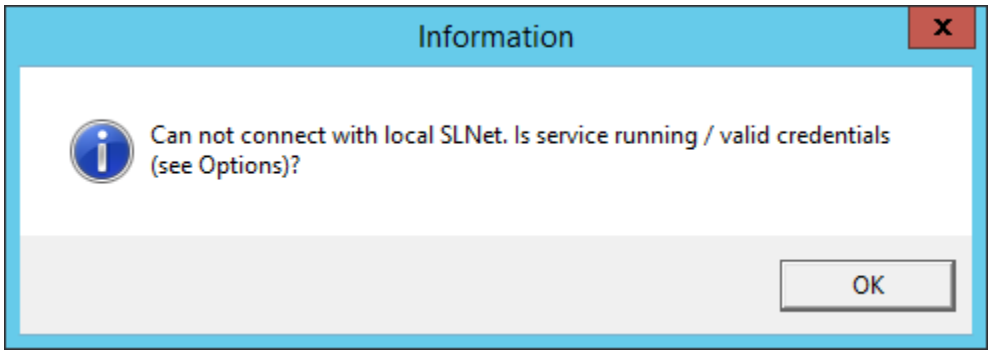


Figure L-16. Cannot Connect with Local SLNet

L.2.4.2 Cause

The administrator user account is not linked to the SLNet service.

L.2.4.3 Solution

1. Connect to the NetVue server using RDP, TeamViewer, KVM, etc.
2. In the Windows System Tray, right-click the DataMiner icon.
3. Select **Options**.
4. In the **Options** pop-up box, click the **slnet** tab.
5. Enter the Administrator **Username** and **Password**.
6. Click **Test & Save Connection**.

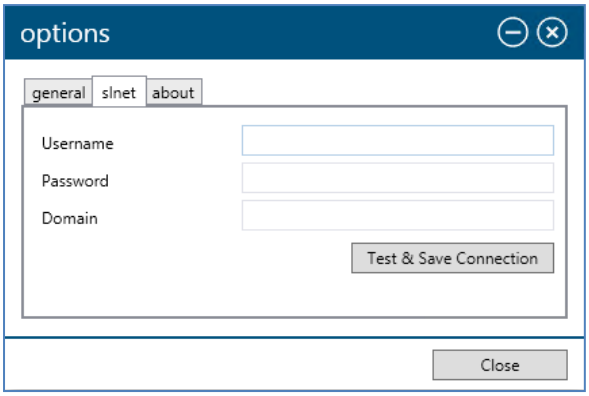


Figure L-17. SLNet Options

A confirmation message shows that the connection was successful.

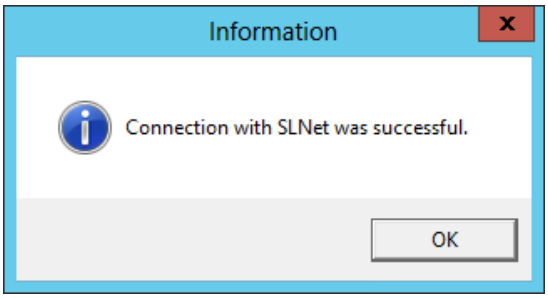


Figure L-18. Successful SLNet Connection

2114 WEST 7TH STREET TEMPE ARIZONA 85281 USA
480 • 333 • 2200 PHONE
480 • 333 • 2161 FAX