

Dell OpenManage Network Manager version 5.1  
**Web Client Guide**



# Notes, and Cautions



A **NOTE** indicates important information that helps you make better use of your computer or software.



A **CAUTION** indicates potential harm to your data or hardware if you proceed as indicated.

---

**Information in this document is subject to change without notice.**

© 2012 Dell Inc. All rights reserved.

Reproduction of these materials in any manner whatsoever without the written permission of Dell Inc. is strictly forbidden.

Trademarks used in this text: Dell™, the DELL logo, PowerEdge™, PowerVault™, PowerConnect™, OpenManage™, EqualLogic™, KACE™, FlexAddress™ and Vostro™ are trademarks of Dell Inc. Microsoft®, Windows®, Windows Server®, MS-DOS® and Windows Vista® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Red Hat Enterprise Linux® and Enterprise Linux® are registered trademarks of Red Hat, Inc. in the United States and/or other countries. Verizon® is a registered trademark of Verizon Wireless.

Other trademarks and trade names may be used in this publication to refer to either the entities claiming the marks and names or their products. Dell Inc. disclaims any proprietary interest in trademarks and trade names other than its own.

# Contents

1	Preface	9
	Why Dell OpenManage Network Manager?	9
	Key Features	9
	Networks with Dell OpenManage Network Manager	11
	Additional Products	11
	Online Help / Filter	12
	<b>How to:</b> Use “How To”	12
	Feedback	13
	A Note About Performance	13
2	Getting Started with Dell OpenManage Network Manager	15
	Overview	15
	System Basics	15
	Single Server Sizing	20
	Sizing for Standalone Installations	21
	Network Basics	22
	Authentication	24
	Supported PowerConnect Models	24
	Windows Management Interface	24
	Getting Started	27
	Installation and Startup	28
	How to: Set Linux Permissions	31
	Perl	32
	Starting Web Client	33
	Control Panel	34
	Search Indexes	34
	[My Account]	35
	RCSynergy / [Domain]	35
	Portal > Users and Organizations	36
	How to: Add Users and connect them to Roles	36
	How to: Configure Organizations	38
	Public / Private Page Behavior	40
	How to: Add and Configure User Roles / Permissions	40
	Portal > Roles	41
	Portal > Portal Settings	41
	Portal > [Other]	42
	Redcell > Permission Manager	42
	Redcell > Data Configuration	45
	Redcell > Mediation	46
	Redcell > Filter Management	48
	Server	49
	Redcell > Database Aging Policies (DAP)	50

How to: DAP Workflow .....	51
Aging Policies Editor .....	52
Aging Policies Options .....	54
Sub-Policies .....	55
Repositories .....	57
Portlet Level Permissions .....	58
How to: Configure Portlet Permissions .....	59
<b>How to:</b> Configure Resource Level Permissions .....	59
Quick Navigation .....	62
License Viewer .....	63
How to: Register a License .....	64
Discovery Profiles .....	65
How to: Discover Your Network .....	65
Discovery Profile Editor .....	65
Managed Resources .....	68
Common Setup Tasks .....	68
SMTP Configuration .....	69
Netrestore File Servers .....	70
<b>3 Portal Conventions .....</b>	<b>71</b>
Tooltips .....	72
Refresh .....	72
The Back Button .....	72
Show Versions .....	72
The Dock .....	73
Status Bar Alerts .....	75
Chat / Conferencing .....	76
Menu Bar .....	77
Site Map .....	77
Graphs .....	77
Portlets .....	78
Expanded Portlets .....	82
How to: Show / Hide / Reorder Columns .....	84
How to: Filter Expanded Portlet Displays .....	85
Common Menu Items .....	86
Import / Export .....	86
Sharing .....	87
How to: Share a Resource .....	88
Edit Custom Attributes .....	89
View as PDF .....	90
Tag .....	90
Audit Trail / Jobs Screen .....	91
Audit Trail Viewer .....	92

	Audit Trail Portlet.....	93
	Schedules.....	95
	Schedules Portlet.....	95
<b>4</b>	<b>Key Portlets.....</b>	<b>99</b>
	Alarms.....	99
	Expanded Alarm Portlet.....	101
	Event History.....	106
	Event Processing Rules.....	108
	How to: Create Event Processing Rules.....	109
	Rule Editor.....	111
	Event Definitions.....	128
	Event Definition Editor.....	128
	Contacts.....	133
	Locations.....	135
	Tag.....	138
	Vendors.....	139
<b>5</b>	<b>Resource Management.....</b>	<b>143</b>
	Authentication.....	143
	Container Manager.....	146
	Container Manager Expanded.....	146
	Container View.....	147
	How to: Use Containers.....	147
	Container Editor.....	148
	Map Context.....	151
	Resource Discovery.....	152
	How to: Discover Resources.....	152
	Discovery Profiles.....	153
	Discovery Profile Editor.....	154
	How to: Edit Discovery Profiles.....	154
	Managed Resource Groups.....	162
	Static Group.....	164
	Dynamic Group.....	165
	Managed Resources.....	166
	New Link.....	175
	Link Discovery.....	176
	Equipment Details.....	178
	Performance Indicators.....	179
	Interfaces.....	180
	Alarms.....	181
	Ports.....	181
	Details.....	185

<b>How to: Schedule Actions</b> .....	186
Direct Access.....	188
MIB Browser .....	188
Terminal .....	190
Ping (ICMP) .....	191
HTTP / HTTPS .....	191
Ports.....	191
Port Editor .....	194
Report Templates.....	195
How to: Create a Report Template .....	195
Report Template Editors .....	196
Reports .....	200
How to: Generate a Report .....	204
Report Editor .....	204
Branding Reports.....	206
<b>6 Visualize My Network</b> .....	<b>207</b>
How to: Create a Visualization .....	207
Configuring Views .....	208
Control and Styles .....	210
Data / Node Finder .....	213
Layout .....	216
OVERVIEW .....	219
Alarms in Visualizations / Topologies.....	219
Links in Visualization.....	220
<b>7 File Servers</b> .....	<b>221</b>
File Server Editor .....	222
File Management.....	223
How to: Backup Configurations .....	225
How to: Restore Configurations .....	227
Configuration Files .....	229
Image Repository.....	233
Firmware Image Editor .....	235
Configuration Image Editor .....	236
Deploy Firmware .....	238
How to: Deploy Firmware .....	239
Deploy Configuration.....	240
How to: Restore a single configuration to many target devices .....	241
<b>8 Monitoring</b> .....	<b>243</b>
How to's.....	243
OpenManage Network Manager Server Statistics.....	244

Resource Monitors .....	245
Retention Policies .....	248
Monitor Editor .....	251
How to: Create an SNMP Interface Monitor .....	262
How to: Create an ICMP Monitor .....	263
How to: Create a Key Metrics Monitor .....	264
How to: Create a Monitor Report .....	265
Monitor Options Type-Specific Panels .....	266
Scheduling Refresh Monitor Targets .....	276
Top [Asset] Monitors.....	276
Top Configuration Backups .....	277
Dashboard Views.....	277
How to: Create a Simple Dashboard View .....	279
Performance Dashboard .....	279
Dashboard Editor .....	281
<b>How to:</b> Create a Custom Dashboard View .....	282
Show Performance Templates .....	286
How to: Create A Performance Template .....	286
Key Metric Editor.....	289
<b>9 Traffic Flow Analyzer .....</b>	<b>293</b>
How does it work?.....	294
Setup .....	294
How to: Use Traffic Flow Analyzer .....	295
Exporter Registration .....	296
Traffic Flow Portlet .....	296
Drill Down .....	299
Search .....	301
Traffic Flow Analyzer - Example .....	301
<b>10 Change Management – ProScan .....</b>	<b>303</b>
<b>How to:</b> Use ProScan / Change Management .....	303
How to: Configure ProScan Groups .....	304
How to: Do Change Management (Example) .....	305
ProScan Portlet .....	306
Compliance Policy Summary .....	308
Creating or Modifying a ProScan Policy .....	310
How to: Create Source Group Criteria .....	316
Creating or Modifying ProScan Policy Groups .....	325
Change Determination Process .....	326
Change Determination Process Workflow .....	327
How to: Run Change Determination .....	329
Change Determination Defaults .....	329

Compliance and Change Reporting .....	329
How to: Report on Change Determination .....	331
<b>11 Storage Arrays .....</b>	<b>333</b>
Introducing Storage Arrays .....	333
Storage Array Portlet .....	333
Storage Array Portlet Expanded .....	334
General .....	337
<b>12 Actions and Adaptive CLI .....</b>	<b>341</b>
Using Adaptive CLI .....	341
Actions Portlet .....	343
Adaptive CLI Editor .....	348
General .....	349
Attributes .....	350
Scripts .....	355
Comparison .....	360
External Commands .....	360
Seeded Scripts .....	362
How to: Create a Monitor for an External Script .....	364
Adaptive CLI Script Language Syntax .....	366
Attributes .....	366
Conditional Blocks .....	367
Perl Scripts .....	368
<b>How to: Create Adaptive CLI Example</b> .....	369
Scheduling Actions .....	369
Active Performance Monitor Support .....	371
Adaptive CLI Records Archiving Policy .....	373
<b>Glossary .....</b>	<b>375</b>
<b>Index .....</b>	<b>381</b>



# Preface

Dell OpenManage Network Manager can give you automated, consolidated configuration and control of your network's resources. It is customizable, unifying multiple systems while still communicating with other software systems (like billing) in generic WSDL, XML and SOAP.

OpenManage Network Manager's *Administration Section* describes security and some of the runtime features supporting these applications. The OpenManage Network Manager Administration Section of the User Guide and *Administration Section* discuss licensing. Consult Release Notes for information about changes not covered in this *Synergy User Guide*.

## Why Dell OpenManage Network Manager?

Dell OpenManage Network Manager's benefits:

### **Productive**

Discovery and wizard-driven configuration features within minutes of installing Dell OpenManage Network Manager, you can monitor your network.

### **Easy**

Dell OpenManage Network Manager provides the network information you need, and offers advanced capabilities with minimal configuration overhead.

### **Valuable**

Dell OpenManage Network Manager often costs less to use and maintain than most other solutions.

### **Scalability**

You can scale Dell OpenManage Network Manager to almost any size.

## Key Features

The following are some key features of Dell OpenManage Network Manager:

### **Customizable and Flexible Web Portal**

You can customize the web portal, even providing custom designed views of your data assigned to individual users. You can even create web portal accounts for departments, geographic areas, or other criteria.

### **Automate and Schedule Device Discovery**

Device discovery populates Dell OpenManage Network Manager's database and begins network analysis. You can also create network discovery schedules to automatically run Discovery whenever you need them.

### **Dell OpenManage Network Manager Administration**

You can now conduct administrative tasks—adding devices, user accounts, and web portal displays—from a secure console on your network.

### **Open Integration**

Dell OpenManage Network Manager supports industry standards. It comes with an open-source MySQL database. It also uses industry-standard MIBs and protocols, and even lets you install open-source screen elements like Google gadgets to the web portal.

### **Topology**

The OpenManage Network Manager topology screen lets you create multi-layered, fully customizable, web-based maps of your network to track devices wherever they are in your network.

### **Alarms**

You can configure custom alarms to respond to hundreds of possible network scenarios, including multiple condition checks. Dell OpenManage Network Manager's alarms help you recognize issues before your network users experience productivity losses. Alarms can also trigger actions like email, executing Perl® scripts, paging, SNMP traps, Syslog messaging, and external application execution.

### **Traps and Syslog**

Dell OpenManage Network Manager lets you investigate network issues with traps and Syslog messages. You can use Dell OpenManage Network Manager to set up events / alarms and then receive, process, forward, and send syslog and trap messages.

### **Reports and Graphs**

Dell OpenManage Network Manager comes with many pre-configured reports and graphs to display data from its database. You can archive and compare reports, or automate creating them with Dell OpenManage Network Manager's scheduler.

### **Modularity**

With additional modules, Dell OpenManage Network Manager can analyze network traffic, manage services and IP address and subnet allocations. OpenManage Network Manager modules save time adding to existing Dell OpenManage Network Manager deployments to add feature functionality without requiring additional standalone software.

## Networks with Dell OpenManage Network Manager

The beginning of network management with Dell OpenManage Network Manager is Discovery Profiles of the resources on a network. After that occurs, you can configure Visualize (topology views), Resource Monitors and Performance Dashboards.

Once you have done these initial steps, Dell OpenManage Network Manager helps you understand and troubleshoot your network. For example: Suppose a OpenManage Network Manager Performance Dashboard displays something you want to troubleshoot. You can right-click the impacted device in the Visualize topology view to access configuration and actions. The color of the icon in this view indicates the highest severity alarm on the device or its sub-components. For example, red indicates a *Critical* alarm.

Displays include right-click access to the Details screen (see Equipment Details on page 178), where you can examine each section of device information and right-click to see further applicable actions. For example right-click to Show Performance, and edit and/or save that view of performance as another Performance Dashboard. Performance can also display portlets that Show Top Talkers (the busiest devices) or Show Key Metrics.

From looking at Performance Dashboards or Top [Asset] Monitors you may conclude some configuration changes made memory consumption spike. Right-click to access resource actions under File Management that let you see the current configuration files on devices, and compare current to previous. You can also back up devices (see Backup Configurations on page 225) and restore previously backed up files (see Restore Configurations on page 227). Finally, you may simply want to Resync (another right-click menu item) to insure the device and your management system are up-to-date.

### Tip

Alternatively, the Alarms portlet also lets you right-click to expose Alarm Actions.

You can right click for Direct Access – Telnet or Direct Access – MIB Browser to display a command line telnetting to the device, or an SNMP MIB browser to examine SNMP possibilities for it.

The Managed Resources portlet can display the anatomy of a Resource with its right-click actions (see Equipment Details on page 178). Click the plus in the upper right corner to see Managed Resources Expanded. This displays detail or “Snap-in” panels with additional information about a selected resource.

Reports let you take snapshots of network conditions to aid in analysis of trends, and Audit Trail Portlets track message traffic between Dell OpenManage Network Manager and devices.

## Additional Products

The following describes how to increase the power of your Dell OpenManage Network Manager installation. While the documents mentioned above describe everything available with Dell OpenManage Network Manager, your installation may provide only a limited subset of those features.

## Updating Your License

If you have a limited license — for example OpenManage Network Manager may limit discovery to a certain number of devices— then your application does not function outside those licensed limits.

You can purchase additional capabilities, and can update your license for OpenManage Network Manager by putting the updated license file in a convenient directory. Then click *License Management* in the Quick Navigation portlet item to open a screen with a button leading to a file browser (*Register License: Select File*). Locate the license file, and click the *Register License* button. Your updated license should be visible in the *License Viewer* (See *License Viewer* on page 63 for details.)

### NOTE:

If you update your installation from a previous one where you upgraded license, you must also re-register those licenses.

You must restart application server or wait up to 15 minutes before a license modification takes effect. (see *Installation and Startup* on page 28). Licenses now support three expiration formats: Never, Date certain, and a format that indicates the license will be valid for a number of days after registration.

## Online Help / Filter

Access general online help by clicking *Help* in the The Dock at the top of the screen. Help appropriate to each portlet appears when you click question mark icon on the portlet title bar.

By default, this opens a separate browser window which is not necessarily always in front of the screen that calls it. Because it is separate, you can arrange the display so the help screen does not conceal the portlet it describes. Click the *Show* button to display the contents, index and search tabs (*Hide* conceals them again), and the *Prev / Next* buttons, or clicking table of contents topics moves to different topics within the helpset.

### Tip

Sometimes your browser's cache may interfere with help's correct appearance. If you see a table of contents node without contents, you can often repair it by refreshing the panel or whole screen.

## How To: Use “How To”

Several sections of what follows contain the “How to” instructions for use. These are typically steps to follow to produce the desired result. For a look at all such steps available, refer to the *How to* section of the Index.

# Feedback

To provide your input about this software click the *Feedback* link in the lower left corner of the Dell OpenManage Network Manager screen. Provide your contact information, enter *Questions*, *Likes*, *New Ideas*, or a *Problem*, in the screen that appears next, then click *Send*.

Dorado Software responds, and often uses customer suggestions in future versions of the software.

# A Note About Performance

Dell OpenManage Network Manager is designed to help you manage your network with alacrity. Unfortunately, the devices managed or the networks that communicate with those devices are not always as fast as this software. If discovery takes a long time (it can), often network and device latency is the culprit. You can also optimize installations to be faster (see the recommendations in the Administration Section of the User Guide and *Administration Sections*), and limit device queries with filters, but device and network latency limit how quickly your system can respond.



## Tip

If you use management systems other than this one, you must perform a device level resync before performing configuration actions. Best practice is to use a single management tool whenever possible.



# Getting Started with Dell OpenManage Network Manager

## Overview

This chapter describes how to install and start Dell OpenManage Network Manager for basic network monitoring and management. For more detailed descriptions of all this software's features, consult its other manuals (the OpenManage Network Manager Administration Section of the User Guide, *Synergy User Guide, Administration Section* and *User Guide*) or the online help.

### Tip

If you want to find something but are unsure about which manual it is in, you can search all text in the Acrobat files in a single directory. You can also click on the blue cross-references to go to the target destination of cross-references in Acrobat, however for such electronic cross-references to the other documents to work, they must be in the same directory. Cross-document links do not work between documents for different versions of this software, but may provide an approximate location to consult.

If you are sure your hardware, software and network is correct and just want to get started immediately, go to Getting Started on page 27.

The Dell OpenManage Network Manager portal delivers powerful solutions to network problems, and, in addition to the OpenManage Network Manager technology documented in the following pages, Dell OpenManage Network Manager offers the following capabilities:

- Message Boards, Blogs, Wikis
- Shared Calendars
- Enterprise Chat / Messaging
- RSS Feeds
- Tagging, Ratings, Comments

The section Server on page 49 describes how to set up some of these features.

## System Basics

System requirements depend on how you use the application and the operational environment. Your specific network and devices may require something different from the recommendations for typical installations.

Generally, base the minimum configuration of any system on its expected peak load. Your installation should spend 95% of its time idle and 5% of its time trying to keep pace with the resource demands.

## Upgrading from a Previous Version

When you upgrade your OpenManage Network Manager installation from a previous version, keep the following in mind:

- Upgrading requires a new license to activate new features.
- Performance capabilities have been completely reconfigured. When upgrading from previous versions, you must (re-)create dashboards from scratch.
- The following require manual migration (export, then import) from previous versions: SMTP settings. Some scheduled items.
- You must re-create topologies as Visualizations. (suggestion: take a screenshot)
- Group Operations have been deprecated, replaced by Adaptive CLIs.
- Command monitors must be recreated, and monitors must be re-configured to monitor Adaptive CLIs that run external scripts.
- User Names / Passwords, and User Groups (Roles) are not automatically reassigned and must be created manually.

## Supported Operating System Versions

The following are supported operating system versions:

**Microsoft Windows**—The supported operating systems are: Windows 2003 (Standard, Enterprise and Web) and Windows Server 2008 (including R2 and Enterprise Edition). This is a 64-bit application, it has been tested for Windows on 64-bit operating system versions.

### NOTE:

Windows Terminal Server is not supported. The installer becomes non-responsive with Data Execution Prevention enabled. This option is disabled by default on Windows Server 2008, but is enabled on a Windows Server 2008 machine running Terminal Server.

- You must disable User Account Control if you are installing Windows Server 2008. Alternatively, you can run application server as service. Another option is to run as administrator on startappserver. In Vista, right click the startappserver icon and select run as administrator.
- Installer may halt when pre-existing bash sessions or cmd sessions are left open. Close all such sessions.

**Linux**—This application supports Red Hat (Enterprise version 5.5 or 6.0) Linux, 64-bit only. (See 32-bit Linux Libraries on page 18 for additional requirements)

### CAUTION:

For Linux, you must install no more than a single instance of MySQL—the one installed with this software. Before you install, remove any MySQL if it exists on your Linux machine.



## Linux Installation Best Practices

How you install Linux has an impact on Dell OpenManage Network Manager's installation. Here are some tested best practices:

- You can install Linux in its Desktop option, or if you select Basic Server (default) - choose additional packages: XWindows, Basic / Core Gnome Desktop without Gnome utilities, although we suspect any Gnome will work).
- Turn off SE Linux in `/etc/selinux/config`. Change `SELINUX=disabled`. This typically requires a reboot.
- You must install compatibility library from installation media (so it is compatible with installation)

```
compat-libstdc++-33.x86_64 3.2.3-69.el6 @InstallMedia.
```

Also: verify that `/etc/hosts` points to new name-use the following command and you should see similar output.

```
[qa@rh6Test Desktop]$ cat /etc/hosts
10.18.0.241rh6Test.localrh6Test# Added by NetworkManager
127.0.0.1localhost.localdomainlocalhost
::1 rh6Test.localrh6Testlocalhost6.localdomain6localhost6
```

## Upgrading on Linux

The following are best practices for upgrading from a previous OpenManage Network Manager version on a Linux machine:

- 1 Make sure Red Hat is not installed with a MySQL database option (or remove the Linux MySQL first).
- 2 Ensure you have installed the 32-bit Linux Libraries, as described below.
- 3 Verify your previous version's installation application server starts without exceptions
- 4 Back up the database, and any other resources that need manual installation. Consult Release notes for a list of these.
- 5 Proceed with the upgrade.

## Disable Firewalls

System->Administration->Firewall - You may be prompted to enter the root password; the password dialog may be hidden behind the Firewall Configuration Startup dialog.

## Directories and Permissions

Create the directory for the installation:

- 1 Open a terminal.
- 2 Change to Super User: `su <enter> password: []`
- 3 Create directory and configure its ownership and permissions:

```
mkdir /opt/  
chown [your login name] /opt/[your installation directory]  
chmod 775 /opt/[your installation directory]
```

 **NOTE:**

[your login name] is the original non-root user available when you imported the machine. Replace [your login name] with whichever user you are logged in as or will be installing as.

You may need to change the permissions on the installer in our package in order to give it execute rights. If you have used the shared folder method from above, you can give the Linux installer rights as follows:

```
chmod uga+x /[Install Media Path]/install/linux_install
```

Make sure that there is no other my.cnf file under the /etc directory. If there is, do the following:

```
mv /etc/my.cnf /etc/my.cnf.original
```

### 32-bit Linux Libraries

For Red Hat Enterprise 64 bit installations, you must identify the appropriate package containing 32-bit libtcl8.4.so (for the example below: tcl-8.4.13-3.fc6.i386.rpm for Red Hat).

 **NOTE:**

Do not use any x86\_x64 rpms; these would not install the 32-bit libraries.

Any 32-bit tcl rpm that is of version 8.4 and provides libtcl8.4.so works. You can download them from Sourceforge: [sourceforge.net](http://sourceforge.net). Download these, then issue the command:

```
rpm -ivh --force tcl-8.4.13-3.fc6.i386.rpm
```

This forces the installation of the 32-bit libraries on a 64-bit system. Ensure that your expect executable in your installation directory is properly linked by issuing the following commands:

```
[someone@RHEL5-64bit ~]$ which expect  
/opt/dorado/oware3rd/expect/linux/bin/expect  
[someone@RHEL5-64bit ~]$ ldd /opt/dorado/oware3rd/expect/linux/bin/expect  
linux-gate.so.1 => (0xffffe000)  
libexpect5.38.so => /opt/dorado/oware3rd/expect/linux/bin/  
libexpect5.38.so (0xf7fd2000)  
libtcl8.4.so => /usr/lib/libtcl8.4.so (0x0094c000)  
libdl.so.2 => /lib/libdl.so.2 (0x0033e000)  
libm.so.6 => /lib/libm.so.6 (0x00315000)  
libutil.so.1 => /lib/libutil.so.1 (0x00b8d000)  
libc.so.6 => /lib/libc.so.6 (0x001ba000)  
/lib/ld-linux.so.2 (0x0019d000)
```

Make sure that `libtc18.4.so` maps to `/lib/libtc18.4.so` An Alternative for Red Hat Linux:

- 1 Copy `/usr/lib/libtc18.4.so` from a 32-bit RH system to `/usr/local/lib/32bit` on your 64-bit Red Hat system
- 2 As root, execute: `ln -s /usr/local/lib/32bit/libtc18.4.so /usr/lib/libtc18.4.so`

## Supported Web Browsers

Supported web browsers include:

- Chrome (v 6 and above)
- Safari (v 5 and above)
- Firefox (v 3.6 and above)
- Internet Explorer (v 9 and above)

Screen resolution should equal or exceed 1280 x N pixels. Users running Safari on an Apple machine must modify Java preference to run applets as their own process. Java Preferences are under Applications > Utilities on OSX.

### NOTE:

Internet Explorer versions 8 and older display alignment issues, have slower JavaScript and Flash processing, and some transparencies do not work. Other anomalies include non-rounded corners, no alpha rendering, scroll bars in performance indicators, non-working multi-level menus, a too-large OS Images schedule form, and others. To fix these anomalies, install the Chrome plug-in at [code.google.com/chrome/chromeframe/](http://code.google.com/chrome/chromeframe/). After it installs, close IE and re-open it. The look and feel should improve.

### Tip

You can often resolve problems by refreshing the browser's display.

### CAUTION:

Opening Dell OpenManage Network Manager, or links originating within it in multiple tabs on multi-tab browsers is not supported. To see "multiple" screens, configure Dell OpenManage Network Manager's Menu Bar.

You can download and install updates if your browser or version varies from those supported. To have all Dell OpenManage Network Manager functionality, you must also install the latest version of Java (v.1.6 or later) Adobe's Flash and Adobe's Acrobat that works with these browsers. Flash for

64-bit browsers is currently a preliminary version, but you can typically run a 32-bit browser even in a 64-bit operating system, so Flash features will still be available even if you do not want to run Adobe's beta software.

 **NOTE:**

If Flash is installed, but the screen still requests it, reload the page in the browser. Also: Your screen must be at least 1250 pixels wide.

 **Tip**

When no cursor or focus is onscreen, some browsers interpret backspace as the *Previous* button.

## Single Server Sizing

The following describes hardware and sizing configuration for common Dell OpenManage Network Manager deployments. Before any deployment, administrators should review and understand the different deployment options and requirements. Consider future growth of the network when estimating hardware sizing. You can generally expand modern systems running Dell OpenManage Network Manager by adding more RAM to the host server(s). Selecting expandable hardware may also be critical to future growth. For ease of management, deployments selection best practice is to use the fewest possible servers. Standalone (single server) deployment offer the simplest and easiest management solution. Where high availability (HA) is required, you can produce the simplest deployment with as few as two servers.

### Minimum Hardware

The minimum hardware specification describes what Dell OpenManage Network Manager needs at a minimum. In such minimum installations, traffic flowing from the network to OpenManage Network Manager may exceed the capacity of the hardware. When estimating the size of a deployment, it is important to understand the applications configurations in the target environment. Applications that are typically the most demanding of resources are Traffic Flow Analyzer (TFA), Event Management and Performance Monitoring.

**REQUIRED Minimum hardware**—6GB RAM, dual core CPU, 200 GB 7200 RPM Disk.

#### Supports:

- Standalone installations (Single Server) is supported when high-resource demand applications are used minimally.

**RECOMMENDED Minimum hardware:** 8GB RAM, quad core CPU, 400 GB 10,000 RPM Disk

#### Supports:

- Standalone installations (non-distributed).

# Sizing for Standalone Installations

The following are suggested sizing guidelines for your Dell OpenManage Network Manager system.

Operating System / Disks / RAM / Hardware	Network Size	Devices <sup>2</sup>	Application Constraints <sup>3</sup>	Installation Changes to Heap (RAM) Settings
64-bit OS with 6GB RAM or 32-bit OS with 4GB RAM  All below are 64-bit OS's:	<5 Users	<20	<2Mbs Internet egress and a 1:1000 sample rate	Use defaults: (1 or 2GB application server heap (32 v. 64-bit) 512M database <sup>4</sup> , 768M Synergy
8GB RAM, single disk, consumer level PC	Single-site, less than 10 concurrent users	<100	<2Mbs Internet egress and a 1:1000 sample rate	3GB application server heap, 2GB database, 1G Synergy
12GB RAM, single disk, business level PC	Single-site, less than 25 concurrent users.	< 500	< 10Gbs Internet egress and a sample rate of 1:1000	4GB application server heap, 3GB database, 3G Synergy
16GB RAM, multi-disk, server level PC	Medium-large network, up to 50 concurrent users	< 1,000	< 50Gbs Internet egress and a sample rate of 1:1000	5G application server heap, 4G database, 4.5G Synergy
32GB RAM, multi-disk, server level PC, recommend fast disk array or SSD drive array for the many database actions	Large network, up to 100 concurrent users	< 2,000	< 200Gbs Internet egress and a sample rate of 1:1000	10G application server heap, 8G database, 9G Synergy

<sup>1</sup> Assumptions: Servers have at least four cores and are no more than four years old. As memory and usage increases, the number of CPU cores increase. Two cores can work for the most basic installations, but are not recommended.

<sup>2</sup> Each device is equivalent to a L2 or L3 switch with a total of 48 interfaces per device being monitored. For each of devices not being monitored for 48 interfaces, one can add another 50 devices to the overall inventory for ICMP-only monitoring.

<sup>3</sup> Application Constraints are most relevant to Traffic Flow Analysis, Performance Management, and Event Management.

Traffic Flow Analysis ratings map to constant throughput divided by sample rate, as in bandwidth / sample rate. 20G / 2000 is easier to manage than 20G / 1000. 20G / 1 is a thousand times more demanding than 20G / 1000. Best practice is to avoid such high sample rates. The bandwidth the hardware your Dell OpenManage Network Manager installation can support is dramatically lower in such cases. Best

practice is to sample a maximum of one traffic flow for every 1000 (1:1000). Higher sampling rates degrade database performance and increase network traffic without adding any significant statistical information.

Performance Management can support 600 inserts per second using a single disk (SSD) Drive. 1 insert = 1 monitored attribute. Expect better performance as you add more drives (and worse performance with slower drives).

Event Management can support a sustained 1200 traps /sec using a single (SSD) drive. Expect better performance as you add more drives (and worse performance with slower drives).

<sup>4</sup> Database memory settings increase as the number of database hits increases. At the 32GB level best practice is to use an SSD drive or fast disk array because of the large number of database actions possible.

You can start and stop the client portion of the software without impacting the application server. Device monitoring stops when you stop the application server or turn off its host machine. The client can also be on a different machine than the application server.

 **NOTE:**

See Starting Web Client on page 33 for more information about using web access to this software.

## **64-bit**

Since Dell OpenManage Network Manager has a web server, demands on 32-bit system resources are near their limits. A standalone 32-bit system with Application server, Web server, and database requires nearly all addressable memory, and is therefore not supported. Applications like Traffic Flow Analyzer and Performance Monitoring require even more memory. For these reasons, and for future scalability, do not install this software on 32-bit systems.

## **Tablets, phones and iPads**

Dell OpenManage Network Manager detects mobile devices and pads. For smaller screens, the Navigation bar collapses to the left hand side and the page only displays a single column. Some limits apply:

- Since touch devices do not support right click, the first time clicking on a row selects it. A repeat click launches a menu displaying the available actions. Click the one you want.
- Charts that require flash may not work (some have HTML5 backup).
- Visualize / Topology is unavailable.
- Phones may limit views further

## **Network Basics**

OpenManage Network Manager communicates over a network. In fact, the machine where you install it must be connected to a network for the application to start successfully. Firewalls, or even SNMP management programs using the same port on the same machine where this software is installed can interfere with communication with your equipment.

Dealing with any network barriers to communicating with OpenManage Network Manager, any required initial device configuration to accept management, and managing security measures or firewalls—all are outside the scope of these instructions. Consult with your network administrator to ensure this software has access to the devices you want to manage with the Protocols described below.



### Tip

One simple way to check connectivity from a Windows machine to a device is to open a command shell with `Start > Run cmd`. Then, type `ping [device IP address]` at the command line. If the device responds, it is connected to the network. If not, consult your network administrator to correct this. No useful information comes from disconnected or powered-down devices.

## Name Resolution

OpenManage Network Manager server requires resolution of equipment names to work completely, whether by host files or domain name system (DNS). The application server cannot respond to hosts with IP addresses alone. The application server might not even be in the same network and therefore the host would be unable to connect.

If your network does not have DNS, you can also assign hostnames in `%windir%\System32\drivers\etc\hosts` on Windows (`/etc/hosts` in Linux). Here, you must assign a hostname in addition to an IP address somewhere in the system. Here are some example hosts file contents (including two commented lines where you would have to remove the `#` sign to make them effective):

```
#      102.54.94.97      rhino.acme.com          # source server
#      38.25.63.10      x.acme.com              # x client host
127.0.0.1      localhost
```

## Protocols

OpenManage Network Manager uses the following protocols: TCP/IP, SNMP, HTTP/S, UDP Multicast.

## Overriding Properties

Dell OpenManage Network Manager lets you fine-tune various features of the application. Rather than lose those changes if and when you upgrade your application, best practice is to override changes. To do this, first change the provided file `\oware\synergy\conf\server-overrides.properties.sample` to `server-overrides.properties`, and enable the properties within it by uncommenting them, and altering them to fit your needs. The comments in this file provide more information.

You can also override application server-related properties in `\owareapps\installprops\lib\installed.properties`.

## Fixed IP Address

OpenManage Network Manager includes a web server and application server which must be installed to hosts with fixed IP addresses or permanently assigned Dynamic Host Control Protocol (DHCP) leases.

### If you do change your host's IP address

To accommodate a changed IP address, first delete the contents of `\oware\temp`. Change your local IP address anywhere it appears in `\owareapps\installprops\lib\installed.properties`. Then restart your machine.

Alternatively, in a shell, after running `oware` to set the environment, you can run `ipaddresschange -n` followed by the new IP address.

#### NOTE:

If you change your host's IP address, you must also change the Virtual host IP to the new IP address in `Manage > Control Panel > Portal`.

If you do change your server's IP address, you must also change the URL for web client access in your browser.

## Authentication

For successful discovery of the resources on your network, this software requires authenticated management access to the device. To get this access, you must provide the correct SNMP community strings, WMI login credentials, and any other command-line (Telnet / SSH) or browser (HTTP/HTTPS) authentication, and SNMP must be turned on, if that is not the device's default. Some devices require pre-configuration to recognize this management software. Consult your network administrator or the device's manuals for instructions about how to enable those. See Authentication on page 143 for more.

## Supported PowerConnect Models

Refer to release notes for a list of supported devices. You can also look at the HTML files in the `SupportedDevices` directory of your installation source for information about supported devices and operating systems.

## Windows Management Interface

The Windows Management driver currently supports any Windows based operating system that supports the Windows Management Interface (WMI).

Windows Management is always installed on the following operating systems (or later):

- Windows XP Professional (with a browser other than Internet Explorer)



- Windows 2003 All Editions
- Windows Vista

The login credentials must be for an administrator on the installation host for complete functionality. Both this and .NET installation are requirements for any installation managing devices supported by this driver.

This driver supports global group operations.



**NOTE:**

Discovery may display benign retry warning messages in the application server shell or log. You can safely ignore these.

## Prerequisites

Before installing this software to manage other computers with a Windows Management Interface driver (assuming you are installing that driver), if you do not already have it installed, you must download and install the Microsoft .Net framework version 3.0 or later on the application server. For complete functionality, the WMI login for this software must be a login for a domain user who also belongs to the administrator group on the WMI device. Both are requirements for any installation managing WMI devices.

The following are common Windows Base prerequisites:

**Credentials**—You must use administrative credentials to manage the computer system.

**Firewall**—Some firewalls installed on the computer may block Windows Management requests. Allow those you want to manage. (See Firewall Issues below.)

**License**—Make sure you have the proper Windows Base driver license installed. If you have a Dell-only license and are discovering a non-Dell computer, discovery does not work. Or if you have a Dell license for desktop discover you cannot discover a server.

License come in the following types:

- Major Vendor by Name—For example: Dell, Compaq, HP, Gateway
- Server/Desktop individual license support
- Generic computers—Non-major vendors
- ALL—This gives the driver all capabilities for any computer system

## Firewall Issues

Configure the firewall between your server and the Internet as follows:

- Deny all incoming traffic from the Internet to your server.
- Permit incoming traffic from all clients to TCP port 135 (and UDP port 135, if necessary) on your server.
- Open Port 445 (WMI)

- Permit incoming traffic from all clients to the TCP ports (and UDP ports, if necessary) on your server in the Ports range(s) specified above.
- If you are using callbacks, permit incoming traffic on all ports where the TCP connection was initiated by your server.”

WMI queries will succeed only if you add the User account to local admin group. Refer to the Microsoft knowledgebase articles for the way to do this. For example: Leverage Group Policies with WMI Filters: [support.microsoft.com/kb/555253/en-us](http://support.microsoft.com/kb/555253/en-us)

For user rights for WMI access, see: [www.mcse.ms/archive68-2005541196.html](http://www.mcse.ms/archive68-2005541196.html)

See also: *Service overview and network port requirements for the Windows Server system* ([support.microsoft.com/kb/832017/](http://support.microsoft.com/kb/832017/))

## Web-Based Enterprise Management (WBEM) Driver

The Web-Based Enterprise Management driver currently supports operating systems supporting the Web-Based Enterprise Management interface (WBEM).

WBEM is always installed on the following operating systems versions (and later):

- Red Hat Linux 5.5 or 6.0
- VM Ware (ESX) with WBEM installed.

You can install Web-Based Enterprise Management on some other systems if they do not already use it, but monitored devices must have this installed.

### NOTE:

To verify WBEM is running on your system, run the following command: `ps -e | grep cim`. You should see a process labelled `cimserver`.

## Installing WBEM on Red Hat

For Red Hat 5, the latest supported release for WBEM is `tog-pegasus-2.7.0-2.e15_2.1.i386.rpm` and this is what you need to download once you have logged into the Red Hat network.

Install this as follows:

Install: `rpm -ih tog-pegasus-2.7.0-2.e15_2.1.i386.rpm`

Upgrade: `rpm -Uh tog-pegasus-2.7.0-2.e15_2.1.i386.rpm`

To determine if `wbem` is running, run `ps -ef | grep cimserver` in a shell.

To start | stop | get status of the WBEM service:

```
tog-pegasus start | stop | status"
```

If the system is running Fedora, then you can access `tog-pegasus` updates at this site: [admin.fedoraproject.org/pkgdb/packages/name/tog-pegasus](http://admin.fedoraproject.org/pkgdb/packages/name/tog-pegasus)

## WBEM Prerequisites

The following are common prerequisites:

**Credentials**—WBEM credentials have a role in discovering the device. Your system must have access to the computer using Administrative only credentials. These are the same credentials as the user installing WBEM on the device.

Telnet / SSH credentials are necessary for other supported applications.

For full functionality, this WBEM device driver requires administrative (root) access. Many devices may only allow root logins on a local console.

In such cases, configure the Telnet/SSH authentication for these devices to login as a non-root user—and, in Authentication Manager, enter *su* in the *Enable User ID* field and enter the root user's password in *Enable User Password* in that same authentication. This enables full device management functionality with root access.



### NOTE:

Credentials for Telnet / SSH should have a privilege level sufficient to stop services and to restart the computer system.

**Firewall**— Some firewalls installed on the computer may block Web-Based Enterprise Management requests. Allow those you want to manage.

**License**—Make sure you have the correct WBEM driver license installed. Licenses come in the following types:

- Major Vendor by Name - Such as Dell, Compaq, HP, Gateway.
- Server/Desktop individual license support.
- Generic computers - non-major vendors.
- ALL - this gives the driver all capabilities for any computer system.



### CAUTION:

If you discover an Amigopod host that does not have its SNMP agent turned on, Dell OpenManage Network Manager labels it a WMI or WBEM host rather than an Amigopod host.

# Getting Started

The following section outlines the steps in a typical installation and subsequent first use. Because the software described here is both flexible and powerful, this section does not exhaustively describe all the details of available installations. Instead, this Guide refers to those descriptions elsewhere in the OpenManage Network Manager *User Guide* or online help.

A typical installation means doing the following:

**Installation and Startup** below includes instructions for a basic installation. If you have a large network, or anticipate a large number of web clients, then best practice is to install Dell OpenManage Network Manager as the Administration Section of the User Guide guide instructs.

**Administering User Permissions**—You can also set up users, device access passwords, and groups for users, as you begin to use it. See Control Panel on page 34.

**Discovering Resources**—After you install the application, you must discover the equipment you want to manage, and model it in the Dell OpenManage Network Manager database. See Discovery Profiles on page 65.

**Resource Management**—See Managed Resources on page 68, and Chapter 4, Resource Management in this Guide.

**Configuration Management**—Use Dell OpenManage Network Manager to backup, restore, and compare configuration files. See Top Configuration Backups on page 277.

**Problem Diagnosis**—See Alarms on page 99 for information about Fault Management.

**Network Troubleshooting**—See Alarms on page 99, and Chapter 7, Monitoring for details of Dell OpenManage Network Manager's performance management capabilities.

**Reports**—Run reports to clarify the state of your network and devices. See Reports on page 200 for details.

**Real-time Diagnosis through Collaboration**—Collaborate with others about network issues, both by sending them messages that display the device conditions of concern, and with online chat within Dell OpenManage Network Manager. See Sharing on page 87, and Status Bar Alerts on page 75 for details.

**Unified View**—You can scale your Dell OpenManage Network Manager installation to handle the largest, most complex environments with distributed deployment.

Finally do not neglect what Common Setup Tasks on page 68 describes.

## Installation and Startup

Application server produces the Dell OpenManage Network Manager information for web clients. It monitors devices, and produces the output which the web server then makes available for those web clients. See Linux Prerequisites on page 30 for advice about installing to Linux.

Initiate installation by executing `win_install.exe` (Windows) or `linux_install` (Linux). Click through the installation wizard, accepting the license and making the appropriate entries.

During some installations, one screen lets you select the application's memory size. Best practice is to select the largest available on your hardware while leaving sufficient memory for the operating system.

## Heap

Memory on a single machine installation serves the operating system, database and web server. You can configure the selected application server heap memory size any time, with the following properties in `\owareapps\installprops\lib\installed.properties`:

```
oware.server.min.heap.size=8192m
oware.server.max.heap.size=8192m
```

To manually change Dell OpenManage Network Manager web portal heap settings, change the `setenv.sh` file:

```
JAVA_OPTS="$JAVA_OPTS -Dfile.encoding=UTF8 -Xmx1024m -XX:MaxPermSize=256m"
```

The file is in `/opt/dorado/oware/synergy/tomcat-x.x.x/bin`. Add the `export` directive in front of the line and change the `-Xmx [max memory]` setting as appropriate. For example, for 8G:

```
export JAVA_OPTS="$JAVA_OPTS -Dfile.encoding=UTF8 -Xmx8192m -
XX:MaxPermSize=256m"
```





### CAUTION:

To manage Windows systems—in single server deployments, you must install this application on a Windows host. In distributed deployments, a mediation server that supports WMI must communicate to managed Windows systems.

Windows installation also installs Internet Information Services (IIS)—formerly called Internet Information Server. That installation does not turn IIS on by default. Do not enable IIS on the host(s) running Dell OpenManage Network Manager.

Also: Do not install if you are logged in as user “admin.”

Installation and startup include:

- Running the installer, responding to its prompts.
-  **Starting application server.** In Windows, you can use the *Start* button (*Start* > OpenManage Network Manager > *Start application server*), or type `startappserver` in a command shell, or right-click the server manager tray icon and select *Start* (if you have installed Dell OpenManage Network Manager as a service and that icon is red, not green).
-  **Starting web server.** If this does not auto-start, you can use the *Start* button (*Start* > OpenManage Network Manager > *Synergy Manager*), or right click the web server’s tray icon to start it. You can also double-click this icon and automate web server startup.

On Linux start (or stop) the web server with scripts `startportal.sh start` (or `startportal.sh stop`) located in the `oware/synergy/tomcat-x.x.x/bin` directory.

- **Starting the Client.** The client provides the user interface. In Windows, click *Start* > OpenManage Network Manager > *Synergy*, or after starting the web server, open a browser and go to the web address `hostname:8080` where `hostname` is the name of the machine running application server (or its IP address). See Starting Web Client on page 33 for more information.



**CAUTION:**

If you are using Dell OpenManage Network Manager in an environment with a firewall, ports 8080 and 8082 must be open for it to function correctly. If you want to use cut-through outside of your network then ports 8082 – 8089 must be open. Dell OpenManage Network Manager uses the first one available, so typically 8082, but if another application uses 8082, Dell OpenManage Network Manager uses 8083 and so on.

- Start using Dell OpenManage Network Manager as outlined in Getting Started on page 27, or below.

## Linux Prerequisites

If you are installing on Linux, you must log in as a non-root user. Linux installation prompts you to run some additional scripts as root.

When installing to Linux, ensure you are installing as a user with the correct permissions, and are in the correct group. You must configure the installation directory so this user and group have all permissions (770, at least). You may install without any universal (“world”) permissions. However, you must create a home directory for the installing user.



**NOTE:**

All files created during installation respect a `umask` of 007. All files from `setup.jar` are 770. Files from `ocpinstall -x` are set for 660. Bin scripts from `ocpinstall -x` are 770.

Best practice is to install as the user designated as DBA and admin of the system (*not* root user). If necessary, create the appropriate user and login as this user for running the install program. The installing user must have create privileges for the target directory. By default, this directory is `/dell/openmanage/networkmanager`.



**CAUTION:**

Linux sometimes installs a MySQL database with the operating system. Before you install this application, remove any MySQL if it exists on your Linux machine.



**NOTE:**

To set the environment correctly for command line functions, after installation, type `oware` (or `. /etc/.dsienv` in UNIX—`[dot][space]/etc/[dot]dsienv`) before running the specified command.

**Also:** This application can run on any Linux desktop environment (CDE, KDE, Gnome, and so on) but the installer will only install shortcuts for CDE.

## File Handles

Best practice is to modify file handles for Linux. If you do not do this, exceptions appear in application server log every fifth minute. To prevent this, alter `/etc/security/limits.conf`. Here, administrators can set hard and soft limits for the file handles for users and user groups. These settings take effect on reboot. Best practice is to set the following for OpenManage Network Manager on a single machine:

```
<Installing User> soft nofile 65536
```

```
<Installing User> hard nofile 65536
```

`<Installing User>` is the installing user login. Set these higher for more heavily used systems. You can also check/set file handles temporarily using the `ulimit -H/Sn` command. Like the following:

```
$ ulimit -Hn
```

```
$ ulimit -Sn
```



## How To:

### Set Linux Permissions

These following ensures appropriate permissions exist so that the install succeeds on Linux. Your steps may vary slightly depending on the version on which you install.

- 1 Create a user, for example “redcell.”
- 2 Typically the redcell user’s home directory resembles `/export/home/redcell`.
- 3 In any case, ensure that user redcell owns its home directory (the `/export/home/redcell` directory).
- 4 Create `/dell/openmanage/networkmanager`, and ensure that your user (redcell) owns `/dell/openmanage/networkmanager`  
`/dell/openmanage/networkmanager` is Dell OpenManage Network Manager’s installation root.
- 5 If necessary, unzip the downloaded installation package into a subdirectory under user redcell’s home directory.
- 6 Ensure the unzipped script file `linux_install` has execute permissions.
- 7 Log in as user redcell



#### CAUTION:

Do *not* install root. During the installation a prompt appears to execute a script as root. This means you need root password and must open another shell where you act as root.

- 8 Execute `linux_install`, this begins the installation process, and follow the prompts.

## Uninstalling

Use Control Panel to uninstall in Windows. Uninstall by running the following on Linux:

```
$OWARE_USER_ROOT/_uninst/uninstall.sh
```



You must uninstall from Linux as root. No graphic wizard appears, and you must respond to the command-line prompts as they appear.

## SNMP in Multi-Homed Environment

Trap listener, Inform listener and all outbound SNMP requests must bind to a specific interface in a multi-homed environment. This interface is considered appropriate to use for all network-facing SNMP activity. By default, this is localhost, interpreted as the application's local IP value (the NIC selected at installation time). The following text in installed.properties provides a specific IP address to control outbound SNMP interface binding on the local machine:

```
# specific interface used for all NMS initiated
# communications to the network
com.dorado.mediation.outbound.address=localhost
```

Include the following text and provide a specific IP address to control inbound (listener) interface binding on the local machine:

```
#
# specific interface used for binding mediation
# listeners such as SNMP trap listener
com.dorado.mediation.listener.address=localhost
```

Events with no corresponding definition appear as alarms of indeterminate severity. The only way to change behavior of an unknown event in this version would be to locate the missing MIB and load it into the system. This creates the missing event definition(s) needed to specify explicit behaviors.

## Perl

If you install Perl to take advantage of this application's use of Perl Scripting capabilities, you must install it on the path on the application server and mediation server host. Best practice is to use Perl version 5.10 or later because some applications also require Perl as well as the Perl module `Net::Telnet`.

This application does not package Perl. If you want to use the Perl scripting features, you must make sure your system has Perl installed. You can find information about Perl at [www.perl.com](http://www.perl.com). Follow the downloads link to find the recommended distribution for your specific platform. (See Adaptive CLI Script Language Syntax on page 366)



One of the recommended Perl packages is from ActiveState which can be found at:  
[www.activestate.com/activeperl/](http://www.activestate.com/activeperl/)

## Starting Web Client

You can also open the client user interface in a browser. See Supported Web Browsers on page 19.  
The URL is

```
http://[application server hostname or IP address]:8080
```

The default login user is *admin*, with a password of *admin*. The first time you log in, you can select a password reminder. If you have forgotten your password, click the *Forgot Password* link in the initial screen to begin a sequence that concludes by mailing your user's e-mail address a password.



### CAUTION:

For this forgotten password sequence to work, you must configure users' e-mails correctly. Click the link that is your user name in the upper right corner of the portal to configure your account's settings for this and other things. The same configuration settings are available in Control Panel's tabs labeled as your login.

The *application server hostname* is the name of the system where OpenManage Network Manager is installed.

## HTTPS

You can connect to application server securely by configuring the included Apache Tomcat server for secure access. Consult your favorite search engine for more detailed information about setting up SSL with Tomcat web servers.

The following sections discuss typical administrative steps in getting started, once you have installed OpenManage Network Manager. See Getting Started on page 27 for a list of, and links to, other initial tasks once you have installed Dell OpenManage Network Manager.

## Changing the Session Timeout Period

The timeout for the web portal extends automatically if data is changing onscreen. Nevertheless, you can change the timeout period with (non-override-able) properties in some files, as follows:

You must modify two `web.xml` files with the same values to alter the session timeout. One controls the overall server and the other is the push servers for Async-based views. These `web.xml` files are in the following directories:

```
/dorado/oware/synergy/tomcat-XX/webapps/ROOT/WEB-INF/web.xml
```

And

```
/dorado/oware/synergy/tomcat-xx/webapps/netview/WEB-INF/web.xml
```

The xml element that contains the session timeout is

```
<session-config>
```

```
<session-timeout>30</session-timeout>
</session-config>
```

The `portal.properties` file is in `/portal/portal-impl/classes`. The property containing the session timeout (in minutes) is:

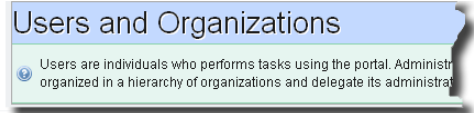
```
session.timeout=30
```

## Control Panel

To configure access to Dell OpenManage Network Manager, you must be signed in as a user with the permissions. (The default `admin` user has such permissions.) The *Go to > Control Panel* menu item opens a screen with the following tabs of interest:

- [My Account]
- RCSynergy / [Domain]
- Portal > Users and Organizations
- Portal > Roles
- Portal > Portal Settings
- Portal > [Other]
- Redcell > Permission Manager
- Redcell > Database Aging Policies (DAP)
- Redcell > Data Configuration
- Redcell > Mediation
- Redcell > Filter Management
- Server

Tips describing these screens and fields appear when you hover the cursor over fields, or click the blue circle around a question mark next to them. This blue circle can also toggle the appearance / disappearance of the tip.



Users with less-than-Administrator permissions may not see all of the features described in this guide.

## Search Indexes

Sometimes Dell OpenManage Network Manager may display Control Panel objects like users, roles, and organizations inaccurately. This occurs because search Indexes need to be re-indexed every so often, especially when changes to roles, users and organizations are frequent.

To re-index go to Control Panel > Server Administration and then click on the *Reindex all search indexes*. This takes little time.

## [My Account]

To configure information for your login, look for the bar titled with your account login's name. It has the following lines beneath it:

**My Account**—This configures your information as a user, including your e-mail address, password, and so on.

**My Pages**—This manages public and private pages visible to you as a user. Use the tree of pages that appears on the left of this screen to drag and drop pages in the order you want. Notice that you can also configure the look and feel, the logo that appears and other settings with the editor screens on the right.

**Contacts Center**—This configures contacts, in other words, people within your system that you are following. Click the *Find People* link to see a list of potential contacts within your system. You must click *Action > Follow* to see them listed in the *Contacts Home*. Use the *Action* button to explore other possibilities.

The contact has to approve you in their requests. To *Follow* means you want to receive the followed person's activity stream, blog postings, and so on. *Friending* means your friends can see your activity and you can see theirs. They have to accept any *Friend* request.



You can export vCards for all contacts in the system to use with other software that uses contacts. For example: e-mail clients.

## RCSynergy / [Domain]

RCSynergy appears as a default domain name in *Control Panel*. *Global* and *[My Login's] Site* configurations appear as additional items to configure when you click the down arrow to the right of RCSynergy.

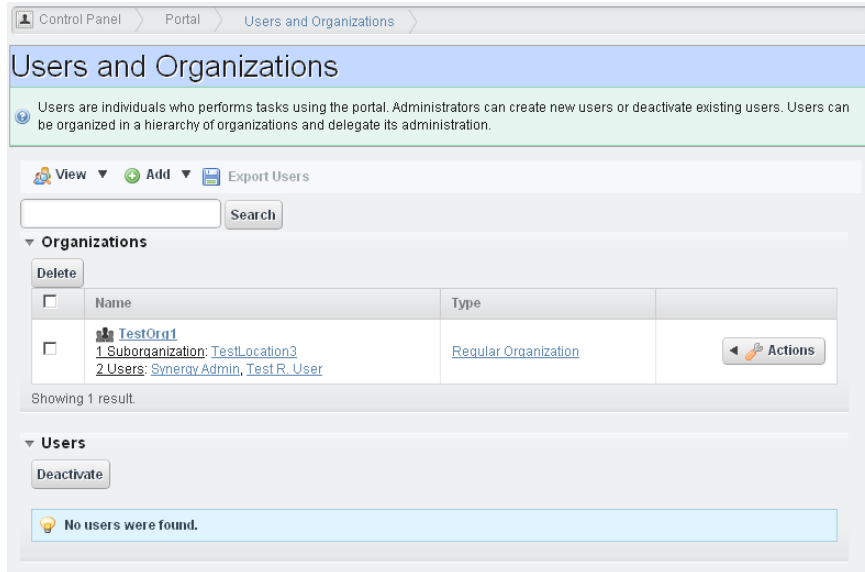
The items under this label configure the overall look and feel of the portal, reference information, and so on. See the tooltips for more complete descriptions. This also configures pages, documents, calendars, blogs, wikis, polls and so on.

*Social equity* lets you alter measurements for user participation in organizations. Equity values determine the reward value of an action; equity lifespans determine when to age the reward of action.

## Portal > Users and Organizations

Create organizations and locations in addition to groups with the appropriate permissions (operators, administrators, and so on) in these screens. Users are individuals who performs tasks using the portal. Administrators can create new users or deactivate existing users. Users can be organized in a hierarchy of organizations and delegate its administration.

After creating them, add Users to roles which configure their permissions for access and action.



The screenshot shows the 'Users and Organizations' control panel. At the top, there are navigation tabs for 'Control Panel', 'Portal', and 'Users and Organizations'. Below the title bar, a green box contains a message: 'Users are individuals who performs tasks using the portal. Administrators can create new users or deactivate existing users. Users can be organized in a hierarchy of organizations and delegate its administration.' Below this, there are buttons for 'View', 'Add', and 'Export Users'. A search bar with a 'Search' button is present. The main content is divided into two sections: 'Organizations' and 'Users'. The 'Organizations' section has a 'Delete' button and a table with columns for 'Name' and 'Type'. The table shows one organization named 'TestOrg1' with a 'Regular Organization' type. Below the table, it says 'Showing 1 result.' The 'Users' section has a 'Deactivate' button and a message box that says 'No users were found.'

### NOTE:

By default, every user is assigned to the role *User*. To assign a new user to specific permissions only, remove all rights on the *User* role, or confine its permissions to those that are universal first. Even though you don't see that user assigned to the *User* role, Best practice to spend some time designing your system's security before creating users, organizations and roles.

When you are signed in, edit your user information by clicking the link with your username in the top right corner of the screen. Your user name does not appear in this screen.

Notice that if you select *View > Hierarchy* you can see organizations, grouped together with their component locations, groups and users.



### How To:

#### Add Users and connect them to Roles

Add Users with the following steps:

- 1 Click *Go to > Control Panel* and navigate to *Portal > Users and Organizations*.

- 2 Click the *Add > User* menu item at the top of the *Users and Organizations* screen.
- 3 Enter the details of the new user. If you are editing an existing user, more fields appear. *Screen Name*, and *Email Address* are required. Optionally, you can enter *Name*, *Job Title*, and so on.
- 4 After you click *Save* notice that the right panel expands to include additional information. Make sure you specify a *Password*.
- 5 Notice that if you are editing an existing user, or creating a new one, you can use the links on the right to configure connections with *Roles*. Roles, in particular, configure the OpenManage Network Manager functional permissions for that user. For example the group of *Operators* would likely have more limited capabilities than *Administrators*.
- 6 Click *Save* again, and the user you just configured should appear listed in the *Users and Organizations* screen when you select *View > All Users*.
- 7 To assign a user to a role, click *Action > Permissions* and check the appropriate box next to the role. Configure OpenManage Network Manager functional permissions for these roles in Roles (see Redcell > Permission Manager on page 42).



### Tip

You can *Export Users* to a comma-separated value (CSV) file.

Once you have configured a user, you can click *Action* and to do the following:

**Edit**—Re-configure the selected user. Select the user's Role in the editor, too. Roles configure access and action permissions.

**Permissions**—Manage the user's access to and control over various parts of the portal.

**Manage Pages**—Configure the *Public* or *Private* pages for a user, depending on the selected tab. Possible actions here include changing the look and feel of pages (for computers and mobile browsers), adding pages and child pages, and importing or exporting page configurations. Notice that you can configure meta tags, and javascript on these pages too.

Exports are in .tar format, and go to the download location configured in the browser you are using. The export screen lets you select specific features, and the date range of pages to export.



### Tip

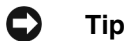
If you want to set up several pages already configured elsewhere for another user, or even for an entire community of users, export those pages from their origin, then *Manage > Pages* menu for the user or community.

**Impersonate User**—Open a web client with the same permissions as the user configured here.

**Impersonate User (Opens New Window)**—This allows you to see the effect of any configuration changes you have made on a user. The new window (typically a new tab) also lets you click the *Sign Out* link in the upper right corner where you can return to your original identity impersonation concealed.

**Deactivate**—Retires a user configured on your system. You can also check users and click the *Deactivate* button above the listed users. Such users are not deleted, but are in a disabled state. You can do an Advanced search for inactive users and *Activate* them or permanently delete them.

Your organization has a number of geographic locations and you plan to manage the network infrastructure for all these locations using RC7 Synergy. You can define the geographic locations to which devices can be associated. This will help you manage and view your network, grouped by location or branches. See Locations on page 135 for the specifics about the portlet where you can set up locations.



### Tip

To edit your own information as a signed-in user, simply click your login name in the upper right corner of the portal screen.

## Organizations

Create Organizations just as you would create Users. You can create a *Regular* or *Location* type of organization.



### NOTE:

You must first create a *Regular* organization to be the parent for a *Location*.



## How To:

### Configure Organizations

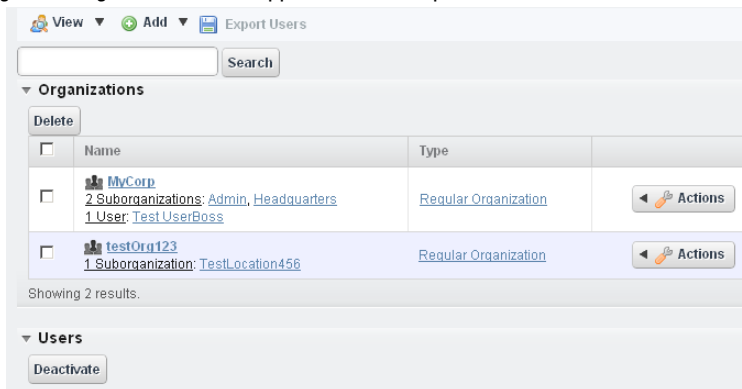
Follow these steps to configure organizations. Associating organizational roles with organization members empowers them to exercise the associated permissions within the organization's site(s).

- 1 Create a new *Regular* organization (*Add > Regular Organization* named MyCorp) as the parent of location organizations.
- 2 Notice that you can add much more identifying information once you have saved the basics (*Name* and *Description*) for the organization. This includes an *Organization Site* (a checkbox) that would create a separate portal for the organization, to which you can add and configure pages, portlets, and so on.
- 3 Create two *Location* organizations (*Add > Location*, for example Admin and Headquarters). Select MyCorp as the parent when you create the organization.
- 4 Create users in MyCorp. TestUserA, TestUserB, and TestUserBoss.

- As you create these users, add each to one of the MyCorp organizational children, Admin or Headquarters.

**Tip**

Notice that you can *View > Hierarchy* to see the parent / child relationships between organizations. Users unassigned to organizations also appear below this portion of the screen.



- Click MyCorp, and a screen appears displaying its components and a management menu where you can add additional properties.
- Click *Assign Organization Roles* in the MyCorp menu.
- Select *Organization Administrator* from the default roles available.  
If you need permissions other than this administrative user provides, you can create an organization role with the correct permissions in Portal > Roles.
- Click the *Available* tab, and select TestUserBoss as the organization’s administrator.
- Click *Update Associations*.
- You can click the Admin location, and similarly configure its user as associated with an organizational role. Do the same for Headquarters.

**Tip**

You are a member of the organization you created, because you created it. By creating an organization, you become both a member and have the Organization Owner role, which gives you full rights to the organization.

## Public / Private Page Behavior

Public pages are visible to everyone; private pages are only visible to the user who created them, and are not vulnerable to others changing their arrangement. Page Standard settings are *Max Items*, *Default Filter*, *Max Items per Page*, and *Column Configuration*. These persist for Admin users or for users who have the portlet on their Public or Private pages (which makes them the owner of that instance).

Some portlets provide extra settings—for example Alarms portlet’s the charting options, or the *Top N* portlets number of Top Items. These persist too.



### Tip

*Max Items*, *Max Items Per Page* and *Columns* persist for both the summary and maximized portlets independently. For example: If *Max Items* is 50 in minimized mode it does not affect the *Max Items* in the Maximized window state. This lets you configure modes independently.

Dell OpenManage Network Manager remembers the default sort column and order per user, whether the user has Admin rights or not. The Sort Column/Order (Descending/Ascending) is also shared between both summary and maximized portlets. A sort on IP Address in Resources persists if you expand the summary portlet to maximized mode.



## How To:

### Add and Configure User Roles / Permissions

Add and configure User Roles with the following steps:

- 1 Click *Go to > Control Panel* and navigate to *Portal > Roles*.
- 2 Click the *Add* tab under the heading at the top of the page, and select *Regular Roles*. Notice that you can also add roles that configure permissions for sites and organizations.
- 3 Enter the details of the new role (*Name*, *Title*, *Description*), then *Save* it.
- 4 Click *Portal > Roles' View All* button to see a list of available roles, including the one you added.
- 5 By clicking the *Action* icon to the right of any listed Role, you can also select the role’s permissions to alter web portal access in a subsequent screen.
- 6 Click *Add* to add permissions. Click the checkboxes to enable the type of permission desired.
- 7 To do more with Dell OpenManage Network Manager’s functional permissions, go to the *Redcell > Permission Manager*, and click to open this screen.
- 8 The Role to Permission mapping screen appears. Click the *Edit* button to the right of listed Roles to see and configure available permissions.
- 9 Click *Advanced* to see available permissions organized by *Read*, *Write*, *Execute*, *Add* or *Delete* actions.



- 10 After you have selected permissions, click *Apply* to accept them and add them to the role.  
Notice that you can revisit this role, manage it and its membership with the *Action* button to the right of the role. You can also add users to the group by selecting and editing that user.

## Portal > Roles

Roles determine the applications permissions available to users assigned them; manage them in this screen. To configure functional permissions for the application, see Redcell > Permission Manager on page 42.

Click *Add* to create a *Regular Role*, *Site Role*, or *Organizational Role*. A *Regular Role* assigns its permissions to its members. A *Site* or *Organizational Role* assigns its permissions to a site or organization to which you can assign users.

Click the *Action* button to the right of a role to *Edit*, view or alter *Permissions*, *Assign Members* (this last works to see and assign users). You can also assign role members in the Portal > Users and Organizations user editor.

### NOTE:

Owner Roles do not have an *Action* button. Owner implies something you have added or created and so actions do not apply.

Notice also that when you *Assign Members*, a screen appears with tabs where you can assign *Users*, *Sites*, *Organizations* and *User Roles*. Typical best practice is to assign users to one of these collective designations, then assign the collection to a role.

Notice also that you can view both *Current* and *Available* members with those sub-tabs. You can even *Search* for members.

Click *Back* (in the upper right corner) or the *View All* tab to return to the screen listing roles and their *Action* buttons.

## Portal > Portal Settings

The *Settings* screens are where users who are administrators can configure the most basic things about Dell OpenManage Network Manager. These include the following:

- Mail hosts
- Email notifications, who sends them, what the contents are for account creation notices, or password change / reset notices.
- Identification, including address, phone, email and web sites.
- Display settings
- Google Apps login / password.



### CAUTION:

Checking *Allow Strangers to create accounts* may produce a defective login screen.

## Portal > [Other]

Some of the remaining portal labels permit the following:

**Sites**—Configure sites. Sites are a set of pages that display content and provide access to specific applications. Sites can have members, which are given exclusive access to specific pages or content.

**Site Template**—Configures pages and web content for organizations.

**Page Template**—Configures a page and portlets, as well as permissions.

**Password Policy**—Configure the security policies you want, including user lockout and password expiration, and assign them to users.

**Custom Fields**—Lets you configure custom fields for Blog entries, Bookmarks or Bookmark Folders, Calendar Events, and so on.

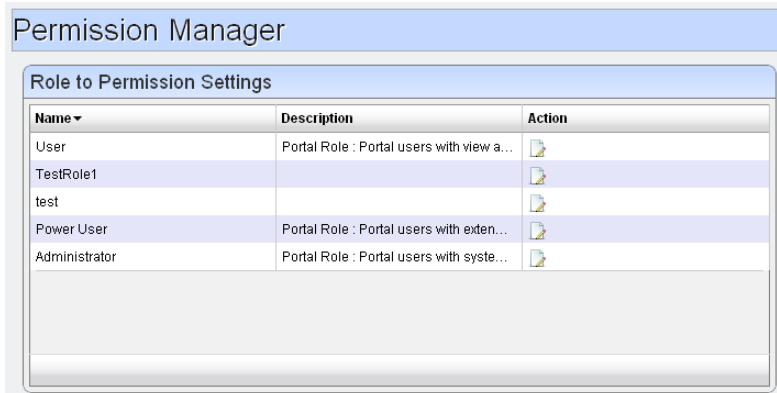
**Monitoring**—Lets you see all the live sessions on the portal. Click a session to see its details. This is usually turned off in production for performance reasons.

**Plugins Configuration**—Configure role access to portlets and features. By default, only administrators can add portlets / plugins to their pages.






## Redcell > Permission Manager

Manage Permissions to manage user access to different features. These are configured as part of Roles, which aggregate users regardless of community affiliation. Create Roles with Portal > Roles.

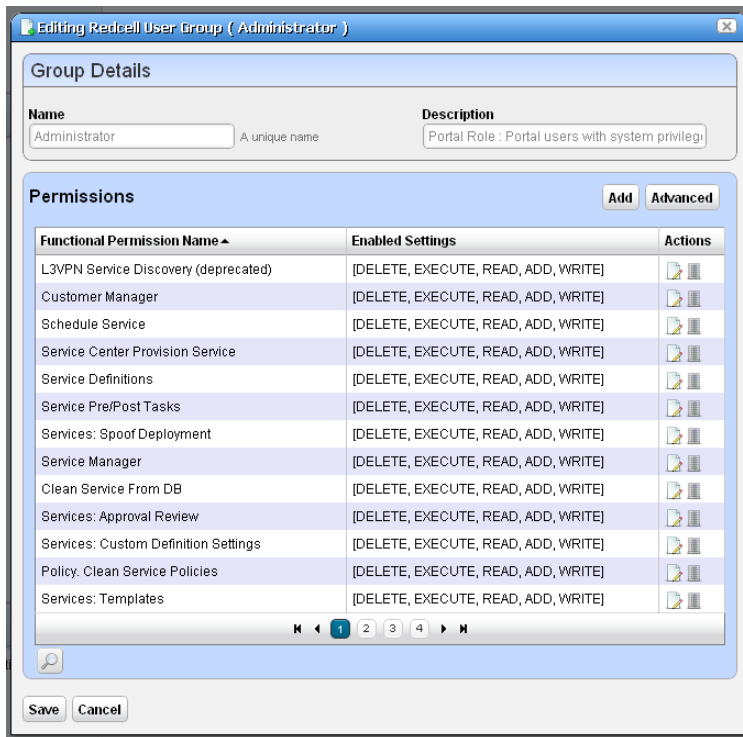
The *Users* editor screen accessible from the *Action* menu for users listed in Portal > Users and Organizations lets you manage groups to which Users are assigned.



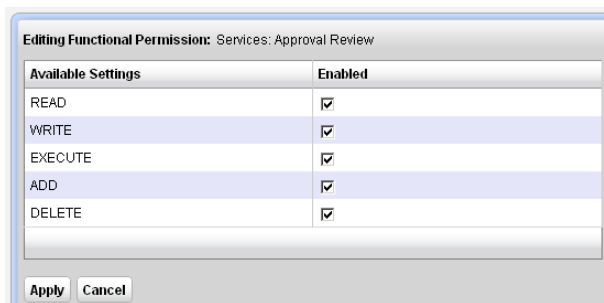
The screenshot shows a web interface titled "Permission Manager". Below the title is a sub-header "Role to Permission Settings". The main content is a table with three columns: "Name", "Description", and "Action". The table lists several roles, including "User", "TestRole1", "test", "Power User", and "Administrator". Each row has a small icon in the "Action" column.

Name	Description	Action
User	Portal Role : Portal users with view a...	
TestRole1		
test		
Power User	Portal Role : Portal users with exten...	
Administrator	Portal Role : Portal users with syste...	

Click the *Edit* button (the pencil and paper) to the right of a listed group to see and configure its permissions.



Edit permissions with the *Edit* button to the right of the listed permission.

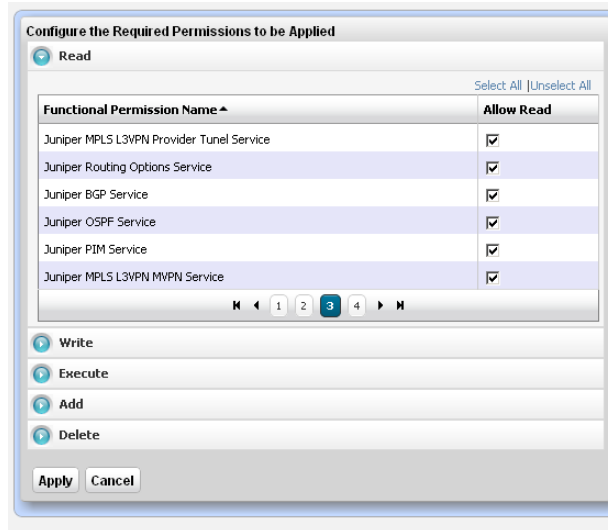


The following describes the actions of the permissions, when checked:

Action	Default Behavior
read	Enables <i>Details</i> , <i>Visualize</i> and <i>View as PDF</i>

Action	Default Behavior
write	Enables the <i>Edit</i> , <i>Save</i> , and <i>Import / Export</i> .
execute	Lets you see the view altogether, launch from a portlet and query for elements. Alternatively this action can control a specific application function, (typically described by the permission name) like provisioning a policy.
add	Enables the <i>New</i> menu item, and <i>Save</i> . If you do not check this action, then the <i>New</i> menu item does not appear.
delete	Enables the <i>Delete</i> menu item.

The *Add* button on the *Permissions* panel lets you add permissions previously deleted, if they are available, and the *Advanced* button lets you configure permissions by type. For example, if you want to see all of the *READ* permissions.

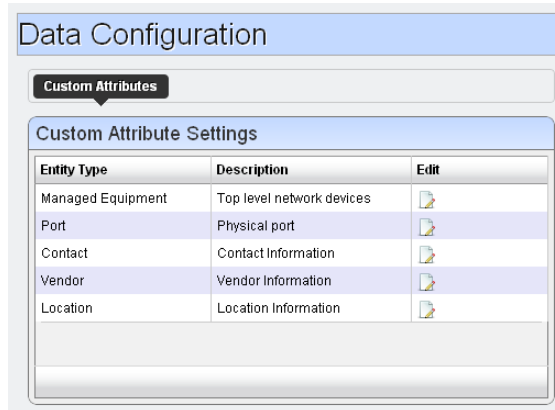


### Tip

When you hover the cursor over a functional permission, tooltips provide a description. You can also click on the *Search* button at the bottom to find a phrase within the functional permissions.

## Redcell > Data Configuration

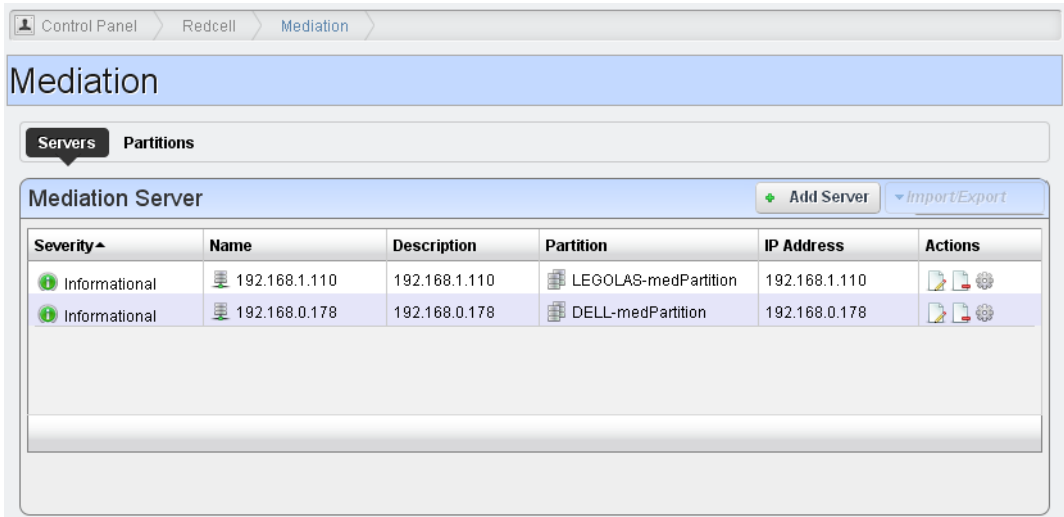
This panel configures custom attributes for Dell OpenManage Network Manager. Click the *Edit* button next to the *Entity Type* (Managed Equipment, Port, Contact, Vendor, or Location) for which you want to create custom attributes.



This opens an editor listing the available custom attributes for the entity type. Edit Custom Attributes on page 89 describes right-clicking to access this directly from the portlet menu, and the details of how to edit custom attributes.

## Redcell > Mediation

This panel monitors mediation servers in your system, appearing only when such servers exist. Mediation servers appear listed in the *Servers* tab of this manager if mediation servers are connected to application server(s).



Severity	Name	Description	Partition	IP Address	Actions
Informational	192.168.1.110	192.168.1.110	LEGOLAS-medPartition	192.168.1.110	
Informational	192.168.0.178	192.168.0.178	DELL-medPartition	192.168.0.178	

Mediation server, routing entries and partition entries appear automatically when mediation server connects for the first time. You can test connectivity from appserver cluster and medserver/partition.

You can export or import both server and partition configurations. Use the button on the right above the listed servers or partitions to do this. Importing Partitions/MedServers overwrites those in the database with the same names. Exporting a partition exports contained medservers too. Importing a partition looks for overlapping routing entries and saves the partition with only its unique entries. If no entries are unique, the partition is not saved.

### NOTE:

This panel does not appear if you install Dell OpenManage Network Manager in stand-alone mode, without a separate mediation server. To make it appear, add `medserver.support=true` to the `portal-ext.properties`. Remember, best practice is to override properties as described in [Overriding Properties on page 23](#).

In addition to automatically detecting mediation servers, you can click *Add Server* to configure additional mediation servers.

The screenshot shows a web-based configuration interface for a Mediation Server. At the top, there are two tabs: 'Servers' (selected) and 'Partitions'. The main area is divided into two sections. The first section, titled 'Mediation Server', contains three input fields: 'Name' with the value 'TestServer', 'Description' (empty), and 'IP Address' with the value '192.168.1.27'. The second section, titled 'Choose Mediation Partition', has two buttons: 'Create Partition' (with a plus icon) and 'Existing Partition' (with a minus icon). Below these buttons are four input fields: 'Name' with 'TestPartition', 'Description' (empty), 'Routable Domain' with 'Default', and 'Routing Entries' with '192.168.1.27/24'. At the bottom of the interface are three buttons: 'Apply' (with a checkmark icon), 'Test' (with a gear icon), and 'Cancel' (with a red X icon).

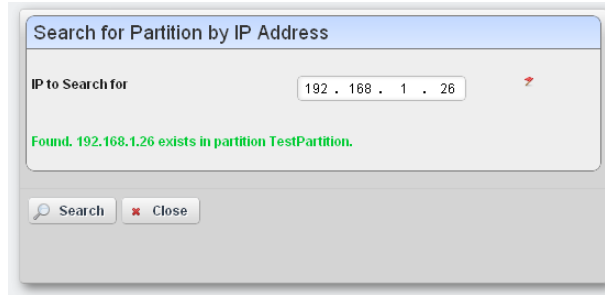
When creating a new server, enter a *Name*, *Description* and *IP Address*. You can also *Add Partitions* (or select from *Existing Partitions*), choosing a *Name*, *Description*, *Routable Domain*, and *Routing Entries* (click the '+' to add your entries to the list).

The *Test* button scanning the ports in the proposed application server / mediation server link, validating the installed versions of Dell OpenManage Network Manager in both locations are the same, and validating the connection between application server and mediation server. A job screen like those described in *Audit Trail / Jobs Screen on page 91* appears to track the progress of testing.

The *Partitions* tab of the Mediation monitor displays already-configured partitions, and lets you edit them with an *Edit this entry* icon. The editor screen is like the one that adds new partitions. Test listed partitions with the gear icon to the right of the partition, or delete it with the *Delete this entry* icon.

## Search for Mediation Server

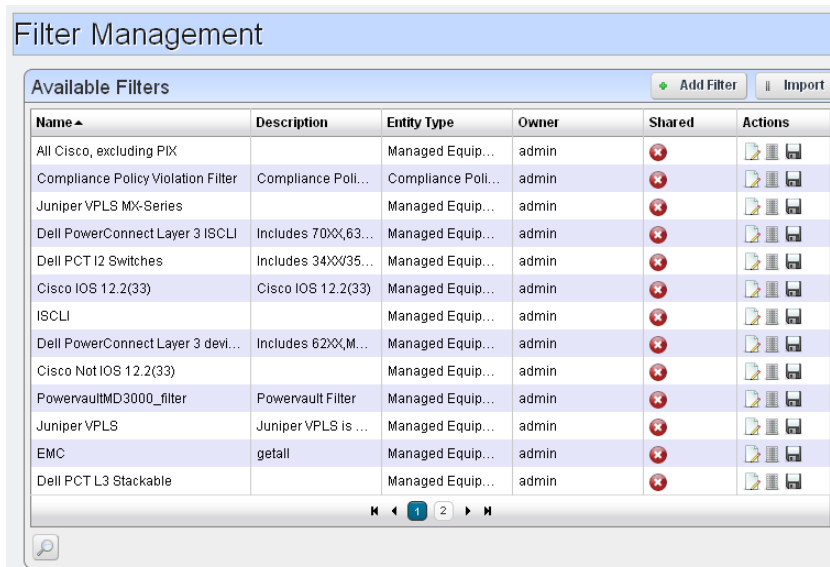
The *Search* button in the *Partitions* tab of the Mediation monitor opens a screen where you can enter an address in *IP to Search for*.



Clicking *Search* locates the mediation partition that services the entered IP address (although it does not determine whether that partition is up and running).

## Redcell > Filter Management

This screen, accessible from *Go to > Control Panel* lets you manage the filters in OpenManage Network Manager.

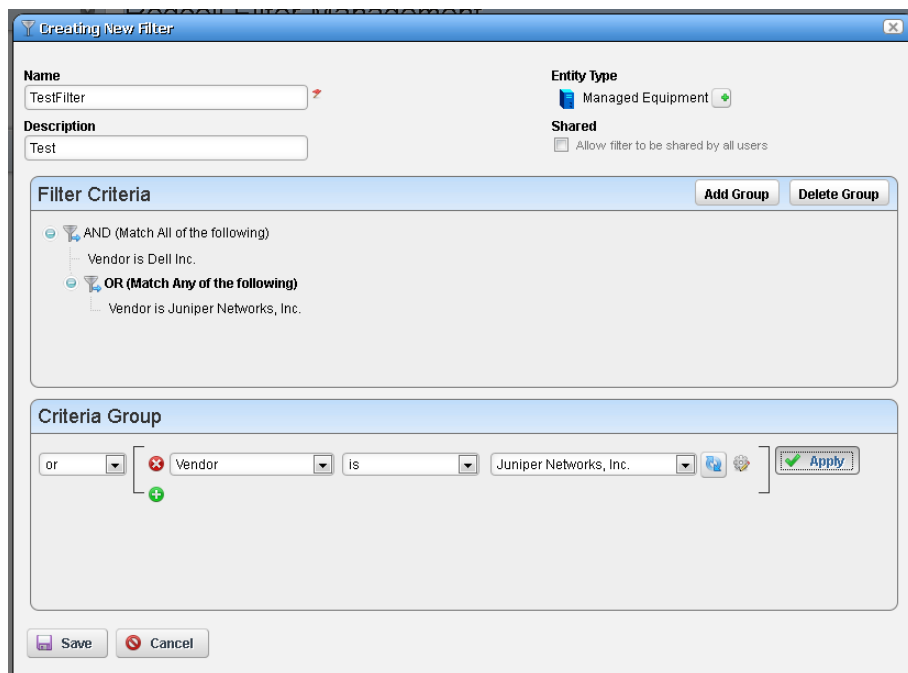




Click the *Delete* icon to the right of a listed filter to remove it from the system. Click the disk icon to export the filter. Clicking the *Import* button at the top of the screen lets you import previously exported filters.

## Tip

To find a particular filter, click the *Search* (magnifying glass) icon in the lower left corner of this screen. Clicking the *Edit* icon to the right of a listed filter, or clicking the *Add Filter* button opens the filter editor.



Use this editor to configure filters. Enter a *Name* and *Description*, and use the green plus (+) to select an entity type. If you check *Shared* to make the filter available to all users. You can add groups of filter criteria (click *Add Group*) that logical AND or OR with each other. Configure the filter in the *Criteria Group* panel as described in the How to: Filter Expanded Portlet Displays on page 85. Delete filters with the *Delete this entry* icon next to the edit icon.

## Server

This portion of the *Control Panel* lets you manage the portal's web server. Tooltips describing these screens appear when you hover the cursor over fields, or click the blue circle surrounding a question mark in the title bar. Here are some of its functions:

**Server > Server Administration**—Monitor resources and administer settings like logging, caching, search indexes, file upload maximums, e-mail settings, and so on. See Search Indexes on page 34 for a description of a particularly important function.

 **Tip**

This panel is visible to administrators only, and contains helpful settings and resource information related to the server.

**Server > Portal Instance**—Lets you configure more than one portal instance on your server.

**Server > Plugins Installation**—Configure portlet theme and layout plugins here. This panel lets you add portlets besides those available from Dell OpenManage Network Manager. You can install free portlets for Google, Youtube, Collab and more. For Dell OpenManage Network Manager, we include Wikis, Journals, Blogs so, in addition to the collaborative features within Dell OpenManage Network Manager itself (as in Sharing on page 87, and Status Bar Alerts on page 75). This means you can collect the knowledge and advice of those managing your network as it expands or changes. To experiment with this screen’s capabilities, click the *Install More Portlets* button near the top and explore the subsequent screens.

**Server > Updates Manager**—Plug-in versioning, uninstalling, and updating.

 **NOTE:**

As long as portlets adhere to open source portlet specifications, you can install them.

## Redcell > Database Aging Policies (DAP)

Database Aging Policies prevent the Dell OpenManage Network Manager database from filling up by filling up by deleting old records. You can also save designated contents to an archive file on a specified cycle. Database Aging Policies configure which contents to archive, the archive location, and the configuration of that archive file.

To view and manage such policies, right click an item with them (for example, an alarm), or click *Manage > Control Panel*, and under Redcell click *Database Aging Policies*.

Enabled	Policy Name	Details	Schedule Interval	Actions
<input checked="" type="checkbox"/>	DataCollection_DAP	Default Printer Data Collecti	Daily (Recommended)	[Edit] [Delete] [Execute]
<input checked="" type="checkbox"/>	Inventory Change Tracking C	Default DAP for Change Trac	Daily (Recommended)	[Edit] [Delete] [Execute]
<input checked="" type="checkbox"/>	EventHistoryDAP	Default Event History Recorc	Daily (Recommended)	[Edit] [Delete] [Execute]
<input checked="" type="checkbox"/>	AuditDAP	Default audit trail DAP	Daily (Recommended)	[Edit] [Delete] [Execute]
<input checked="" type="checkbox"/>	JobDAP	Default job status record DA	Daily (Recommended)	[Edit] [Delete] [Execute]
<input checked="" type="checkbox"/>	AlarmsDAP	Default Alarm Records DAP	Daily (Recommended)	[Edit] [Delete] [Execute]
<input checked="" type="checkbox"/>	Discovery Definition Data D	Default DAP for archiving sta	Daily (Recommended)	[Edit] [Delete] [Execute]
<input checked="" type="checkbox"/>	RTCPSessionsDAP	Default RTCP Session Recc	Daily (Recommended)	[Edit] [Delete] [Execute]
<input checked="" type="checkbox"/>	InventoryReportDAP	Default Inventory Report DAF	Daily (Recommended)	[Edit] [Delete] [Execute]
<input checked="" type="checkbox"/>	Adaptive CLI DAP	Default Adaptive CLI Record	Daily (Recommended)	[Edit] [Delete] [Execute]
<input checked="" type="checkbox"/>	ConfigFileDAP	Default Configuration File D	Daily (Recommended)	[Edit] [Delete] [Execute]
<input checked="" type="checkbox"/>	ConfigChangeRecordDAP	Default DAP for archiving cor	Daily (Recommended)	[Edit] [Delete] [Execute]
<input checked="" type="checkbox"/>	Transparent Bridging Entry L	Default DAP for archiving sta	Daily (Recommended)	[Edit] [Delete] [Execute]

Policies appear in the *Aging Policies* tab of this screen, with columns that indicate whether the policy is *Enabled*, the *Policy Name*, *Details* (description), *Scheduled Intervals* and icons triggering three *Actions* (*Edit*, *Delete* and *Execute*). Notice that the bottom right corner of this page also lets you *Enable / Disable / Execute All* policies listed.



## How To:

### DAP Workflow

The following are steps typical for implementing DAP:

- 1 From the screen listing Database Aging Policies (DAP), click *Add Policy*, and select a policy from the displayed list of alternatives.
- 2 This opens Aging Policies Editor.
- 3 In the *Aging Policies > General* tab, specify the name, schedule interval, whether this policy is *Enabled*, and so on.
- 4 Specify the *Archive Location*. Those listed are the *Repositories* listed on the *Repositories* tab. You can manage those on that tab.

- 5 In the Aging Policies Options tab, specify either the archiving and retention you want, or further specify Sub-Policies that refine the items archived, and specify archiving and retention for those sub-policy elements. Which one you can specify depends on the type of DAP you are configuring.
- 6 Click *Apply* until the displayed screen is the DAP manager.

## Aging Policies Editor

When you click *Add Policy* in the upper right corner of the Redcell > Database Aging Policies (DAP) screen, first a selector appears where you can click on the kind of policy you want to create, then the editor appears. If you click the *Edit* icon to the right of a listed policy, the Aging Policies Editor appears with that policy's information already filled out, ready to modify.

The *General* screen has the following fields:

**Name**—An identifier for the policy

**Description**—A text description of the policy

**Enabled**—Check to enable the policy.

**Schedule Interval**—Use the pick list to select an interval. Once you have configured an interval here, you can re-configure it in the Schedules Portlet.

**Base Archive Name**—The prefix for the archived file.

**Compress Archive**—Check to compress the archive file.

**Archive Location**—Select from the available Repositories in the pick list.

The contents of the *Options* tab depend on the type of DAP you are configuring. Typically, this tab is where you set the retention thresholds.

## DAP SubPolicies

Some Options tabs include sub-policies for individual attribute retention.



Click *Add SubPolicy* or click the *Edit* button to the right of listed policies to access the editor.

## Editing Tips

Archiving options that appear in the Aging Policies Editor vary, based on type of policy selected. Inventory Change Tracking DAPs ask how long you would like to keep Config reports, Inventory Report DAPs ask how long you would like to keep your Historical Reports based on number of instances, days, and weeks, months or years.

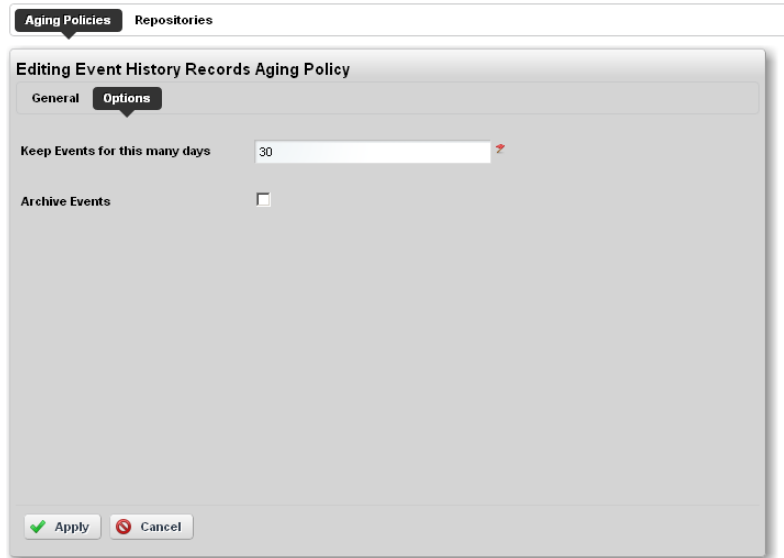
Set these thresholds in the *Options* tab. All DAPs require a Name and a record threshold. Check the *Enabled* checkbox to enable the policy.

DAPs run on a schedule. If the record threshold number is greater than or equal to the configured threshold then the DAP runs at the scheduled time. You may also manually click the gear icon to the right of a listed policy, and execute a DAP at any time to check that threshold figure. In either case, if the threshold is not crossed Dell OpenManage Network Manager creates no archives.

To verify when current DAPs are scheduled to run, open the Schedules portlet, and select the schedule on which it runs. For most DAPs, this is the Daily (recommended) DAP. Right-click to edit it. The Scheduled Aging Policies list should include all DAPs that have selected that schedule.

## Aging Policies Options

The *Options* tab in this editor can vary, depending on the type of policy.



The screenshot shows a dialog box titled "Editing Event History Records Aging Policy". At the top, there are two tabs: "Aging Policies" (selected) and "Repositories". Below the tabs, there are two sub-tabs: "General" and "Options" (selected). The "Options" tab contains two settings: "Keep Events for this many days" with a text input field containing the number "30" and a red error icon to its right; and "Archive Events" with an unchecked checkbox. At the bottom of the dialog, there are two buttons: "Apply" (with a green checkmark icon) and "Cancel" (with a red X icon).

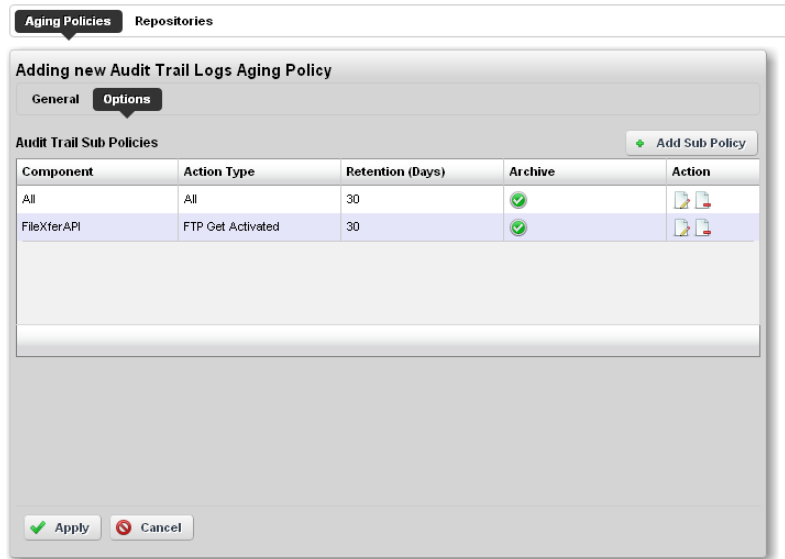
Typical fields can include the following:

**Keep [Aged Item] for this many days**—The number of days to keep the aged item before archiving it.

**Archive [Aged Item]**—Check this to activated archiving according to this policy.

# Sub-Policies

Some types of Database Aging Policies can have sub-policies that further refine the aging for their type of contents.



These appear listed in the Aging Policies Options tab. Click *Add Sub Policy* to create them. Notice that you can *Edit* or *Delete* listed policies with the icons in the far-right *Action* column in this list.

The screenshot shows a dialog box titled "Editing Audit Trail Sub Policy". At the top, there are two tabs: "Aging Policies" (selected) and "Repositories". The dialog contains the following fields:

- Component:** A dropdown menu with "FileXferAPI" selected. Below it is the text "Filter by Component".
- Action Type:** A dropdown menu with "FTP Get Activated" selected. Below it is the text "Select Action Type to apply sub policy to".
- Retention (Days):** A text input field containing the number "30". Below it is the text "Enter number of days." and a red arrow icon.
- Archive:** A checked checkbox. Below it is the text "Check to activate archiving of data removed from the database".

At the bottom of the dialog are two buttons: "Apply" (with a green checkmark icon) and "Cancel" (with a red 'X' icon).

Such sub-policies contain the following types of fields:

**Component**—Select the component for the sub-policy from the pick list.

**Action Type**—This further sub-classifies the *Component*.

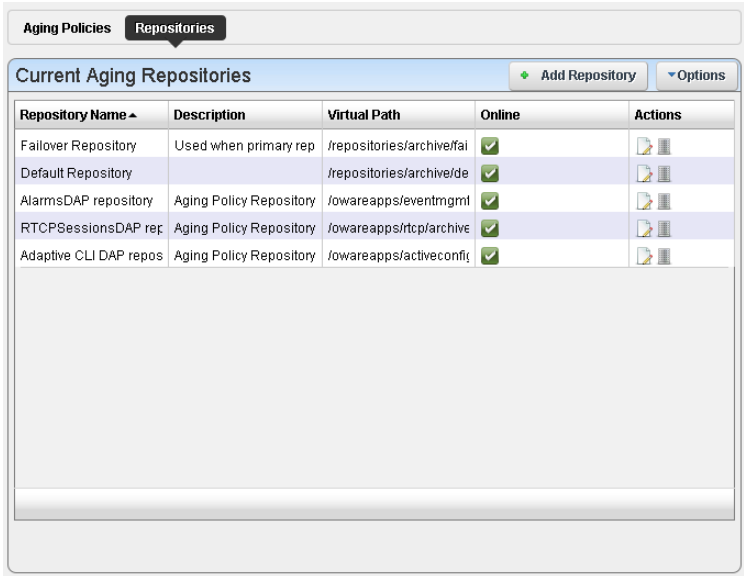
**Retention (Days)**—The number of days to keep the aged item before archiving it.











**Archive**—Check this to activated archiving according to this policy.



# Repositories

When you select a repository in the Aging Policies Editor, the available policies come from what is configured in this tab of the editor.



Repository Name ▲	Description	Virtual Path	Online	Actions
Failover Repository	Used when primary rep	/repositories/archive/fai	✓	 
Default Repository		/repositories/archive/de	✓	 
AlarmsDAP repository	Aging Policy Repository	/owareapps/eventmgml	✓	 
RTCPSessionsDAP rep	Aging Policy Repository	/owareapps/rtcp/archive	✓	 
Adaptive CLI DAP repos	Aging Policy Repository	/owareapps/activeconfi	✓	 

Available repositories appear listed in the initial screen. Like the Aging Policies Editor, you can click *Add Repository* to create a new repository, and *Edit* or *Delete* selected, listed policies with the icons in the *Action* column. Notice the listed policies indicated whether the archiving destination is *Online* with a green icon (this is red, when the destination is offline).

The screenshot shows a dialog box titled "Adding new Aging Repository". It has two tabs: "Aging Policies" and "Repositories". The "Repositories" tab is active. The dialog contains the following fields and controls:

- Repository Name:** A text input field containing "TestRepository". Below it is the placeholder text "Enter a repository name".
- Description:** A text input field containing "Test". Below it is the placeholder text "Optional description".
- Virtual Path:** A text input field containing "Amg/repository". Below it is the placeholder text "Enter path for repository".
- Online:** A checkbox that is checked. Below it is the text "Check to mark repository in online state".

At the bottom of the dialog are two buttons: "Apply" (with a green checkmark icon) and "Cancel" (with a red X icon).

When you *Add Repository* or *Edit* an existing one, the following fields appear in the editor:

**Repository Name**—An identifier for the archiving destination.

**Description**—A text comment.

**Virtual Path**—This is the path relative to the installation root directory. Any user with administrator permissions can specify or change the default archive path here.

**Online**—Check this to put this repository online.

Dell OpenManage Network Manager automatically writes to any configured failover repository if the primary repository is full or not writable.

### **Tip**

To view any archived DAP file, use `dapviewer`. Type `oware` in a command shell, then, after pressing [Enter], type `dapviewer` to use this utility.

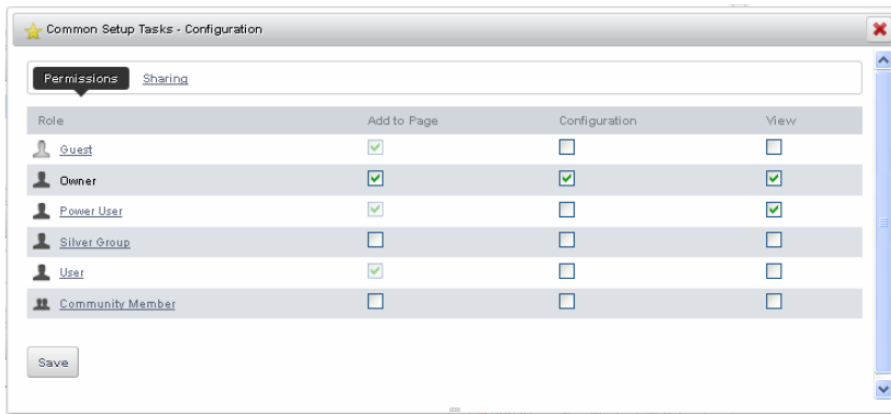
## Portlet Level Permissions

You can also provide permission for a user/group/role/organization on a defined portlet.



## How To: Configure Portlet Permissions

- 1 As an admin user, click on the Configuration icon (the wrench) in the top right corner of the portlet of interest.
- 2 Click on the *Configuration* and go to the Permissions tab in the next screen.
- 3 Uncheck the View permission for Guest and Community members. Make sure Owner and PowerUser still have View permissions.



- 4 Now check View for the relevant roles (for example, *Silver Group*).
- 5 Click *Save*.
- 6 You should now be able to log out as admin, and log in as Guest or other community members and confirm you cannot view the portlet you just configured.



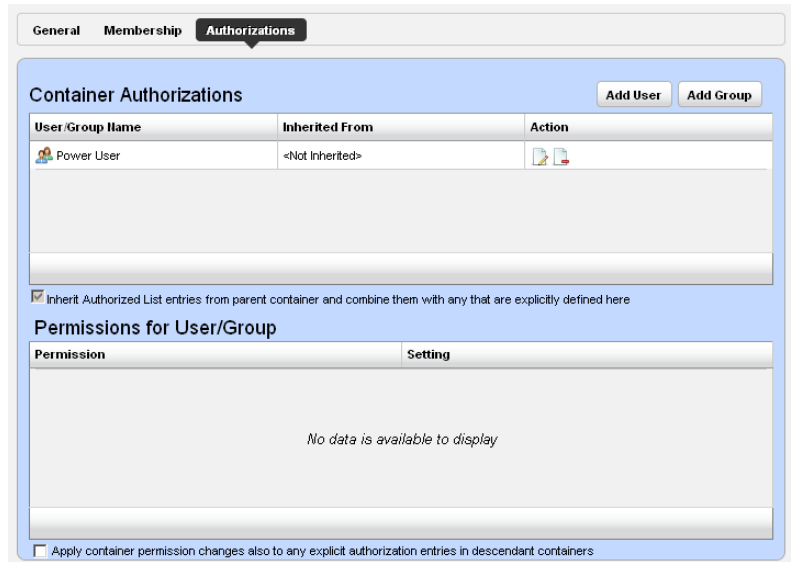
## How To: Configure Resource Level Permissions

You can provide permission for a user/group/role/organization on a defined resource. The following outlines the steps:

- Create a Container for each Customer
- Configure Membership for Container (resources that customer can access)
- Set Authorization for User Container
- Set up a Page for Device Level View

## Create a Container for each Customer

- 1 In Container Manager Portlet, right-click to select *New*.
- 2 Create a container for the desired customer, naming and describing it.
- 3 In the *Authorizations* tab for this container, delete authorization for ALL (non-portal), Add authorization for Synergy Admin, Add authorization for Power User Role, and delete the *Vendors Child Container*.



## Configure Membership for Container

- 4 Create Gold Customer as a Top Level Container.
- 5 Make it Shared, and configure its membership (Select and Add a group of devices)

## Set Authorization for User Container

- 6 In the Authorizations tab, Add Gold Customer (with limited permission), and User Synergy Admin (with full permission).
- 7 Delete Group: User
- 8 Create a Gold Customer user as described above.

## Set up a Page for Device Level View

- 9 Add a Container View to the page of interest with portlets for which you want to restrict access. Currently Container View is enabled for the following portlets: Managed Resources, Alarms, Ports, Audit Trails, Printers.

- 10 Log out as admin, and log back in as a user with Gold Customer permissions.
- 11 Confirm your permission configuration is operating on this page.

## Database Backup

To back up your database, open a command shell (*Start > Run cmd*, in Windows), and then type the following at the prompt replacing USERNAME and owbusdb. By default, the database is owbusdb.

```
mysqldump -a -u USERNAME --password=[name] owbusdb > FILENAME.mysql
```

For example:

```
mysqldump -a -u oware --password=dorado owmetadb > owmetadb.mysql
```

If you have Performance monitors or Traffic Analyzer, you must also back up your stored procedures otherwise they do not get restored when you restore the database. The command line here adds `--routines`. For example:

```
mysqldump -a -u oware --password=dorado --routines owbusdb > owbusdb.mysql
```

This writes the owbusdb to a plain-text file called FILENAME.mysql (owbusdb.mysql in our examples). This file is a full backup with which you can fully restore your database in case of problems.



### NOTE:

Defaults for the database are oware (login) and dorado (password). These are typically different from the login / password for the application.



### Tip

To get a rough estimate of database size, looking at the size of the directory  
`\oware3rd\mysql\data`.

## Restoring Databases

Restoring from FILENAME.mysql is a three step process. This occurs, again, in a command shell:

- 1 Drop the database:

```
mysqladmin -u USERNAME -p drop owbusdb
```

or

```
mysqladmin -u USERNAME --password=[password] drop owbusdb
```

- 2 Recreate the database

```
mysqladmin -u USERNAME -p create owbusdb
```

or

```
mysqladmin -u USERNAME --password=[password] create owbusdb
```

- 3 Import the backup data

```
mysql -u USERNAME -p owbusdb < FILENAME.mysql
or
mysql -u USERNAME --password=[password] owbusdb < FILENAME.mysql
```

## Portal Database Backup / Restore

The web portal itself has a MySQL database. Back it up as follows:

- 1 Open a command shell and type `oware`.
- 2 Then type the following command:  

```
mysqldump -uroot --password=dorado lportal > mybackup.sql
```
- 3 The `mybackup.sql` file is the backup.

To restore the database, use another `oware` shell:

- 1 Drop the database:  

```
mysqladmin -uroot --password=dorado drop lportal
```
- 2 Recreate the database  

```
mysqladmin -uroot --password=dorado create lportal
```
- 3 Import the backup data  

```
mysql -uroot --password=dorado lportal < mybackup.sql
```

# Quick Navigation

The Quick Navigation portlet lets you quickly perform some basic tasks:

**Resource Discovery**—Discover devices in your network with the Quick Discovery defaults, or lets you construct a Quick Discovery profile if none exists. See Resource Discovery on page 152 for details.

**Link Discovery**—After you have discovered resources, this discovers their connections. See Link Discovery on page 176.

**Backup Config Files**—This lets you back up discovered devices' configuration files. Before you can use this feature, you must have servers configured as described in Netrestore File Servers on page 70 and/or File Servers on page 221. See also File Management on page 223.

**OS Image Upload**—Upload firmware updates for devices. See Firmware Image Editor on page 235 for more about these capabilities.

**Deploy OS Image**—This deploys firmware updates. To deploy images, you must have File Servers configured, as described above for Backup. See Deploy Firmware on page 238.

**License Management**—This lets you see and manage the licensed capabilities of Dell OpenManage Network Manager. See License Viewer below for details.



**CAUTION:**

Do not remove this portlet. You cannot re-enable it once it is removed.

Admin user and Power User can see all the above menu items. The User role sees only sees four. Link discovery and OS image upload do not appear by default. To see them, you must give User 'write' permission.

## License Viewer

This screen appears when you click *License Management* in the Quick Navigation portlet.

Product	Edition	Expiration Date	Valid	IP	User	Version
Active Config	COMMON	12-Jul-2012	✓	*	DoradoSoftware	7.0
Aruba restricted actions	ALL	12-Jul-2012	✓	*	DoradoSoftware	7.0
Cisco MDS restricted actions	ALL	12-Jul-2012	✓	*	DoradoSoftware	7.0
Cisco XR-Router Series Drivers	CORE	12-Jul-2012	✓	*	DoradoSoftware	7.0
Change Management	COMMON	12-Jul-2012	✓	*	DoradoSoftware	7.0
ConfigX	COMMON	12-Jul-2012	✓	*	DoradoSoftware	7.0
Brocade restricted actions	ALL	12-Jul-2012	✓	*	DoradoSoftware	7.0

```
Product License for AC
EDITION = COMMON
DESCRIPTION = Active Config
USER = DoradoSoftware
IP = *
EXPIRATION = 11-Jul-2012
EXPIRATION DATE = 12-Jul-2012
VERSION = 7.0
KEY = AMW-43198010-17280-E -- IS VALID
APPPROPS:
  APPTYPE-ACMonitor=true:
  PERMISSION-AC: AdaptiveCI.T=FFFF:
```

Click *Close* to return to Dell OpenManage Network Manager. You may find Licenses in a name slightly different from the one you expect. For example, the *Reports* portlet is licensed as part of the Inventory Manager product.



## How To: Register a License

To register a license click the *Select File* button at the top, and use the subsequent screen to select a license file.



### Tip

To import a license when application server is not running, type `licenseimporter [license file name]` on a command line.

You must restart application server or wait up to 15 minutes before a license modification takes effect.

### Product Licenses

This portion of the License Viewer lists the products for which you have licenses already, displaying the *Product*, *Edition*, *Expire Date*, whether the license is *Valid*, any *IP* restrictions, the *User* who installed the product and/or license, and the *Version* of product for which the license is valid.

### License Details: [Product]

This portion of the screen displays the details of a license selected in the *Registered Product Licenses* portion of the License Viewer screen. It is blank if you have not selected a license in the list above this panel.

### Device Licenses

This tab displays the *Maximum Allowed* number of licenses for devices, the *Count Managed* the *Variance* between maximum and managed, and *Type* of license along with sums of the maximum and count managed.

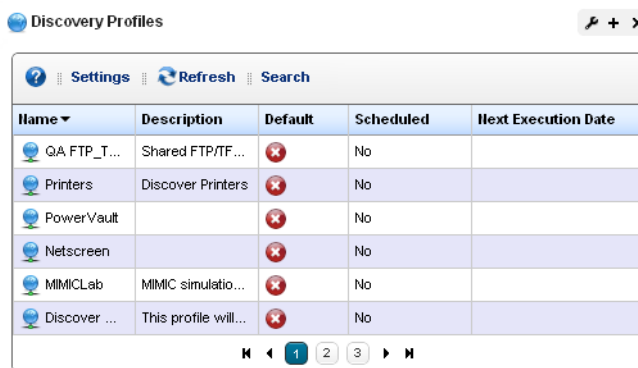


# Discovery Profiles

Discovery profiles configure equipment discovery for Dell OpenManage Network Manager.

The summary view displays the *Name*, *Description*, *Default* (the green check indicates the default profile), whether the profile is *Scheduled* and *Next Execution Date* for scheduled discovery.

The Expanded portlet adds a Reference Tree snap panel that displays a tree of associations between selected profiles and authentication and tasks that they execute. See Discovery Profiles on page 153 for more about this portlet.



Name	Description	Default	Scheduled	Next Execution Date
QA FTP_T...	Shared FTP/TF...	<input checked="" type="checkbox"/>	No	
Printers	Discover Printers	<input checked="" type="checkbox"/>	No	
PowerVault		<input checked="" type="checkbox"/>	No	
Netscreen		<input checked="" type="checkbox"/>	No	
MIMICLab	MIMIC simulatio...	<input checked="" type="checkbox"/>	No	
Discover ...	This profile will...	<input checked="" type="checkbox"/>	No	



## How To:

### Discover Your Network

- 1 Right click the Discovery Profiles list and select *New*.
- 2 The Discovery Profile Editor appears, with a step-by-step set of screens to configure resource discovery. You can navigate through it by clicking the screen tab names at the top, or by clicking the *Next* button at the bottom of the page.

## Discovery Profile Editor

Use this editor to configure discovery once you have started Discover Your Network. Baseline discovery is the initial discovery to compare to later discoveries. Follow these steps to discover equipment on your network:

### General

- 3 **General Parameters**—Set the *Name*, *Description* and whether this profile is the baseline default.
- 4 **Profile Options**—Select the *Device Naming Format* (how the device appears in lists, once discovered), whether to *Manage by IP* address or hostname, and check whether to *Resolve Hostname(s)*, *ICMP Ping Device(s)*, *Manage ICMP-only Device(s)*, or *Manage Unclassified Device(s)*. This last checkbox determines whether Dell OpenManage Network Manager

attempts to manage devices that have no device driver installed. Management may be possible, but more limited than for devices with drivers installed, provided this capability is one you have licensed.

The Filters (by *Location*, *Vendor*, or *Device Type*) let you narrow the list of devices discovered by the selected item(s). As the screen says, this filtering will not have any impact on the processing that occurs during the Inspection step.

## Network

- 5 After you click *Next*, the *Network* screen appears.

**Network Type and Addresses**—Select the type of entry in the pick list (*IP Address(es)*, *CIDR Address*, *Hostname*, *SNMP Broadcast*, *Subnet*).



You can specify an IP Address range by separating the beginning and end with a dash. For example: 192.168.1.1 - 192.168.1.240.

The tooltips in the data entry field describe what valid entries look like.

- 6 **Authentication**—You can *Create new*, or *Choose existing* authentications. (See Discovery Profiles on page 153 for details.) Notice that authentications appear with *Edit / Delete* icons and *Up / Down* arrows on their right. The *Edit* icon opens the authentication editor. Click the arrows to arrange the order in which credentials are tried (top first). Ordering only applies when two credentials are of the same type.

## Actions

- 7 You can configure Actions to run as part of discovery. By default, the actions screen includes the *Resync* action. Use *Add Action* to select others to enter here. You can also edit parameters (if available), delete and re-order the actions listed here by clicking the icons to the right of them. Dell OpenManage Network Manager executes them in top-to-bottom order.

## Inspection

- 8 **Inspect Network using your current settings**—This screen lets you preview the discovery profile's actions and access to devices. If you clicked *Next* rather than *Inspect* at the bottom of the previous screen, click *Start Inspection* to begin the inspection process for selected authentications that validates the device's credentials.

Notice that the *Inspection Status* fields below listed authentications indicates the success or failure of Ping, Hostname resolution, and the listed Authentications.

If the device does not match all required authentications, you can click the *Fix it* icon (a wrench with a red or yellow dot) to edit them for the selected device. You can also click *Test Device*, *Create New*, or *Choose Existing* authentications while in the editor clicking the *Fix it*

icon displays the authentication selection panel. The yellow dot on the *Fix it* icon means an optional authentication is missing. A red dot means a required one is missing.

When authentications are unsuccessful, you can remove or edit them in this editor too. Click the icons to the right of listed authentications to do this.

When they test successfully, the authentications appear in a nested tree under the *Discover* checkbox (checked when they test successfully).

- 9 **Save**—Click *Save* to preserve the profile. You can then right-click it to select *Execute* and begin discovery. If you select *Execute* from the profile editor, Dell OpenManage Network Manager does not save the profile to execute later.

## Results

- 10 **Execute**—Clicking *Execute* begins discovery, confirm you do not mind waiting, and the message traffic between Dell OpenManage Network Manager and the device appears on the *Results* screen.  
This is a standard *Audit* screen. See *Audit Trail / Jobs Screen on page 91* for more about it.
- 11 A message (*Discovery Profile Execute is complete*) appears in the *Messages* at the bottom left of the status bar.



### Tip

You can also schedule discovery profiles to run periodically, updating your Dell OpenManage Network Manager database with any network changes. For more, see *Schedules on page 95*.

- 12 The devices in your network now appear in the *Managed Resources* portlet, and elsewhere (in *Topology*, for example).

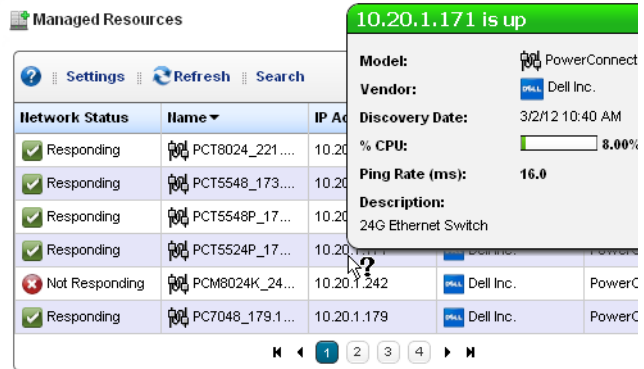
See *Discovery Profiles on page 153* for more about these capabilities.

# Managed Resources

This portlet displays all the devices you have discovered.

See Managed Resources on page 166 for the details of this screen’s capabilities.

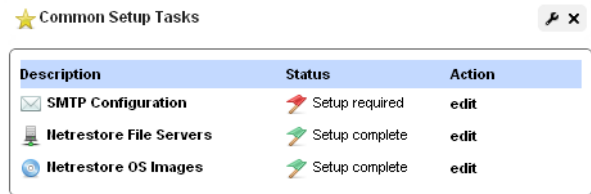
See also Managed Resource Groups on page 162.



# Common Setup Tasks

If you install it (*Add > Applications*), the Common Setup Tasks portlet can appear on the page of your choice. It reminds you of the following common tasks:

- SMTP Configuration
- Netrestore File Servers
- Netrestore Image Repository



A red flag appears with the “Setup required” message in the *Status* column when these are not configured. Configuring them displays a green flag with the “Setup complete” message. Click the *edit* link in the *Action* column to open editors for each of these.

## SMTP Configuration

You can use Dell OpenManage Network Manager's messaging capabilities to communicate with other users, but if you want to receive e-mails automated by actions like configuration file backups, Dell OpenManage Network Manager must have a mail account. This screen configures the e-mail server so Dell OpenManage Network Manager can send such automated e-mails.

The screenshot shows a window titled "SMTP Configuration" with a close button in the top right. The main area is titled "System SMTP Settings" and contains several configuration fields arranged in two columns. The left column includes: "SMTP Server Host" with the value "MySMTP.com", "SMTP Server Port" with "110", "Authentication Enabled" with a checked checkbox, "User Name" with "test", "Password" with a masked field of dots, and "Use SSL" with an unchecked checkbox. The right column includes: "Return Address" with "test@rcsenergy.com", "Default Subject" with "Enter your subject", "Connection Timeout" with "30 milliseconds", "Send Timeout" with "30 milliseconds", and "Max Per Minute" with "30". At the bottom of the window are three buttons: "Apply" (with a green checkmark icon), "Cancel" (with a red X icon), and "Test" (with a globe icon).

The *Apply* button accepts your edits. *Test* tries them. *Cancel* abandons them and returns to Dell OpenManage Network Manager. This screen contains the following fields:

**SMTP Server Host**—The IP address or hostname of your SMTP server.

**SMTP Server Port**—The port for your SMTP server (110 is typical).

**Authentication Enabled**—Check this to enable authentication for this server. Checking enables the next two fields.

**User Name**—The login ID for the SMTP server, if authentication is enabled.

**Password**—The password for the SMTP server, if authentication is enabled.

**Use SSL**—Enable Secure Sockets Layer protocol to interact with your SMTP server.

**Return Address**—The return address for mail sent from Dell OpenManage Network Manager.

**Default Subject**—Text that appears by default in the subject line of mail sent by Dell OpenManage Network Manager.

**Connection / Send Timeout**—The time-outs for mail sent by Dell OpenManage Network Manager.

**Max Per Minute**—The maximum number of e-mails Dell OpenManage Network Manager can send per minute.

**SMTP Server Host**—The IP address or hostname of your SMTP server.

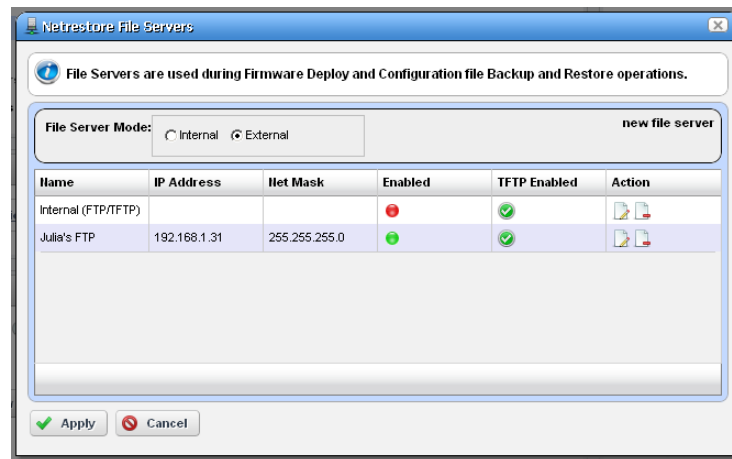
**SMTP Server Port**—The port used by your SMTP server.

Two settings for e-mail servers appear in Control Panel, one in the Control Panel > Portal > Settings Mail Host Names edit screen, and another in Control Panel > Server Administration > Mail. The Portal-based e-mail settings help Administrators limit signups to e-mails only existing in their organization. The screen in that panel provides a list of allowed domain names, if that feature is enabled.

Control Panel > Server Administration > Mail is where to configure the Main server and authentication for routing mail

## Netrestore File Servers

The Netrestore file servers provide FTP connections for retrieving and deploying devices' configuration files, and for deploying firmware updates to devices on your network. See File Servers on page 221 for a description of the portlet that manages file servers. If you want to configure servers from the *Common Setup Tasks* portlet, a slightly different screen appears when you click *Edit*.



This displays configured file servers. Configure new servers by clicking the *new file server* link in the upper right corner. The editing process after that is as described in File Server Editor on page 222.

### ⚠ CAUTION:

If you select the internal file server, make sure no external file server is running on the same host. A port conflict prevents correct operation. Either turn off the external file server, or use it as the FTP server.

Dell OpenManage Network Manager selects the file server protocol for backup, restore or deploy based on the most secure protocol the device supports.

## Portal Conventions

This section explains how to navigate and configure the Dell OpenManage Network Manager web portal. Because this portal is based on open source features, and can be so flexible, this is not a comprehensive catalog of all its features. The following discusses only features significant for using Dell OpenManage Network Manager.

The application's web Portal contains the following common elements:

- The Dock
- Status Bar Alerts
- Menu Bar
- Portlets

Because the elements that manage the Web portal are so flexible, and can be very detailed, only Dell OpenManage Network Manager's most important, or most-frequently-used features appear documented below.



Clicking *Go to* in the Dock and selecting *My Private Pages* to open pages not shared with others, unless you configure sharing. (See *Sharing* on page 87.)

Because they are so fundamental to Dell OpenManage Network Manager's functioning, this section also describes the following portlets:

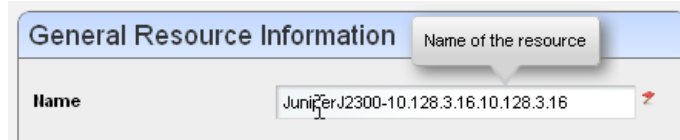
- Audit Trail Portlet
- Schedules



You can rename any portlet by clicking its title. You can also configure portlets' default filters to work in concert with the title. See *Filtering / Settings* on page 112.

## Tooltips

Dell OpenManage Network Manager has extensive tooltips that appear when you click the blue circle with a question mark (one help icon—see also Online Help / Filter on page 12), or when you hover the cursor over a field.



Tooltips also display the content most fields in portlets. If the screen does not allow a full field to appear, you can still find out what is in a field by letting the tooltip re-state what it contains.

## Refresh

You may have to refresh your browser to see screen updates. One way to refresh without re-loading the entire window, however, is to click the *Refresh* button at the top of an individual portlet. (See Settings on page 80)

## The Back Button

Although browsers have a *Back* button, this is not always the best way to return to a previous screen within the portal. For example, clicking *Back* within a breadcrumb trail of links returns to the root of that trail. If it is available, the *Return to previous* button in the upper right corner of a screen provides the most dependable way to return to a previous screen.



## Show Versions

To see which products are installed, and what versions, select the *Manage > Show Versions* menu item.

This can be critical information if you request support for your Dell OpenManage Network Manager installation. The *Application Software Versions* screen appears with the product versions listed in the bottom. Device drivers list supported devices and their operating systems. This can be important for troubleshooting, and is vital information for support.

### NOTE:

Tabs can display more information about supported devices.



## Custom Debug

For more advanced users, any component under `owareapps` can define a `log4j.xml` file for each component matching the following pattern:

```
owareapps\<component-dir>\server\conf\*log4j.xml
```

Consult these files for categories you want to change, and copy those (altered) properties to the file you created in `owareapps\installprops`. The categories altered in this file override any others.

Changing such properties can produce enhanced error output in server logs.

# The Dock

This menu bar appears at the top of portal pages. Its exact appearance depends on your package. With it, you can open online help, add, edit, and navigate to portal pages and content.

Click the down arrow to see menus for items on the dock. Here are its functions

**Help**—Opens the online help.

**Add**—This menu lets you add *Pages*, or *Applications*.



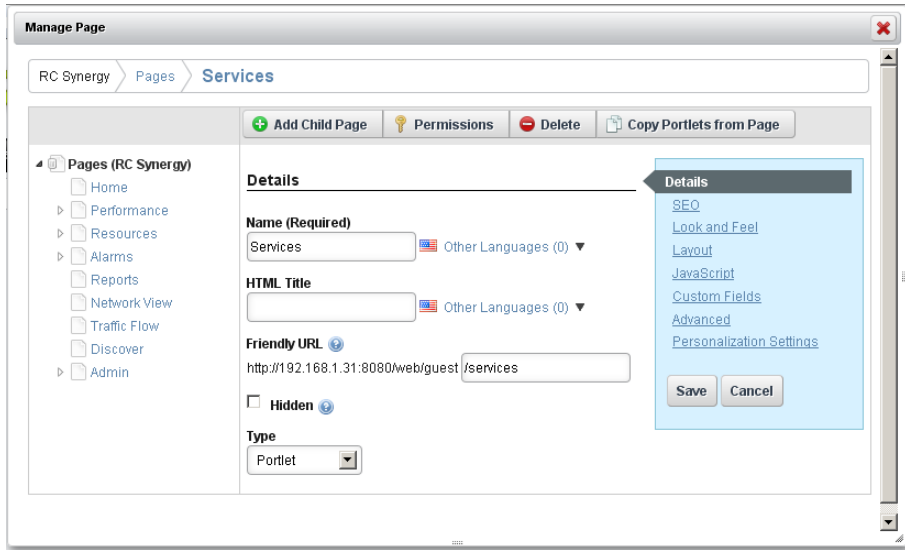
### Tip

The “breadcrumb” trail that appears near the top of pages lets you navigate directly through the hierarchy of parent / child pages directly by clicking links displayed there.

The *More...* menu item contains Dell OpenManage Network Manager’s content. Click a node to see available portlets. See Portlets on page 78.

**Manage**—This menu lets you alter the following:

*Page* (page order [note that you can drag-and-drop pages within the *Pages* tab] permissions, appearance and so on). You can create Children pages, and can Import / Export page configurations as described below.



Use the screen that appears after selecting *Manage > Page* to configure add or delete pages and to manage their appearance and permissions. You must refresh any altered page before edits take effect.

**Tip**

You can create a new page, then *Copy Portlets from Page* you can duplicate another page's portlets on the selected page.

*Page Layout*—Configure the page's columns. This menu item does not appear if you have an expanded portlet open, because the focus is not in the context of a page.

**Tip**

The *Freeform* page layout may stack portlets on top of one another. Toggle the *Fullscreen* icon in the upper right corner to see portlets so you can re-arrange them.

*Site Settings*—Configures page behavior, look and feel. See also Import / Export on page 86.

*Show Versions*—See Show Versions on page 72.

**Go To**—Makes the selected screen type appear. Select *My Public Pages* or *My Private Pages*, for example. When you add a new Community, its configured pages appear in this menu too. This also provides access to *Control Panel* (see Control Panel on page 34).



**CAUTION:**

Dell OpenManage Network Manager does not support multiple tab browsing as a reliable way to see its screens. Pages overcome that limitation.

Administrators can permanently configure *Public* pages, while users with fewer rights can only configure their *Private* pages. Any page changes persist after you make them, provided you have the rights to make changes on a page. See Public / Private Page Behavior on page 40 for the details.

**[User Name] (sign out)**—Opens the *Manage My Account* screen, where you can configure your name, job title, image, e-mail and so on. The *Sign out* link lets you log out of Dell OpenManage Network Manager.

**Toggle Full Screen**—The icon on the far right of this bar toggles its appearance / disappearance so you can use more screen area for portlets if you need it. This toggle also impacts the Menu Bar.

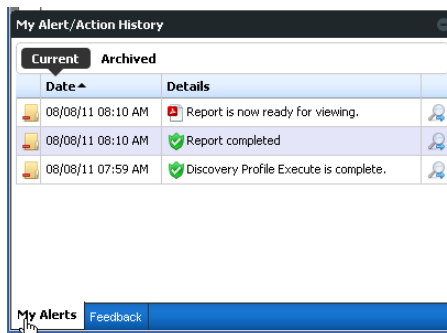
## Status Bar Alerts

The Status bar appears at the bottom of the portal. On the left, it catalogs messages and notifications you have received, including generated reports in *My Alerts*. Click the magnifying glass to the right of reports and Job Status notifications to open a separate viewing window. The panel includes *Current* and *Archived* messages tabs.



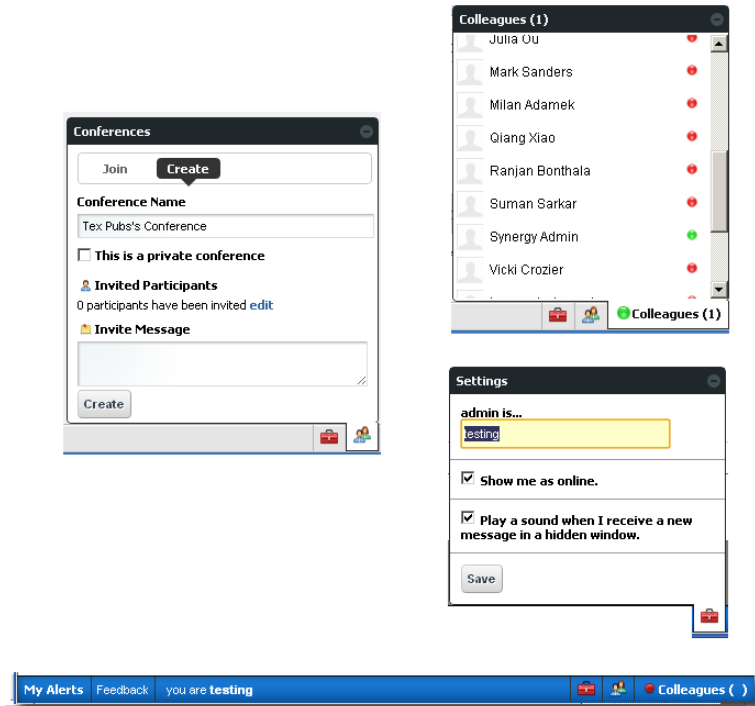
**Tip**

You can see the portal when web server is up, but application server is not. When application server runs after web server has started, and you have already started the portal, an alert appears letting you know it is up.




## Chat / Conferencing

This portion of the message bar lets you send and receive messages to colleagues who are online at the same time you are.




This has the following fields and other possibilities for you to configure:

[Saying]—Configure this text in the menu produced by the *Settings* icon (the next item).

 (**Settings**)—This configures your user settings for any online chat with your colleagues, including the saying, whether your online presence appears, and whether to play a sound when messages arrive.

### Tip

When you have a message from another user, that user's name appears on the status bar to the left of this icon.

 (**Conferences**)—This configures your user settings for any online chat with multiple colleagues. The *Create* tab lets you *edit* to invite colleagues, configure an invitation message and check to make a private conference that only invites can attend. The *Join* tab becomes active when you are invited to a conference. An online chat window appears after you join.

**Colleagues (n)**— A green dot indicates others are online (it is red when you are alone), and *n* is the number of colleagues online. Click to open the chat screen. Click on a colleague and enter text at the bottom of the popup that appears to send messages. Previous chat history also appears above any current text on that chat popup.

Click the minus icon in the top right corner of these screens to close them.

## Menu Bar

The Menu Bar appears on the left side of the screen. It consists of Menu items that lead to separate pages configured with *Manage > Page*.

The pages that appear on this bar can vary, depending on which Dell OpenManage Network Manager package you have installed. The toggle on the right side of the The Dock makes this menu bar appear or disappear.



### Tip

You can drag and drop the menu bar labels to different positions, and can click a label to rename the page, or delete it (with the “x”).

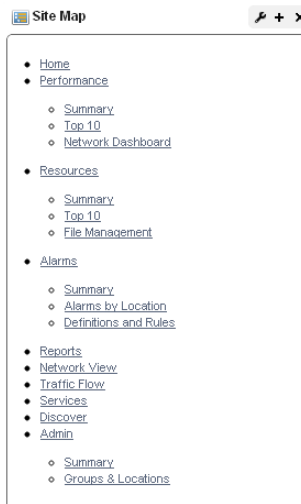
## Site Map

To see where pages and sub-pages are within your installation look at the Site Map portlet.

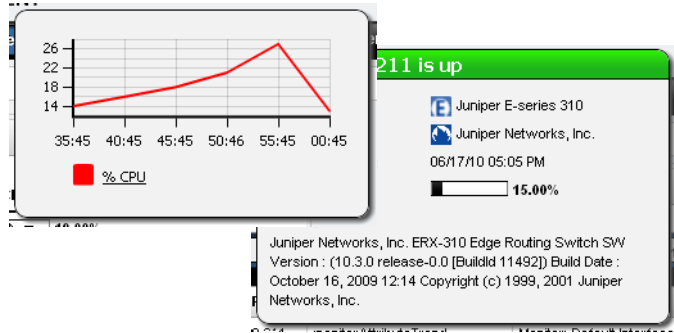
Click the listed link(s) to go to the location(s).

## Graphs

Graphs can appear in alarm and performance portlets. These display the real-time division of total alarms or performance metrics, and you can change their appearance, or associated data lists display. See Alarms on page 99 for more graphs / charts in that portlet.



Hovering the cursor over a listed item in the column where a question mark appears indicates a “tooltip” with more information is available for this item. An informational popup screen appears after a brief wait to query the application server. These popups can include graphs of recent activity too.



Graphs can appear as lines, bars or pie graphs, depending on the portlet, device and activity monitored.

 **NOTE:**

Install the latest Adobe Flash for graph functionality.

## Portlets

Portlets are the elements of any page within the Dell OpenManage Network Manager web client. Initially, they appear in a small, summary screen format. Click *Add > More...* to add a portlet to a page you have created. See Portlet Instances on page 81 below for the distinction between portlets that display the same data, and portlets that can exist in more than one instance, displaying different data.

For a more specific look at available portlets, see the chapters following this one. The following describe common portlet features.

One of the first portlets typical users see is Discovery Profiles.

To act on listed items, right-click. A menu appropriate to the portlet appears.


The title bar for the portlet displays its name. To rename it, click on the name, and the field becomes editable. You can make changes, then click the green checkmark to accept them (or the red “X” to abandon them). The right portion of the title bar

The screenshot shows a portlet titled 'Discovery Profiles' with a title bar containing a question mark, 'Settings', 'Refresh', and 'Search' icons. Below the title bar is a table with the following data:

Name	Description	Default	Scheduled	Next Execution Date
QA FTP_T...	Shared FTP/TF...	<input checked="" type="checkbox"/>	No	
Printers	Discover Printers	<input checked="" type="checkbox"/>	No	
PowerVault		<input checked="" type="checkbox"/>	No	
Netscreen		<input checked="" type="checkbox"/>	No	
MIMICLab	MIMIC simulatio...	<input checked="" type="checkbox"/>	No	
Discover ...	This profile will...	<input checked="" type="checkbox"/>	No	

At the bottom of the table, there is a navigation bar with a home icon, left and right arrows, and numbered buttons for 1, 2, and 3.

contains several editing controls. Clicking on the wrench icon produces a menu that leads to editors for the *Configuration* of this portlet (user permissions to view and configure, Sharing, and so on).

 **Tip**

Some portlets, like Site Map, let you import or export .lar files of their setup and user preferences.

The plus or minus (+ or -) icons *Minimize*, displaying only the title bar, or *Maximize*, displaying an Expanded Portlets, and X removes the portlet from the page.

 **Tip**

To see information about listed items in a portlet, hover your cursor over the row until a question mark appears. A mini-query about the selected item appears in a large tooltip. See Portlet Toolbar below for a description of the buttons at the top of portlets.

 **NOTE:**

Portlet summary screens support displaying up to 200 rows, the expanded portlet supports 1000. Using the portlets' filtering capability makes more sense than trying to see more rows. (See *How to: Filter Expanded Portlet Displays* on page 85.)

### Portlet Toolbar

Buttons on portlet toolbars let you do the following:



?—The Question Mark icon accesses online Help, opening the page appropriate for the portlet.

**Refresh**—Isolates the browser's page refresh to the selected portlet

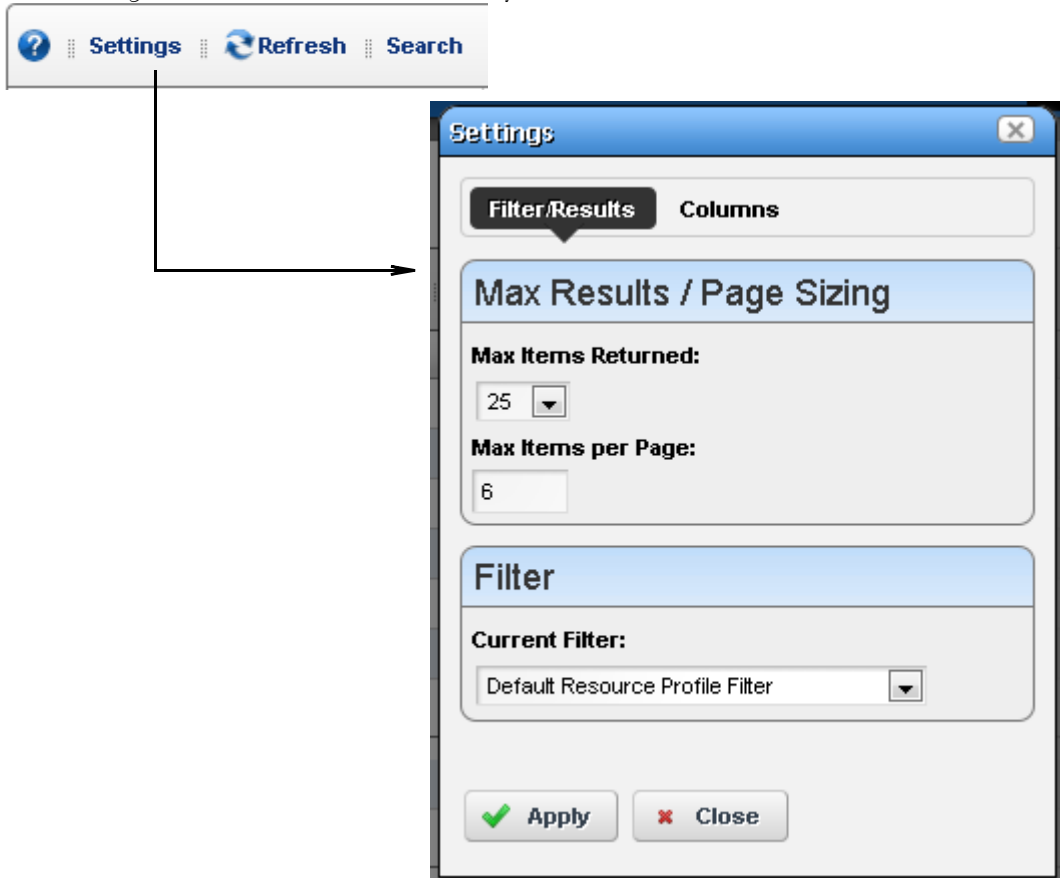
**Settings**—Configures the portlet's filter, size, and so on. In portlets like Alarms, this also can configure whether charts / graphs appear.

**Search**—Locates an item in the portlet. When you click this, the columns filtered in the database appear indented. For example, *Name* and *Model* appear indented in the Managed Resource portal.

Similar functionality is available in Expanded Portlets when you click these buttons in the upper right corner. The *Settings* button also lets you configure the columns displayed and their order. See *How to Show / Hide / Reorder Columns* on page 84.

## Settings

The *Settings* button opens a screen where you can configure the *Max Items* that appear in, and the *Filter* applied to the summary portlet with an *Apply* button to activate any changes you make there. The *Settings* screen also includes a tab where you can Show / Hide / Reorder Columns.



For performance reasons, Max Items are set to relatively low defaults.

*Settings* in expanded portlet does not include the *Filter* item. See *Filter Expanded Portlet Displays on page 85* for information about the alternative.

### Tip

As an Administrator, you can configure a portlet's default display filter, then click the portlet name and rename it. For example, make the default filter in Managed Resources display only Powerconnect, then click Managed Resources in the upper left corner of the portlet to rename it *Powerconnect Routers*.

If you are not an administrator, you must make a personal page for such portlets if you want the filter settings to persist.



## Search

You can search by clicking *Search* at the top of portlets. This opens a search field where you can enter search terms for all the fields that appear in the list at the top of the portlet. The search is for what you enter, no wildcards are supported. To clear a search, clear the field.

This searches all available items in the database, whether they appear listed or not.



### Tip

Sort on a column by clicking on that column's heading. Reverse the sort order by clicking it again. This only sorts what appears in the portlet, whether expanded or not. The application remembers each user's choice saving the last Sort Column and Order on any page. Most portlets also "remember" settings for Max Items and the selected Filter.

## Portlet Instances

When you add content to a page, some portlets (for example, the OpenManage Network Manager Container View portlet) appear with a purple icon and others (for example, the Authentication or Container Manager portlets) have green icons. The green-icon portlets are instanceable and the purple-icon portlets are non-instanceable.



In other words, you can add only one instance of the (purple-icon) Container View portlet to a community; and it displays the same data, even if it appears on more than one screen.



### NOTE:

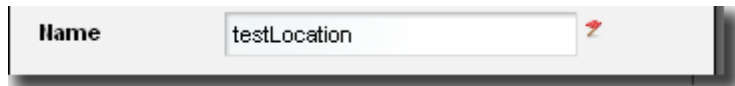
Once you have added a non-instanceable portlet to a page, its entry in the *Add* menu appears grayed out and disabled. You can add more than one non-instanceable portlets to different pages, but they display the same data. Instanceable portlets can appear multiple times on the same page, and can display different data.

The Authentication portlet, for one example, is different. You can add it many times to pages in the community, and can configure each instance of the portlet to display different authentication data.

## Mandatory Fields

Some portlets include editors. These appear after you select an item, right-click, and select either

*New* or *Open*. Mandatory fields in these editors appear with a red flag icon to their right.



## Sorting Portlet Lists

Sorting tables that list items occurs when you click a column heading. The arrow to the right of that heading's text displays the direction of the sort (ascending or descending). When the arrow appears in a heading, the selected column is the basis for sorting.

Location Name ▼
testLocation
neotel
lost in space

## Expanded Portlets

Some portlets appear with a plus (+) icon in their upper-right corner, and can expand to display more information and permit multi-selection of listed items. Return to the smaller portlet by clicking *Return to Previous* in the expanded portlet's upper right corner.



### Tip

If you want to multi-select within listed items in a portlet, you must expand it. The one exception to this rule: the File Management portlet.

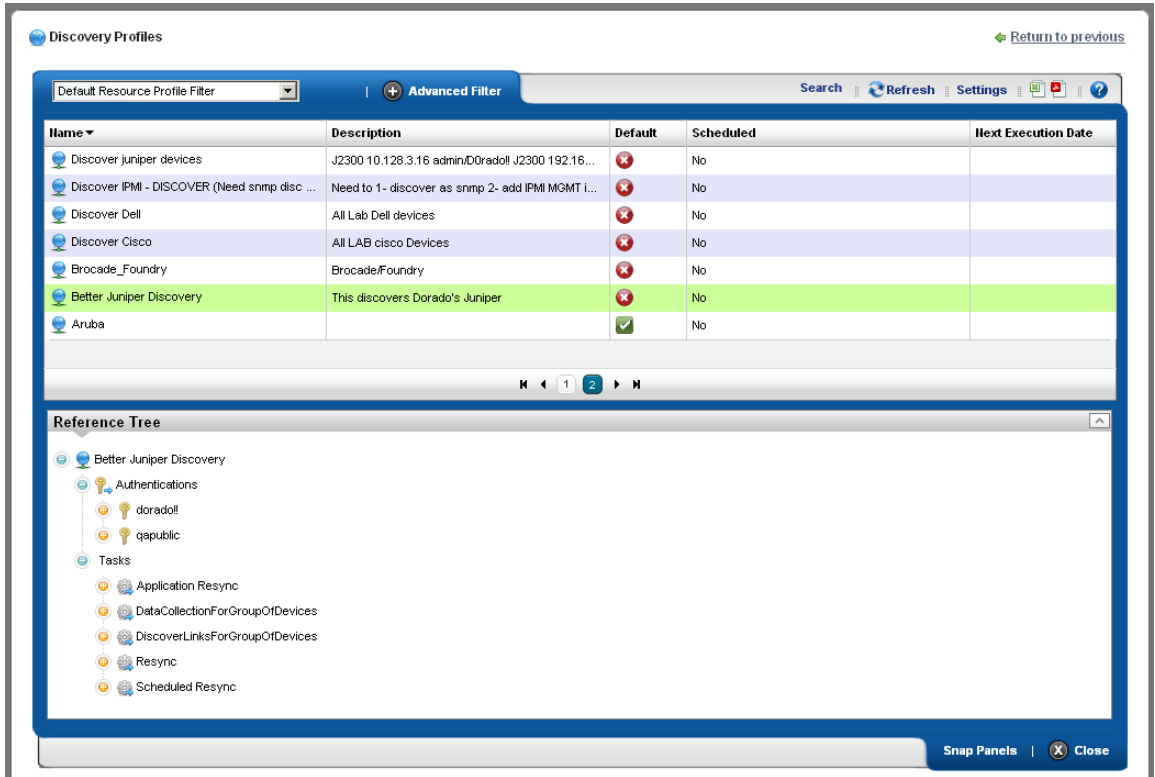
User permissions may limit access to the expanded portlets. For example, OpenManage Network Manager can have many communities and limit users' memberships. Such users can lightly browse other Communities' screens without full privileges.



### NOTE:

Screen size limitations may require you to expand the browser to see expanded screens correctly. You must have at least 1250 pixels in width.

See Control Panel on page 34 for more about setting up user privileges for portlets.

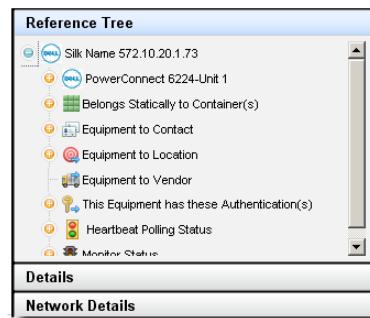


You can right-click to act on listed elements as in the basic, smaller portlet, but here you can also see details about a selected row in the Snap Panels below the table list items in an expanded portlet.

## Snap Panels

The snap panels that appear below the expanded portlet's list can "stack" on top of each other, so several can appear simultaneously in each slot for Snap Panels. Click the title bar of the panel to toggle its expansion or collapse. In the Reference Tree snap panel, click the plus (+) to expand the tree of connections.

You can collapse the entire snap panel area with a *Close* button at the bottom right of expanded portlets. These panels re-appear when you click the *Open* button.





## How To:

### Show / Hide / Reorder Columns

Click the *Settings* button in an expanded portlet, and screen appears with a *Columns* tab where you elect to show or hide columns. Click the appropriate buttons (they change color) to display the columns you want. You can also drag-and-drop the order in which columns appear to re-arrange the display. Click *Apply* to change the columns that appear on screen by default. Abandon any changes and *Close* this screen. The changes appear instantaneously when you return to the expanded portlet.



### Pages

Most portlets use the “recorder” icons to page through a list that occupies more than one screen. The right/left arrows go forward and back one page. The icons at either end go to the beginning or end of the pages.



### Exports

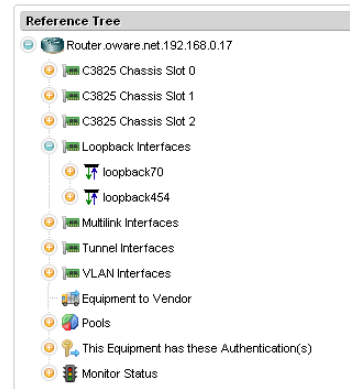
Excel and Acrobat icons appear at the top right corner of the expanded portlet. Click these to export the list contents as either an Excel spreadsheet (.xls), or a pdf file. These download to the default download location you have configured on your browser. Some browsers display the pdf before you can save it.



## Snap Panels (Reference Tree)

These vary, depending on the portlet, but the convention of displaying a *Reference Tree* panel is common. This displays items related to the selected list item in tree form. Click the plus (+) to expand a node on the tree.

Click *Return to previous* in the upper right corner of the expanded portlet to return to the page where you started, with the smaller portlet. If the page you are on has a “breadcrumb trail” of intervening detail pages (for example), you can click an intervening page’s breadcrumb if you do not want to return to the previous screen

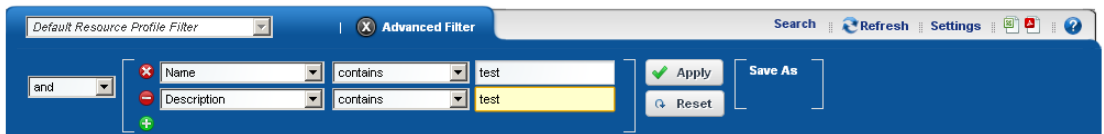


## How To:

### Filter Expanded Portlet Displays

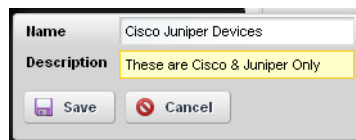
Among other places, filters appear at the top of expanded portlets. Many pre-installed filters come from drivers your installed package. Filters match entity types, but may not necessarily be sensible in the context of a particular portlet.

You can pick from already-configured filters with the drop-down on the left, or you can click *Advanced Filter* to create one of your own.



After you click the green plus (+), select *and* or *or* on the left to combine more than one filter. Click *Apply Filter* to see the list after the filter acts on it. Click *Reset* to return the list to its original state.

Click *Save As* to preserve a filter you have configured for future use. The pick list in the upper left corner of this filter panel is where you would select it.



Create a name and description, then click *Save* on the next screen to preserve your filter configuration. See Redcell > Filter Management on page 48 for the screen that lists all such filters.

 **Tip**

You can also filter what appears on a page with the Container View portlet. Select a container, and the rest of the portlets on that page confine displayed data to reflect the selected container's contents.

 **NOTE:**

When using a filter you must click the refresh icon to the right of the drop down list to populate it.

## Common Menu Items

Several menu items appear in multiple portlets. In addition to editing commands (*New*, *Open*), such menus let you:

- **Import / Export** [All]
- **Share with User**—See Sharing, below.
- **Edit Custom Attributes**
- **View as PDF**
- **Tag** items with a location.

 **NOTE:**

You can also export or import page configurations as well as items Dell OpenManage Network Manager manages like equipment, discovery profiles, locations and so on.

**Aging Policy**—See Redcell > Database Aging Policies (DAP) on page 50 for instructions about configuring these.

## Import / Export

Menus often contain these options:

**Import**—Retrieve a file with an XML description of the listed items in the manager. Some imports can come from a URL.

**Export Selection**—Export a file with a text or XML description of the selected item(s) in the manager

**Export All**—Export a file with a text or XML descriptions of all listed items in the manager.



**Tip**

Printing manager contents: You can *Export* a full size manager into PDF or Excel format and print from there.



**CAUTION:**

You must import into the correct portlet. You cannot import event processing rules into the Actions portlet, for example. You must import event processing rules into the Event Processing Rule portlet.

## Sharing

You can share elements within Dell OpenManage Network Manager with colleagues when more than one user exists on your Dell OpenManage Network Manager system, and consult with them using the texting described in Status Bar Alerts on page 75.



## How To:

### Share a Resource

To share an something, first select it where it appears listed in the appropriate portlet. Right click and select *Share Asset*.

Name	Title	Online	Last Login	Status Message
Suman Sarkar		●	N/A	
Jack Black		●	06/18/10 02:43 PM	
IT dorado		●	06/14/10 05:15 PM	
sample account		●	06/14/10 10:32 AM	
Bill Acevedo		●	06/21/10 12:21 PM	
Mark Sanders		●	06/15/10 02:27 PM	

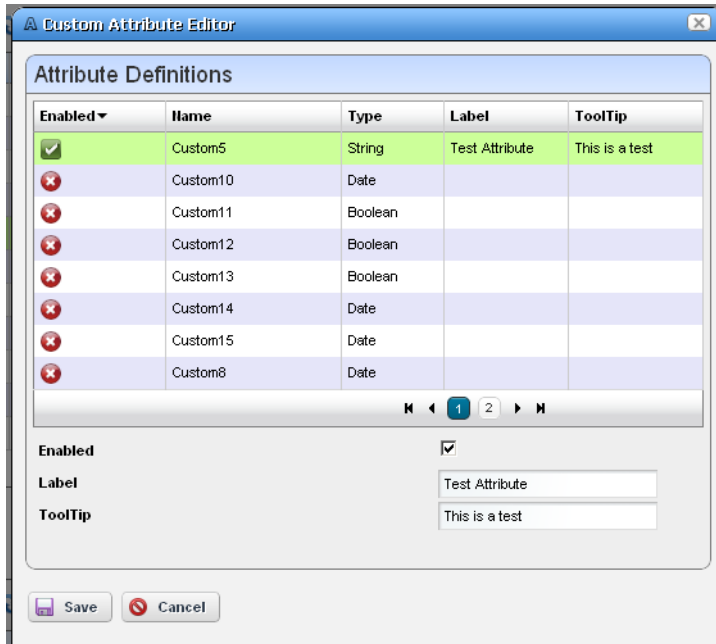
Attachment: [1 - Informational] redcellEquipmentResynchNotification, Result: Success

In the subsequent screen, select a user with whom you want to share, type any message you want to include and click *Share Asset*. The chat message to the selected user includes your text and a link that opens to display the Snap Panels for the selected item. *Cancel* aborts sharing.



## Edit Custom Attributes

In several right-click menus (Managed Equipment, Port, Contact, Vendor, or Location), the *Edit Custom Attributes* menu item lets you open the custom attribute editor appropriate for the device type listed in the portlet. See Redcell > Data Configuration on page 45 for another way to get to this editor.



Selecting a row in the editor lets you edit rows describing custom fields directly. The following are the custom attribute properties you can alter:

**Enabled** — Check Enabled to activate the selected custom field.

**Label** — This is a label for the tooltip identified in the *Name*. The Label is what you see in the portlets appropriate for the entity type you have selected. The *Type* column in the attribute describes the data type of the custom attribute (String, Integer, Date, Boolean—read only). When you select Boolean the field is a checkbox.

**Tooltip** — The tip that appears when you hover the cursor over the custom field.

Click *Save* to preserve any changes you have made, or *Cancel* to abandon them.

## View as PDF

This displays the selected asset's information as a PDF.



You can search, print or save this to file, and use any of the other Acrobat capabilities. Clicking the acrobat logo docks the floating / disappearing Acrobat toolbar within this screen.

### Tip

To search the PDF produced, click the binocular icon in the docked toolbar.

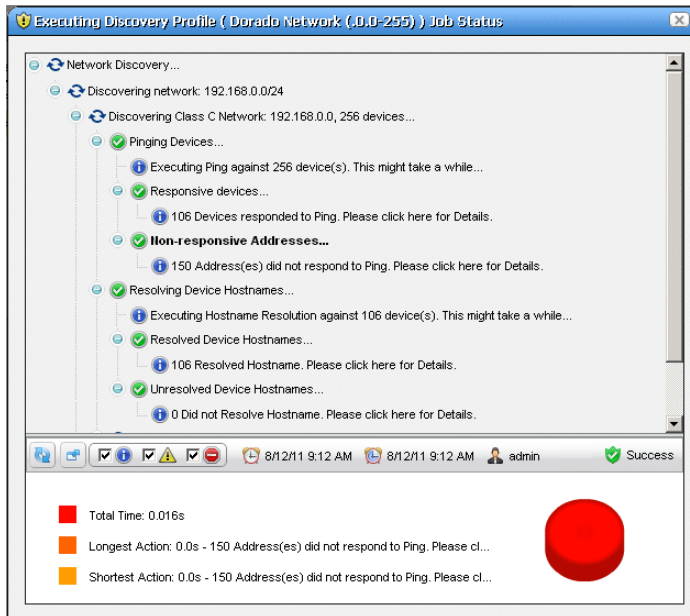
You can also create PDF reports containing descriptions of multiple selected assets, but you must open an expanded portlet to multi-select.

## Tag

The right-click menu of many items lets you tag them, for example Managed Resources, Locations, Contacts, Customers, Services and Containers. When you select the *Tag* menu item, and *Coordinates*, a new Map popup appears (see Tag on page 138) and you can search for an address or click on the map to specify its coordinates. See Map Context on page 151 for more information about the uses of tagging.

# Audit Trail / Jobs Screen

When you execute an action, for example discovering network resources, an audit trail screen appears with a tree displaying the message traffic between Dell OpenManage Network Manager and the device(s) the action addresses.



To see the details of any message, click on it, and those details appear in the lowest panel of this screen. If you click on a summary message (not a “leaf” on the tree), a graph appears displaying the duration for its component messages. Hover your cursor over each portion of the graph for more details.

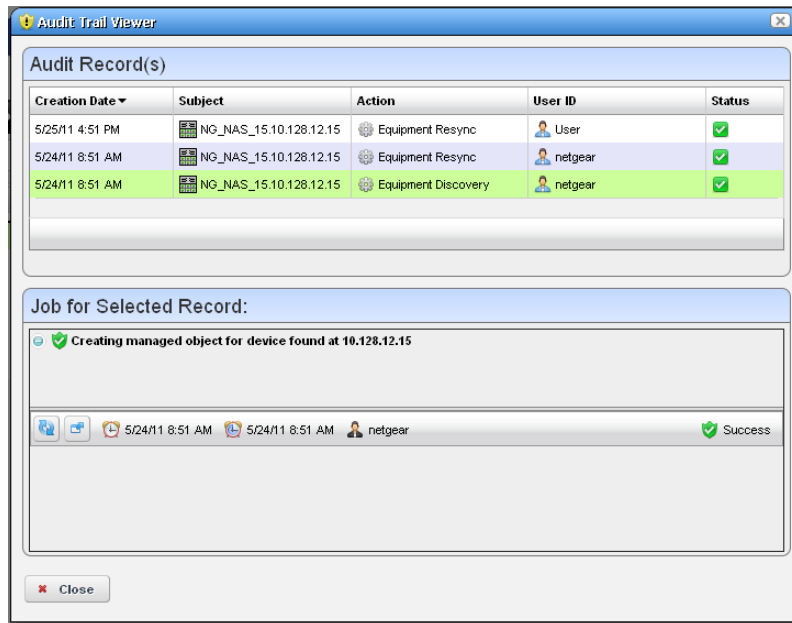
## Tip

The time for messages and logged in user initiating the action appear on the bar between the upper and lower screen, and an icon summarizing the action appears on its right. Click the second icon from the left to configure the amount of detail displayed in audit messages. Click the first (*Refresh*) icon to re-display messages if you re-configure the type(s) displayed.

Close the audit trail viewer any time, and the action continues in the background. The the audit trail is archived in the portlet described in Audit Trail Portlet on page 93.

# Audit Trail Viewer

Some portlets also offer an Audit Trail menu item that displays Audit Trail / Jobs Screens for the selected item.



The top of this screen contains a list of Audit Records. Click one of this list to see the Job details as you would in the Audit Trail / Jobs Screen.

# Audit Trail Portlet

The audit trail summary portlet displays an archive of the message traffic between Dell OpenManage Network Manager and monitored devices, as well as OpenManage Network Manager’s reaction to failed message transmission.

The screenshot shows the 'Audit Trail' portlet with a table of messages. The table has columns for Creation Date, Subject, Action, User ID, and Status. The messages are as follows:

Creation Date	Subject	Action	User ID	Status
8/8/11 9:10 AM	admin	User Modifi...	OWSYSTEM	?
8/8/11 9:07 AM		Proscan Tar...	admin	✓
8/8/11 9:03 AM	admin	User Modifi...	OWSYSTEM	?
8/8/11 8:33 AM	CiscoCat60...	Pool Synchr...	admin	✓
8/8/11 8:33 AM	CiscoCat60...	Equipment R...	admin	✓
8/8/11 8:33 AM	Router.10.1...	Pool Synchr...	admin	✓

The *Creation Date*, *Subject*, *Action* (the summary message of the audit trail), *User ID* (the login ID of the user whose actions resulted in this trail), and *Status* of the messages appear in the table (hover the cursor over the icon for a text message describing status). Right click to *Delete* a message, manage its *Aging Policy* or *View as PDF*. See Redcell > Database Aging Policies (DAP) on page 50 for more about such policies.

## Tip

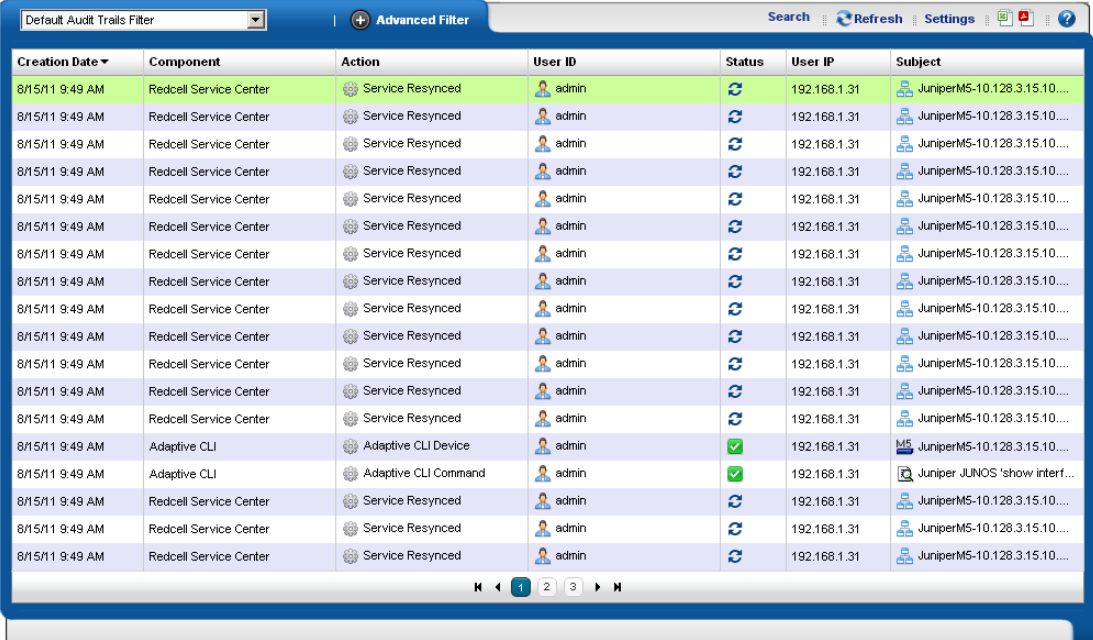
To see the audit trail for recently completed processing, open the *My Alerts* tab in the lower left corner of the portal, and click the magnifying glass to the right of the appropriate message.

The screenshot shows the 'Notifications' portlet with a list of messages. The messages are as follows:

Date	Details
10/11/10 08:37 AM	Learned MAC has been completed.
10/08/10 08:07 AM	Report is now ready for viewing.
10/08/10 08:07 AM	Report completed
10/06/10 02:51 PM	
10/06/10 02:51 PM	
10/06/10 02:51 PM	

## Expanded Audit Trail Portlet

When you click the plus (+) in the upper right corner of the summary screen, the expanded portlet appears. Click the *Settings* button to configure the columns that appear in this screen and their order. Filter the appearance of the screen with the *Advanced Filter* capabilities at its top.



The screenshot shows the 'Audit Trail' portlet interface. At the top, there is a 'Default Audit Trails Filter' dropdown, an 'Advanced Filter' button, and a 'Return to previous' link. Below these are 'Search', 'Refresh', and 'Settings' buttons. The main area is a table with the following columns: Creation Date, Component, Action, User ID, Status, User IP, and Subject. The table contains 18 rows of data, mostly showing 'Service Resynced' actions performed by 'admin' on 'Redcell Service Center' components. One row shows an 'Adaptive CLI Device' action with a green checkmark status. The bottom of the table has a pagination control showing '1', '2', and '3'.

Creation Date	Component	Action	User ID	Status	User IP	Subject
8/15/11 9:49 AM	Redcell Service Center	Service Resynced	admin	🔄	192.168.1.31	JuniperM5-10.128.3.15.10...
8/15/11 9:49 AM	Redcell Service Center	Service Resynced	admin	🔄	192.168.1.31	JuniperM5-10.128.3.15.10...
8/15/11 9:49 AM	Redcell Service Center	Service Resynced	admin	🔄	192.168.1.31	JuniperM5-10.128.3.15.10...
8/15/11 9:49 AM	Redcell Service Center	Service Resynced	admin	🔄	192.168.1.31	JuniperM5-10.128.3.15.10...
8/15/11 9:49 AM	Redcell Service Center	Service Resynced	admin	🔄	192.168.1.31	JuniperM5-10.128.3.15.10...
8/15/11 9:49 AM	Redcell Service Center	Service Resynced	admin	🔄	192.168.1.31	JuniperM5-10.128.3.15.10...
8/15/11 9:49 AM	Redcell Service Center	Service Resynced	admin	🔄	192.168.1.31	JuniperM5-10.128.3.15.10...
8/15/11 9:49 AM	Redcell Service Center	Service Resynced	admin	🔄	192.168.1.31	JuniperM5-10.128.3.15.10...
8/15/11 9:49 AM	Redcell Service Center	Service Resynced	admin	🔄	192.168.1.31	JuniperM5-10.128.3.15.10...
8/15/11 9:49 AM	Redcell Service Center	Service Resynced	admin	🔄	192.168.1.31	JuniperM5-10.128.3.15.10...
8/15/11 9:49 AM	Redcell Service Center	Service Resynced	admin	🔄	192.168.1.31	JuniperM5-10.128.3.15.10...
8/15/11 9:49 AM	Adaptive CLI	Adaptive CLI Device	admin	✅	192.168.1.31	M5 JuniperM5-10.128.3.15.10...
8/15/11 9:49 AM	Adaptive CLI	Adaptive CLI Command	admin	✅	192.168.1.31	Juniper JUNOS 'show interf...
8/15/11 9:49 AM	Redcell Service Center	Service Resynced	admin	🔄	192.168.1.31	JuniperM5-10.128.3.15.10...
8/15/11 9:49 AM	Redcell Service Center	Service Resynced	admin	🔄	192.168.1.31	JuniperM5-10.128.3.15.10...
8/15/11 9:49 AM	Redcell Service Center	Service Resynced	admin	🔄	192.168.1.31	JuniperM5-10.128.3.15.10...

In addition to the summary screen's columns, the following are available in this screen:

**User IP**—The IP address of the user who created this audit trail.

**Subject**—The equipment at the origin of the message traffic with Dell OpenManage Network Manager.

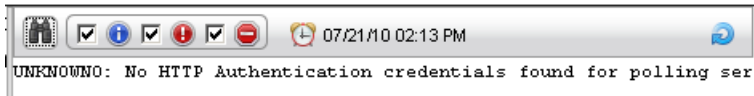
You can right-click a selected item and either *Delete* it, or *View Job*. This last option displays a screen with the details of the job itself.

### View Job

The *Audit Job Viewer* displays the audit trail messages in tree form. To see the contents of an individual message that appears in the upper panel, select it and view its contents in the bottom panel. The divider has the binoculars in the left corner, and the *Refresh* icon in the right. Click *Refresh* to clear an old message so you can view a new one.

Click the binocular icon to check (info, warning, error) filters that limit the types of visible messages.

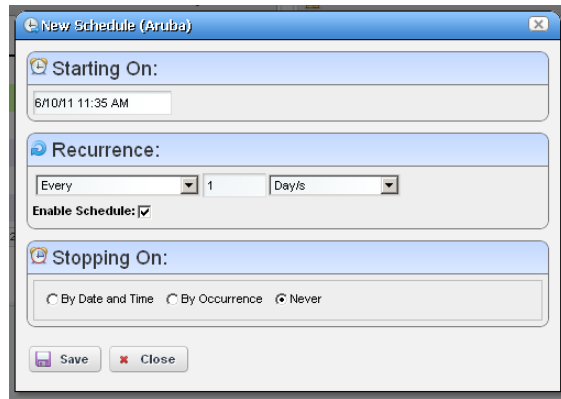
Notice that the date and time of the message appears to the right of the binocular icon.



## Schedules

To schedule an action, for example using a discovery profile, right click and select *Schedule*. The Schedule panel appears, where you can create a new schedule, entering a *Starting On* date and time, and *Stopping On* date and time or occurrence number. You can also configure recurrence in this screen.

Once you save the schedule, the action (for example Discovery Profile) it also appears in the Schedules Portlet as a scheduled item.



## Schedules Portlet

You can view and modify schedules in the *Schedules* portlet, or the Expanded Schedules Portlet

Enabled	Description	Type	Next Execution	Recurrence
<input checked="" type="checkbox"/>	Weekly	Database Agin...	8/12/11 2:00 AM	Recur Weekly
<input checked="" type="checkbox"/>	Refresh Pr...	Refresh Prosc...	8/8/11 3:07 PM	Recur Every 6 ...
<input checked="" type="checkbox"/>	Refresh M...	Refresh Monto...	8/8/11 1:00 PM	Recur Every 6 ...
<input checked="" type="checkbox"/>	Network Li...	Network Link Di...	8/9/11 3:00 AM	Recur Daily
<input checked="" type="checkbox"/>	Network D...	Network Data ...	8/9/11 12:00 AM	Recur Daily
<input checked="" type="checkbox"/>	Monthly	Database Agin...	8/25/11 3:00 AM	Recur Monthly

This displays the *Enabled* status, a *Description*, the *Type* of schedule, its *Next Execution* and *Recurrence* in columns. You can do the following by right-clicking a scheduled item, and selecting the appropriate menu item:

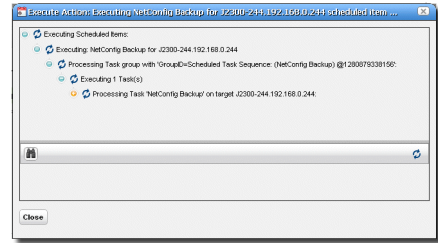
**Delete**—Deletes the selected scheduled item, displaying a confirming dialog box.

**Enable Schedule**—Appears on an already disabled scheduled item so you can change its status. To enable the schedule, you can also edit it and check the *Enabled* check box.

**Disable Schedule**—Appears on an already enabled scheduled item.

**Execute**—Executes the scheduled item. If the scheduled item is an activity-based or discovery-profile based scheduled item, an audit viewer appears progress of the selected item.

For other types of scheduled actions, a dialog appears saying *The scheduled item(s) has been sent to the application server for immediate execution.* You can monitor its progress in the audit trail portlet. (see *Audit Trail / Jobs Screen on page 91*)



**New**—This lets you initiate new schedules for a variety of actions, selected from a sub-menu. The subsequent screen's appearance depends on the action selected. See *Managed Resources on page 166* for more about available actions. See *Scheduling Actions on page 369* for the details of scheduling actions that require parameters.

**Open**—This appears for an activity-based scheduled items. It opens the activity editor, and lets you modify the activity's data/properties and schedule parameters.

To edit an existing schedule for an already scheduled action like a Discovery Profile, just right click the item in its portlet and select *Schedule*. This displays the schedule information for the discovery profile and lets you make modifications.

 **Tip**

Schedule new actions from the portlet that ordinarily executes them, for example *Resource Discovery on page 152*.

If you have Dell OpenManage Network Manager's Change Management / Proscan capabilities installed, you can use Schedules to initiate the Change Determination process. See *Change Determination Process on page 326*. It is disabled by default.



## Expanded Schedules Portlet

When you expand this portlet, the additional columns that appear include *Submission Date*, *Start Date*, whether the schedule is still active (*Scheduled*), and the *Execution Count*.

The screenshot shows the 'Schedules' portlet interface. At the top, there is a 'Default Schedules Filter' dropdown and an 'Advanced Filter' button. To the right are 'Search', 'Refresh', and 'Settings' options. The main table lists various schedules with the following columns: Enabled (checkbox), Description (calendar icon), Type, Submission Date, Start Date, Next Execution, Recurrence, End Date, Scheduled (checkbox with green or red icon), and Execution Count. Below the table is a 'Reference Tree' showing a 'Weekly' schedule icon.

Enabled	Description	Type	Submission Date	Start Date	Next Execution	Recurrence	End Date	Scheduled	Execution Count
<input checked="" type="checkbox"/>	Weekly	Database Agi...	2/24/11 8:19 AM	2/25/11 2:00 AM	8/19/11 2:00 AM	Recur Weekly	Never Ending	<input checked="" type="checkbox"/>	0
<input checked="" type="checkbox"/>	Refresh P...	Refresh Pros...	12/15/10 2:06 PM	12/15/10 2:07 PM	8/15/11 3:07 PM	Recur Every ...	Never Ending	<input checked="" type="checkbox"/>	1
<input checked="" type="checkbox"/>	Refresh ...	Refresh Mont...	12/4/09 5:27 PM	12/7/09 6:00 AM	8/15/11 1:00 PM	Recur Every ...	Never Ending	<input checked="" type="checkbox"/>	1
<input checked="" type="checkbox"/>	Network ...	Network Link ...	12/15/10 10:11 AM	7/1/10 3:00 AM	8/16/11 3:00 AM	Recur Daily	Never Ending	<input checked="" type="checkbox"/>	0
<input checked="" type="checkbox"/>	Network ...	Network Data...	12/15/10 10:11 AM	7/1/10 12:00 AM	8/16/11 12:00 AM	Recur Daily	Never Ending	<input checked="" type="checkbox"/>	0
<input checked="" type="checkbox"/>	Monthly	Database Agi...	2/24/11 8:21 AM	2/25/11 3:00 AM	8/25/11 3:00 AM	Recur Monthly	Never Ending	<input checked="" type="checkbox"/>	0
<input checked="" type="checkbox"/>	Every 12 ...	Database Agi...	2/24/11 8:17 AM	2/25/11 12:00 AM	8/15/11 1:00 PM	Recur Every ...	Never Ending	<input checked="" type="checkbox"/>	0
<input checked="" type="checkbox"/>	disL3-aug...	Tasks	12/31/09 4:00 PM	8/15/11 9:45 AM		Recur Once ...	End after 1 oc...	<input checked="" type="checkbox"/>	0

If a green icon appears in the *Scheduled* column, it means the schedule will be executed on next start date. If the schedule has exceeded execution count or passed stop date (if specified), then a red icon appears there.



## Key Portlets

This section describes some of the key Dell OpenManage Network Manager portlets. You may not have access to all of these in your installation, or you may not be able to use them with the user permissions you have been assigned by the portal administrator.

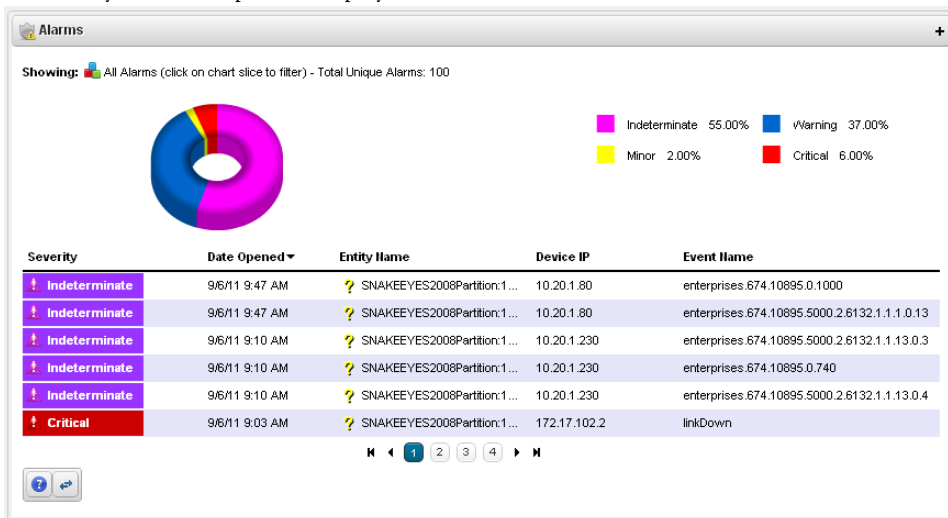
To see all available Dell OpenManage Network Manager portlets, click *Add > Applications* and use the field at the top of the menu to search for the portlet functionality you want to add. This limits the display to Dell OpenManage Network Manager portlets. The previous chapter discussed the Schedules Portlet on page 95.

### Tip

Filter what appears on a page with the Container View portlet. Select a container, and the rest of the portlets on that page filter their data reporting to reflect that container's contents. The only caveat for this advice is that Container View is non-instanceable. In other words, you can only add one of them.

## Alarms

In its summary form, this portlet displays alarms



The chart can act as a filter, too. For example, clicking the *Critical* alarms slice means only *Critical* alarms appear listed. Notice also that the chart “explodes” to highlight the selected slice. Hover the cursor over a portion of the chart and a tooltip with information about that slice also appears.

By default, the chart appears only when there are alarms. See *Configuring the Alarms Chart* below for options available in configuring the display. See *Menu* on page 102 for details about menu items available when you right-click in the summary and expanded portlets. The following columns appear in this screen by default:

**Severity**—The alarm severity indicated by the color of the leftmost icon. The severity only has meaning for Alarms and Security Alarms. Informational Alarms get a severity level of Indeterminate. Closed alarms appear without color.

**Date Opened**—The date the alarm appeared.

**Entity Name**—The entity emitting this alarm (often within the Equipment).

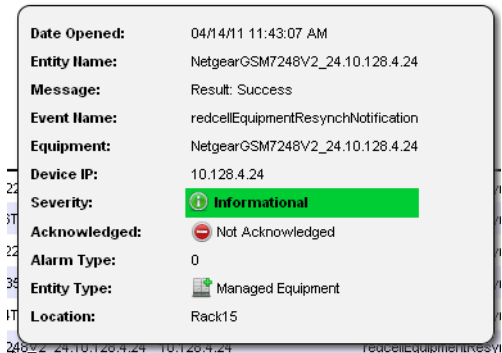
**DeviceIP**—The IP address of the equipment where the alarm appeared.

**Event Name**—The event associated with the alarm.

 **Tip**

If you hover the cursor over a row in the portlet display, a tooltip appears with information about the alarm. This can include the alarm’s *Date Opened*, the *Entity Name*, any alarm *Message*, *Event Name*, *Alarm* and *Entity Type*, its status as *Service Effecting*, *Notification OID*, *Equipment*, *Severity*, whether the alarm was *Suppressed*, or *Acknowledged* and the *Device IP*.

If an alarm is **Service Effecting**, (reflect an impact on a service) it can propagate to appear as components of service- and link-related alarms. Service-effecting alarms are of indeterminate or greater severity.



See *Alarms in Visualizations / Topologies* on page 219 for a description of how alarms appear in the topology portlet. The next section (*Expanded Alarm Portlet*) describes alarm actions and additional alarm capabilities.

## Configuring the Alarms Chart

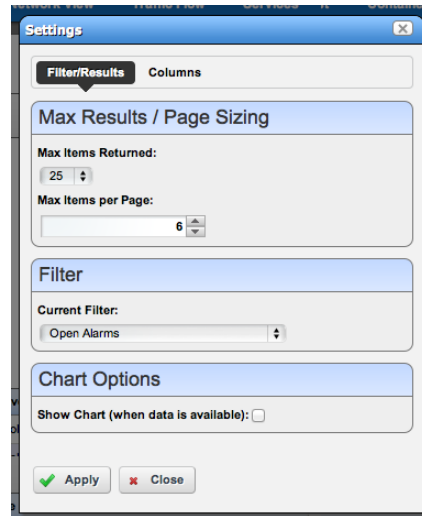
Turn the chart on or off in the *Settings* screen's *Chart Options* panel. If no data exists for the chart and the Chart option is on, the portlet returns to “no-chart” mode.

When you enable the chart Filtering is disabled since the chart, in effect, provides the filter. When the chart is disabled then filtering options are available.

Settings are saved if you have Admin rights or the Portlet is on your Public / Private pages (like standard behavior).

### NOTE:

Changes appear after you click *Apply*. The *Filter* panel disappears when you check the *Show Chart* checkbox.



## Expanded Alarm Portlet

The expanded Alarm portlet appears when you click the plus (+) in the top right corner of the smaller screen.

Severity	Date Opened	Count	Entity Name	Device IP	Entity Type	Event Name	Message
Minor	8/15/11 9:54 AM	1	JuniperJ2300-1...	10.128.3.16	Managed Equipment	redcellNetConfigBackupFailu...	Unable to identify or resol...
Minor	8/15/11 9:54 AM	1	JuniperM5-10.1...	10.128.3.15	Managed Equipment	redcellNetConfigBackupFailu...	Unable to identify or resol...
Minor	8/15/11 6:43 AM	116	QA-XP-004Parti...	10.20.1.157	Unknown	authenticationFailure	

This displays listed alarms and Snap Panel details of a selected alarm. By default this screen adds the first of the following columns to those visible in the Event History's summary screen view. To add the others listed here, right click, and select *Add Columns* to change the screen appearance. The following are available additional columns, besides those visible in the Alarms summary portlet:

**Count**—A count of the instances of the alarm. Multiples of the same alarm appear as a single row, but increment this count.

**Entity Type**—The type of monitored entity.

**Message**—Any message that accompanies the alarm / event.

**Alarm State**—The state (open / closed) of the alarm.

**Date Cleared**—The date and time that the alarm was closed.

**UpdateDate Time**—The time stamp for when this alarm was updated (for an additional count, the time the last duplicate was received).

**Notification OID**—The identifier of the notification displayed as an alarm.

**Equipment**—The name for the entity emitting the alarm.

**Acknowledged**—*True* or *False*.

**Assigned User**—The user who has been assigned this alarm (right click or click *Action* to do this).

**Date Assigned**—The date and time that the alarm was assigned.

**Ack Time**—The time the alarm was acknowledged.

**Cleared By**—The user who cleared the alarm.

**MIB Text**—The alarm's MIB Text.

Rather than filtering with the pie graph, the expanded portlet lets you either the pick list at the top left, or create custom filtering by clicking *Advanced Filters*.

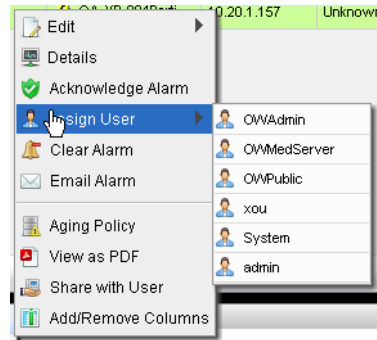
## Menu

Right clicking an alarm lets you select from the following menu items:

**Edit**—Access the editors for *Event Definition* (see Event Definition Editor on page 128) or the *Details* screen for the entity emitting the alarm (see Equipment Details on page 178 for an example).

**Details**—Open a Details screen for the alarm itself, not the entity emitting it. This contains information like the MIB text, any Event Processing Rules invoked, and a Reference Tree for the alarm.

**Visualize**—Display a topology map that includes the selected alarm(s). See Chapter 5, Visualize My Network for more about these maps.

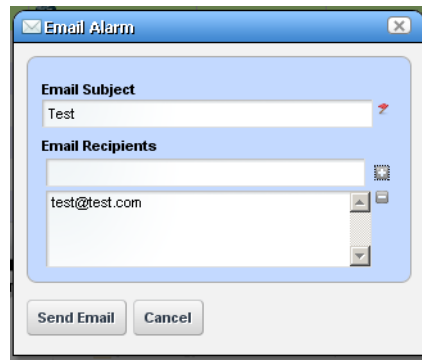


**Acknowledge / Unacknowledge Alarm**—Acknowledges the selected Alarm(s). The current date and time appear in the Ack Time field. Unacknowledges previously acknowledged alarm(s), and clears the entries in the Ack By and Ack Time fields. The red “unacknowledged” icon appears in the expanded portlet and turns to a green check “acknowledged” icon the alarm has been acknowledged.

**Assign User**—Assign this alarm to one of the users displayed in the sub-menu by selecting that user. An icon also appears in the expanded portlet indicating the alarm has been assigned to someone.

**Clear Alarm**—Clearing the alarm removes the alarm from the default alarm view and marks it as a candidate for the database archiving process (DAP). Essentially it is an indication to the system that the alarm has been resolved/addressed. If your system has enabled propagation policies, clearing recalculates dependent alarms.

**Email Alarm**—E-mail the alarm. Enter a subject an e-mail address to which you want to mail the alarm’s content, and click the + to add to the list of addresses (the minus deletes them). Then click *Send Email*. Clicking *Cancel* ends this operation without sending e-mail. See SMTP Configuration on page 69 for instructions about setting up e-mail from Dell OpenManage Network Manager. See Alarm Email on page 104 for an example of what the content looks like.



**Show Performance**—Displays a performance dashboard for the alarmed equipment. See Dashboard Views on page 277 for more about these.

**Aging Policy**—This lets you select a policy that determines how long this alarm remains in the database. See Redcell > Database Aging Policies (DAP) on page 50 for information about configuring such policies.

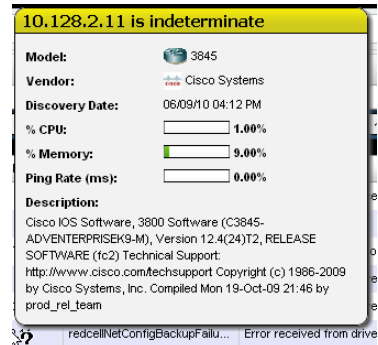
**View as PDF**—Create an Acrobat PDF document containing this portlet’s contents.

**Share with User**—Selecting this opens a screen where you can select the user you want to send the selected alarm, and can enter a message you want to send with it. See Sharing on page 87. Clicking *Share Asset* sends a chat message to the selected user with a link that opens to display the Alarm Snap Panels for the selected item.

 **Tip**

Hover your cursor over the *Device IP Address* column, and a tooltip appears with information about the alarm source's *Model*, *Vendor*, *Discovery Date*, and a *Ping Rate* bar graph. This can also include other device-dependent items. For example: bar graphs to display the *% CPU* [utilization], *% Memory*, and *Description*.

The convention indicating such tooltips are available is the question mark that appears next to the cursor when you hover it over the displayed field.



**Alarm Snap Panels**

These include the following:

**Alarm Details**—The source, *Severity*, *Message*, *Date Opened*, and so on.

**MIB Details**—The *Notification OID*, and *MIB Text* for the selected alarm.

**Reference Tree**—The connection between the alarm and its source in tree form.

**Total Occurrences by Date**—A graph of the total occurrences of this alarm, by date.

**Alarm Email**

The e-mail sent by right-clicking an alarm has the subject specified when you send it, and contains the information within the alarm. For example:

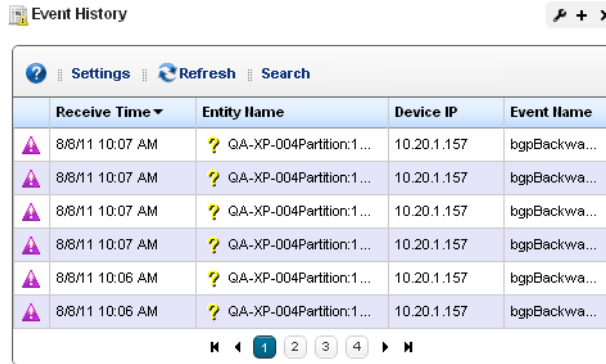
```
Alarm: monitorIntervalSkip
Alarm Attributes:
=====
Device IP           =
Message             =
Alarm State         = Open
Severity            = 5 - Major
Count               = 1
Date Opened         = Tue Dec 14 22:01:30 PST 2010
Update Date/Time    = Tue Dec 14 22:01:36 PST 2010
```



Entity Name =  
Entity Type =  
Entity Description =  
Equipment =  
Region = SUPDEMOPartition  
Location =  
Assigned By = OWSystem  
Date Assigned = Thu Dec 16 10:40:24 PST 2010  
Assigned User = qatester  
Acknowledged = false  
Ack By =  
Ack Time =  
Cleared By =  
Date Cleared =  
MIB Text = Monitor session was skipped due to resource  
constraints. Typically, this implies one or more monitors should run  
less frequently. This may also be caused by a large number of timeouts  
which force executions to take longer to complete than normal.  
Advisory Text =

# Event History

Not all events appear as alarms. Event History preserves all event information for your system.



The screenshot shows the 'Event History' portlet interface. At the top, there are icons for 'Settings', 'Refresh', and 'Search'. Below this is a table with the following columns: 'Receive Time', 'Entity Name', 'Device IP', and 'Event Name'. The table contains six rows of event data. Below the table is a pagination control with buttons for 'Previous', '1', '2', '3', '4', and 'Next'.

Receive Time	Entity Name	Device IP	Event Name
8/8/11 10:07 AM	QA-XP-004Partition:1 ...	10.20.1.157	bgpBackwa...
8/8/11 10:07 AM	QA-XP-004Partition:1 ...	10.20.1.157	bgpBackwa...
8/8/11 10:07 AM	QA-XP-004Partition:1 ...	10.20.1.157	bgpBackwa...
8/8/11 10:07 AM	QA-XP-004Partition:1 ...	10.20.1.157	bgpBackwa...
8/8/11 10:06 AM	QA-XP-004Partition:1 ...	10.20.1.157	bgpBackwa...
8/8/11 10:06 AM	QA-XP-004Partition:1 ...	10.20.1.157	bgpBackwa...

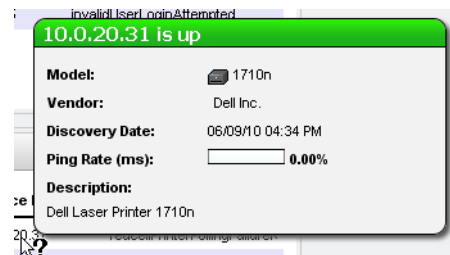
The initial portlet view displays an icon whose color reflects any alarm state associated with the event. It also displays the *Receive Time*, *Entity Name*, *Device IP*, and *Event Name*. You can right-click to *Share with User* in this screen.

## Tip

Hovering the cursor over the *DeviceIP* column produces a tooltip that lets you know the device's current state (*up / down*) and that contains *Model*, *Vendor*, *Discovery Date*, *Ping Rate (ms)*, and the device's *Description* information.

## NOTE:

The default filter for this portlet displays only recent events. If you do not see events, expand the period for which they appear.



## Expanded Event History Portlet

Clicking the plus (+) in the upper right corner of the initial portlet view displays the expanded Event History. As in other expanded portlets, you can use the filtering capabilities at the top of the screen to further limit the default view of all events.

The screenshot shows the 'Event History' portlet interface. At the top, there is a 'Default Event History Filter' dropdown and an 'Advanced Filter' button. To the right are 'Search', 'Refresh', and 'Settings' buttons. Below this is a table with the following columns: Receive Time, Entity Name, Event Name, Entity Type, Device IP, Message, and Protocol. The table contains several rows of event data, including 'serviceResyncNotification' and 'adaptiveCLIRunSuccessNotifica...'. Below the table is a navigation bar with page numbers 1 through 6. At the bottom of the portlet, there are three panels: 'Reference Tree', 'Bindings', and 'MIB Details'. The 'Reference Tree' panel shows a tree view of the event. The 'Bindings' panel shows various attributes like serviceName, serviceState, serviceStatus, serviceSummary, sysUpTime, snmpTrapOID, serviceID, and serviceType. The 'MIB Details' panel shows the notification OID and MIB text.

Receive Time	Entity Name	Event Name	Entity Type	Device IP	Message	Protocol
8/15/11 9:58 AM	JuniperMS-10.1...	serviceResyncNotification	Service			System
8/15/11 9:58 AM	JuniperMS-10.1...	adaptiveCLIRunSuccessNotifica...	Managed Equi...	10.128.3.15	Success: Juniper JUNOS 'show...	System
8/15/11 9:58 AM	JuniperMS-10.1...	serviceResyncNotification	Service			System
8/15/11 9:58 AM	JuniperMS-10.1...	adaptiveCLIRunSuccessNotifica...	Managed Equi...	10.128.3.15	Success: Juniper JUNOS 'show...	System
8/15/11 9:58 AM	JuniperMS-10.1...	serviceResyncNotification	Service			System
8/15/11 9:58 AM	JuniperMS-10.1...	serviceResyncNotification	Service			System
8/15/11 9:58 AM	JuniperMS-10.1...	adaptiveCLIRunSuccessNotifica...	Managed Equi...	10.128.3.15	Success: Juniper JUNOS 'show...	System
8/15/11 9:58 AM	JuniperMS-10.1...	serviceResyncNotification	Service			System

**Reference Tree**

- 2011-08-15 09:58:18 serviceResyncNotification
  - JuniperMS-10.128.3.15.10.128.3.15\_vrf1-aug9th11\_...

**Bindings**

**serviceName.0:** JuniperMS-10.128.3.15.10.128.3.15\_vrf1-aug9th11\_MS DP\_PEER\_1.1.1.16

**serviceState.0:** Provisioned

**serviceStatus.0:** Ok

**serviceSummary.0:** JuniperMS-10.128.3.15.10.128.3.15\_vrf1-aug9th11\_MS DP\_PEER\_1.1.1.16 (714)

**sysUpTime.0:** 3 hours, 18 mins, 29 secs

**snmpTrapOID.0:** 1.3.6.1.4.1.3477.397.2.1

**serviceID.0:** 714

**serviceType.0:** Juniper MSDP Peer

**MIB Details**

**NOTIFICATION OID:** 1.3.6.1.4.1.3477.397.2.1

**MIB TEXT:** Service Modified (Resync)

This screen has columns described in Alarms on page 99 or Expanded Alarm Portlet on page 101. Configure these as visible or hidden by clicking *Settings*. The following are some additional columns available.

**Receive Time**—The date the event was received.

**Event Name**—The event identifier.

**Location**—The location of the equipment emitting the event.

**SubType**—A classification for the event. For example: *Trap*.

**Protocol**—The protocol that delivered the event. Frequently: *System*, indicating Dell OpenManage Network Manager itself delivered it.

**Notification OID**—The object identifier (OID) for the event type.

**Instance ID**—The instance identifier for the event.

## Event History Snap Panels

Click a listed alarm to display its details in the Snap Panels. The *Reference Tree* displays the event's relationship to any alarms, and to the source device. Click the plus (+) next to an item in the tree to unpack it.

The *Bindings* Snap Panel displays the event's varbind information, including the trap OID, the device's IP address, and other event-specific information.

The *MIB Details* Snap Panel includes MIB information like the Notification OID and MIB Text.

You can right-click the listed events and *Share with User* (see *Sharing on page 87*), or (How to:) Show / Hide / Reorder Columns.

# Event Processing Rules

This portlet manages Dell OpenManage Network Manager's response to events. By default it appears with seeded rules, but you can create your own (*New*), copy or modify (*Copy* or *Open*) or delete (*Delete*) existing rules by right-clicking in the portlet. You can also *Import* and *Export* rules to files.

The *Rule Type* column indicates whether rules are Pre-Processing (Correlation) or Post-Processing (Automation).

Icons in the *Enabled* and *System* columns indicate whether the rule is enabled—green is enabled, red is not—and whether it is a *System* rule, or a non-system (user-created) rule.

Modifying or creating rules opens Rule Editor. See *How to: Create Event Processing Rules* for steps to create these rules.

When you *Copy* an event processing rule, Dell OpenManage Network Manager generates a new name, but you must change that name before you save the event processing rule.

Rule Name	Rule Type	Enabled	System
swTrackChangesTrapV2	Automation	✓	✓
swSensorScnV2	Automation	✓	✓
swFCPortScanV2	Automation	✓	✓
swFaultV2	Automation	✓	✓
swFabricWatchTrapV2	Automation	✓	✓
swEventTrapV2	Automation	✓	✓

## Expanded Event Processing Rules Portlet

The expanded portlet displays additional columns. Details about selected rules appear in the snap-in panels at the bottom of this screen.

Rule Name	Rule Type	Enabled	System
Dell Powerconnect Login Failed	Event Correlation	✓	✓
Database Free Space Low	Event Correlation	✓	✓
Configuration Change	Automation	✓	✓
ciscoConfigManEvent	Automation	✓	✓
Cisco User Login Failed	Event Correlation	✓	✓
Cisco User Logged In	Event Correlation	✓	✓
Backup and Change Determination Process	Automation	✓	✓
Add new equipment to heartbeat	Automation	✗	✓

**Reference Tree**

- Add new equipment to heartbeat

**Rule Actions**

Name	Description
Add to default Heartbeat P...	

**Event Filter Summary**

- Match All of the following
  - Event Name is redcellEquipmentDiscoveryNotificati...

The *Reference Tree* panel displays the selected rule's connection to events. The *Rule Actions* list any configured actions associated with the rule. The *Event Filter Summary* summarizes any configured filter(s) for the selected rule.



### How To:

#### Create Event Processing Rules

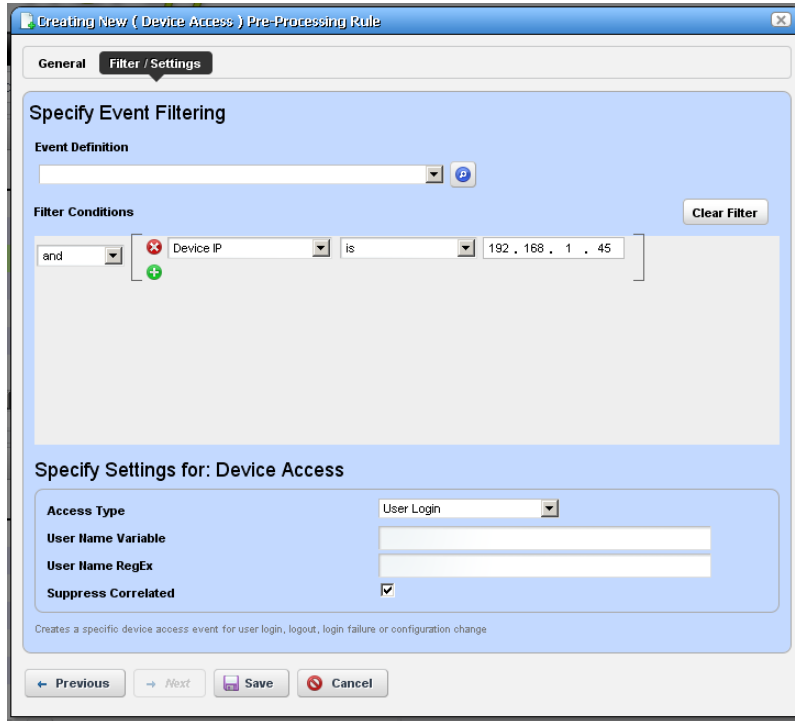
To create a rule in this portlet, follow these steps:

- 1 Right-click and select *New*, then select a rule type. These can be *Pre-Processing* (correlation) or *Post-Processing* (automation) rules.

If *Pre-Processing* is your selection, *Device Access*, *Frequency Throttle*, *Reject Event*, *Set Severity*, *State Flutter*, *Suppress Alarm*, and *Syslog* are the types available. See *Filtering /*

Settings on page 112, Syslog Escalation Criteria on page 115, and Actions on page 116 for more about the differences available between rule types.

- 2 For this example, we select Pre-Processing > Device Access. The Rule Editor screen appears. Enter a *Name* to identify the rule, an optional *Description*, and check *Enabled* if you want this rule to begin working immediately.
- 3 Click *Next* to open the Filtering / Settings tab.



### Specify Event Filtering

In this panel select the *Event Definition*. Click pick list to find available events. Typing a letter goes to that letter in the list. You can then click to select from the pick list.

Click *Add Filter* to further filter the selected events. See Filter Expanded Portlet Displays on page 85 for more about this feature.

### Specify Settings for: [Selected Rule Type]

This panel's appearance depends on the type of rule you selected when you clicked *New*. When you are editing an existing rule, it defaults to that rule's screen. For more about the available alternatives, see Filtering / Settings on page 112.

- 4 The *Device Access* example creates a specific device access event for user login, logout, login failure or configuration change. Select the *Access Type* (*Config Change, Login Failure, User Login, User Logout*) from the pick list for that field.
- 5 Enter the *User Name Variable* and/or *User Name RegEx* match string in those fields. This confines rule response to the selected users.
- 6 Check *Suppress Correlated* events if you do not want to see events correlated with this one.
- 7 Click *Save* to preserve the event processing rule.

## Rule Editor

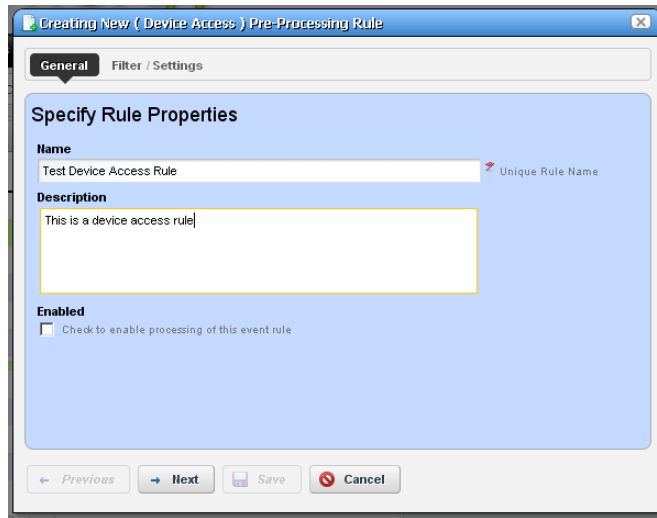
After you select between pre- and post-processing rules for new rules, the following screens manage the event processing described in brief in the Create Event Processing Rules on page 109. The following screens and fields appear in this editor.

- General
- Filtering / Settings
- Syslog Escalation Criteria (for pre-processing Syslog rules)
- Actions (for post-processing, automation rules)

The following sections describe these in detail.

### General

The General screen is common to all rule types.



The screenshot shows a window titled "Creating New ( Device Access ) Pre-Processing Rule". The window has a tabbed interface with "General" selected and "Filter / Settings" as an alternative. The main area is titled "Specify Rule Properties" and contains the following fields:

- Name:** A text input field containing "Test Device Access Rule". To the right of the field is a red asterisk icon and the text "Unique Rule Name".
- Description:** A text area containing "This is a device access rule".
- Enabled:** A checkbox labeled "Check to enable processing of this event rule", which is currently unchecked.

At the bottom of the window, there are four buttons: "Previous" (with a left arrow), "Next" (with a right arrow), "Save" (with a floppy disk icon), and "Cancel" (with a red circle and slash icon).

It contains the following fields:

**Name**—A text identifier for the rule.

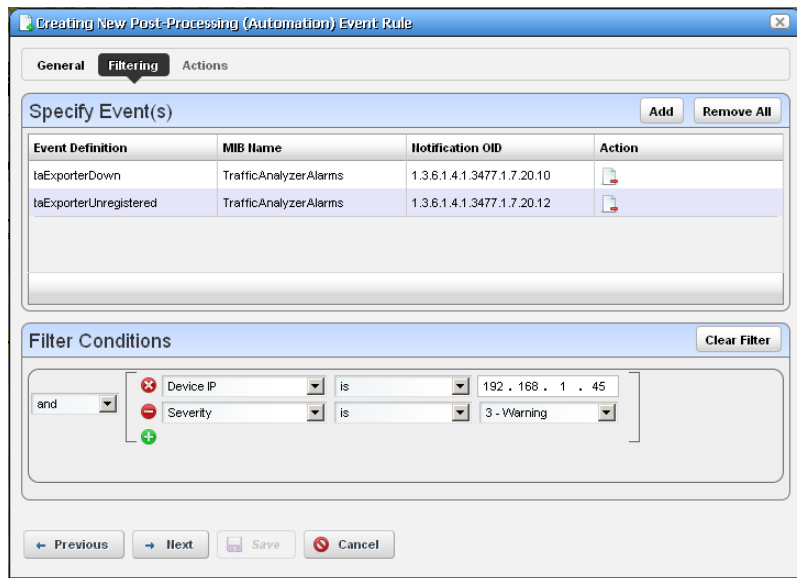
**Description**—An optional text description of the rule

**Alarm Only**—This is visible only in post-processing rules. Check this to enable the rule only if an alarm is generated, not suppressed.

**Enabled**—Check this to enable the rule.

## Filtering / Settings

For all rule types, select the *Event Definition*. Click *Add* to open a screen where you can select events to include in the event you are creating. This includes a filter at the top that you can use to search for specific events. For example: *Event Name Contains \_\_\_\_\_*. You can then click *Add Selection* to include selected items in this filter, or *Add All* to include all displayed events. After you finish event selection, click *Done* at the bottom of this selection screen.



Click *Add Filter* to further filter the selected events. See *Filter Expanded Portlet Displays* on page 85 for more about this feature. After you *Add Filter* the button changes to *Clear Filter* so you can remove any filter from the event rule.

### Tip

Dell OpenManage Network Manager supports multiple IP addresses per resource. During event processing, filters that include IP address criteria may behave incorrectly when Dell OpenManage Network Manager evaluates the filter. Best practice is using resource name(s) instead of IP addresses.

The following are processing rule types, and a description of their properties.



**Pre-Processing**—These rules either override the event definition, change the behavior of an event or generate another event. The following are the different subtypes. These are also called *Correlation* rules. See the descriptions below for additional information about the available types.

**Post-Processing**—Also called *Automation* rules, these execute specified actions for the rule after the event processing occurs.

The following are *Pre-Processing/ Correlation* rule subtypes:

**Device Access**—The Device Access example creates a specific device access event for user login, logout, login failure or configuration change. Select the *Access Type* (*Config Change, Login Failure, User Login, User Logout*) from the pick list for that field.

**Specify Settings for: Device Access**

<b>Access Type</b>	User Login
<b>User Name Variable</b>	test
<b>User Name RegEx</b>	
<b>Suppress Correlated</b>	<input checked="" type="checkbox"/>

Creates a specific device access event for user login, logout, login failure or configuration change

Enter the *User Name Variable* and/or *User Name RegEx* match string in those fields. This confines rule response to the selected users.

Check *Suppress Correlated* events if you do not want to see events correlated with this one.

**Frequency Throttle**—This rule type changes event behavior based on the frequency of the selected event.

**Specify Settings for: Frequency Throttle**

<b>Time Period specified in seconds</b>	5
<b>Maximum events to publish within time period</b>	2
<b>Event action to take when throttle exceeded</b>	Reject <input checked="" type="radio"/> Suppress <input type="radio"/>
<b>Publish frequency start and stop notifications</b>	<input type="checkbox"/>

Changes event behavior based on occurrence frequency

Enter the *Time Period*(seconds) and *Maximum events to publish within time period* for the event, then select an *Event Action to take when throttle exceeded* (*Reject* or *Suppress* the event) and check *Publish frequency start and stop notifications* if you want it to register for Dell OpenManage Network Manager. If you *Reject* an event, it does not appear in Event history; if you *Publish* it, however, listeners for that event will “hear” it.

**Reject Event**—This screen presents the *Specify Event Filtering* portion of the screen without any *Settings* in the lower screen. Specify events to reject with this selection and filtering.

**Set Severity**—This rule overrides the default alarm severity of an event selected and filtered in the upper screen.

**Specify Settings for: Set Severity**

Set Severity

Overrides the default severity of the event

**State Flutter**—This type of rule changes event behavior on transient state change events like a series of LinkUp and LinkDown events for the same interface.

**Specify Settings for: State Flutter**

Interval

Action Reject  Suppress

Publish Event

Changes event behavior on transient state change events such as a series of linkDown and linkUp events for same interface

After you select the event and filtering, enter the *Interval* (seconds), the *Action* (*Reject* or *Suppress* the event) and check *Publish Event* if you want it to register for Dell OpenManage Network Manager. If you *Reject* an event, it does not appear in Event history; if you *Publish* it, however, listeners for that event will “hear” it.

**Suppress Alarm**—This screen presents the *Specify Event Filtering* portion of the screen without any *Settings* in the lower screen. Specify events/alarms to suppress with this selection and filtering.

**Syslog**—This screen presents the *Specify Event Filtering* portion of the screen without any *Settings* in the lower screen. Specify events to select. Then click *Next* to go to the *Escalation* tab.

Post-processing (automation) rules let you modify the *Specify Event Filtering* portion of the screen without any *Settings* in the lower screen. Specify events to select. Then click *Next* to go to the *Actions* tab. See Actions on page 116 for more about that feature.

## Syslog Escalation Criteria

This tab of Syslog Event Rules lets you manage events based on matching text, and configure messages in response to such matches.

The screenshot shows a configuration window titled "Adding New Syslog Escalation Criteria" with three tabs: "General", "Filtering", and "Escalation". The "Criteria" tab is active, and the "Message Test" sub-tab is selected. The "Syslog Match Text" section contains a "Message Match Text" input field with a plus icon, a list box containing "test" and "test2", and a "Match Any" checkbox which is checked. Below this is the "Syslog Event Setup" section with fields for "Category" (TestVarBind), "Event Severity" (Indeterminate), "Message Pattern" (\*), and "Message Template" (TestTemplate). At the bottom are "Apply" and "Cancel" buttons.

### Criteria: Syslog Match Text

In this tab, enter the Syslog Match Text. Click the plus to add matching text to the list below the *Message Match Text* field. Check the *Match Any* to match any or all of the entered match text, rather than one or more specific strings.

### Criteria: Syslog Event Setup

This portion of the Criteria screen sets up the event emitted when matching occurs. Here are the fields:

**Category**—The syslog category varbind value.

**Event Severity**—Select the alarm severity of the event emitted when a match occurs.

**Message Pattern**—An optional regular expression for the text to retrieve and transmit in the created event's message.

**Message Template**—The configuration of the message when sent. For example: the template %1 occurred on %3 for %2 creates a message with the first message pattern retrieved, followed by the third, then the second within the specified text.

### Message Test

This screen lets you test your message against the pattern and/or template. Click the *Test* button to the right of the top field to activate this testing.

**Test Message**—Enter a message to test.

**Test Message Result**—The text extracted for the event as it appears in the template.

Click *Apply* to accept these escalation criteria, or *Cancel* to abandon them without saving.

### Actions

This screen catalogs the actions configured for the Post-Processing (Automation) rule you have configured in previous screens.



Click *Add Action* to create a new action in the editor. The *Actions* column lets you revise (*Edit this entry*) or *Delete* entries in this table. Click *Save* to preserve the action(s) configured here, or *Cancel* to abandon any edits.

Clicking *Add Action* lets you select from the following:

- Forward Northbound
- Email
- Custom

Click *Apply* to accept configured actions, or *Cancel* to abandon their editor and return to this screen.



### Tip

Actions available here are like those for Discovery Profiles on page 153.

## Forward Northbound

When you want to forward an SNMP v2 event (trap) to another host, then configure automation in this screen to do that.

**Adding New Northbound Forwarding Action**

**Settings for Northbound Forwarding as SNMPv2**

**Destination Address**  
192.168.1.126

**Destination Port**  
162

**Community String**  
public

**Send as Proxy**

Enter the following fields:

**Destination Address**—The IP address of the northbound destination.

**Destination Port**—The port on the northbound destination.

**Community String**—The SNMP community string for the northbound destination.

**Send as Proxy**—When checked, this sends the IP address of the application server as the source of the event. Unchecked, it sends the IP address of the source device. (See Send as Proxy on page 118 for more.)

## Trap Forwarding Process

### SNMPv1 and SNMPv3 traps become SNMPv2 Traps

SNMPv1 traps are converted according to RFC 1908. SNMPv3 traps are already in SNMPv2 format and the application simply does not use SNMPv3 security when sending these northbound. The following is the relevant snippet from RFC 1908:

#### 3.1.2. SNMPv1 -> SNMPv2

When converting responses received from a SNMPv1 entity acting in an agent role into responses sent to a SNMPv2 entity acting in a manager role:

(1) ...

(2) If a Trap-PDU is received, then it is mapped into a SNMPv2-Trap-PDU. This is done by prepending onto the variable-bindings field two new bindings: `sysUpTime.0` [6], which takes its value from the timestamp field of the Trap-PDU; and, `snmpTrapOID.0` [6], which is calculated as follows: if the value of `generic-trap` field is `enterpriseSpecific`, then the value used is the concatenation of the `enterprise` field from the Trap-PDU with two additional sub- identifiers, '0', and the value of the `specific-trap` field; otherwise, the value of the corresponding trap defined in [6] is used. (For example, if the value of the `generic-trap` field is `coldStart`, then the application uses the `coldStart` trap [6]) Then, one new binding is appended onto the variable-bindings field: `snmpTrapEnterprise.0` [6], which takes its value from the `enterprise` field of the Trap-PDU. The destinations for the SNMPv2-Trap-PDU are determined in an implementation-dependent fashion by the proxy agent.

Despite this description, many vendors defined a trap for SNMPv2 and then had to support sending as SNMPv1 protocol. The assembly of v2 OID from v1 enterprise and specific is supposed to include an extra '0'; `enterpriseOID.0.specific`. However, if a v2 trap is defined that has no '0' in it, so it cannot be sent as v1 and converted back following the specifications

### Send as Proxy

This application can forward a trap as though it came from device (sourceIP spoofing) or act as an agent proxy according to the SNMP-COMMUNITY-MIB.

If not sending as proxy, we forward trap from application server cluster as an SNMPv2 notification as though it is coming directly from the originating agent (device). This is a common and desired behavior. Some operating systems prevent packet spoofing as a security measure so this behavior is necessarily optional.

If sending as proxy, the trap is forwarded from application server using the application server IP as sourceIP. The relevant snippet from SNMP-COMMUNITY-MIB is the following:

```
--
-- The snmpTrapAddress and snmpTrapCommunity objects are included
-- in notifications that are forwarded by a proxy, which were
-- originally received as SNMPv1 Trap messages.
--

snmpTrapAddress OBJECT-TYPE
    SYNTAX  IpAddress
    MAX-ACCESS accessible-for-notify
    STATUS  current
    DESCRIPTION
        "The value of the agent-addr field of a Trap PDU which
        is forwarded by a proxy forwarder application using
        an SNMP version other than SNMPv1. The value of this
        object SHOULD contain the value of the agent-addr field
        from the original Trap PDU as generated by an SNMPv1
        agent."
-- 1.3.6.1.6.3.18.1.3 -- ::= { snmpCommunityMIBObjects 3 }

snmpTrapCommunity OBJECT-TYPE
    SYNTAX  OCTET STRING
    MAX-ACCESS accessible-for-notify
    STATUS  current
    DESCRIPTION
        "The value of the community string field of an SNMPv1
        message containing a Trap PDU which is forwarded by a
        proxy forwarder application using an SNMP version
        other than SNMPv1. The value of this object SHOULD
        contain the value of the community string field from
        the original SNMPv1 message containing a Trap PDU as
        generated by an SNMPv1 agent."
-- 1.3.6.1.6.3.18.1.4 -- ::= { snmpCommunityMIBObjects 4 }
```

Dell OpenManage Network Manager always adds `snmpTrapAddress` to every trap forwarded as proxy, (never adding `snmpTrapCommunity`). It does not keep track of the community string on the traps received.

## Email

Email actions configure destinations and messages for e-mail and SMS recipients. You can include fields that are part of the event by using the variables described in Email Action Variables on page 122.

The screenshot shows the 'Adding New Email Action' dialog box. The 'Description' field contains 'TestEmail'. The 'Notify Associated Contact' checkbox is unchecked. The 'Email' tab is selected, and the 'Configure Email' section is visible. The 'Recipients' list contains 'test@test.com'. The 'Subject' field contains 'This is a test', the 'Email Header' contains 'Testing 1, 2, 3', and the 'Email Footer' contains 'Bye!'. At the bottom, there is an information icon and a note: 'Did you know that variables from the event can be substituted into the Subject, Header or Footer using {}. For example: {Name} event with severity {Severity} was received at {RecvTime}. Refer to help for a complete list of available variables.' Below this note are 'Apply' and 'Cancel' buttons.

Notice that below the Description of the e-mail action, you can check to send this mail (and/or SMS) to associated Contacts, if any are available, even if you specify no mail address destination. The SMS tab is similar to the e-mail tab, but limits the number of characters you can enter with a field at its bottom.



The SMS tab is similar to the e-mail tab, but limits the number of characters you can enter with a field at its bottom.

 **NOTE:**

You must send SMS to the destination phone carrier's e-mail-to-SMS address. For example sending text to 916-555-1212 when Verizon is the carrier means the destination address is 9165551212@vtext.com.

When enabled, notification emails go to the Contact associated with the Managed Equipment for the notification event. For the contact's email address, mail goes to the first specified address from either the Work Email, Home Email or Other Email fields in the Contact editor. SMS messages go to the Pager Email field for the contact. If a Contact was not found or the required addresses are not specified for the Contact, then Dell OpenManage Network Manager uses the Recipient addresses configured in the the Email Action.

This screen has the following fields:

**Recipient Addresses**—Enter an e-mail address in the field below this label, then click the plus (+) sign to add it to the list of recipients. The minus (-) removes selected recipients.

**Subject**—The e-mail subject.

**Email Header / Footer**—The e-mail's heading and footing.

**SMS Body**—The e-mail contents to be sent as text.

**SMS Max Length**—The maximum number of characters to send in the SMS. Typically this is 140, but the default is 0, so be sure to set to your carrier's maximum before saving.

Here is what Email looks like when it arrives:

```
Sent: Wednesday, March 02, 2011 2:37 PM
To: techpubs@oradosoftware.com
Subject: Web Test
Notification: redcellInventoryAttribChangeNotification
Notification Attributes:
=====
sysUpTime.0                = 5 hours, 16 mins, 43 secs
snmpTrapOID.0              = 1.3.6.1.4.1.3477.2.2.1
redcellInventoryAttrName.0 = RedCell.Config.EquipmentManager_Notes
redcellInventoryAttrChangedBy.0 = admin
redcellInventoryAttrNewValue.0 = hello
world
severity
auto
redcellInventoryAttrOldValue.0 = hello
world
```

severity

## Custom

This screen lets you configure *Action* based on Adaptive CLI actions available in the system. Notice that you can select by *most common* or by *keyword search*, depending on which of the links in the upper right corner of the screen is selected.

The screenshot shows a configuration window titled "Select an Action to add to the Rule". The "Action" dropdown is set to "Juniper MPLS L2 ELAN LDP VPLS Backup Neig". The "Target" dropdown is empty. Below the "Target" field, there are several input fields: "VPLS Name" (testVPLS), "Remote Neighbor IP" (10.10.20.10), "Backup Neighbor IP" (10.10.20.11), "PSN Tunnel Endpoint" (highlighted in yellow), "Community Name", "Community Target", and "Standby" (checkbox). A tooltip for the "PSN Tunnel Endpoint" field reads: "Packet Switched Network (PSN) endpoint of the transport tunnel on the remote PE". At the bottom, there are "Apply" and "Cancel" buttons. To the right, a partial view of a table with columns "Enabled" and "System" is visible.

The *most common* actions include those you have used most recently. To search for actions, either enter a keyword, or click the search icon (the magnifying glass) to produce a pick list below the *Action* field. Select an action by clicking on its appearance in that list.

Select the device target of the custom action by selecting from the *Target* pick list. If you do not specify an explicit target, Dell OpenManage Network Manager uses the default entity for the event as the target.

If you select an action with additional parameters, those parameters appear in the screen below the *Target* field. To see definitions for such parameters, hover the cursor over the field and a tooltip describing the field appears.

Click *Apply* to accept your edits, or *Cancel* to abandon them.

## Email Action Variables

The following are the Email Action variables you can use in customizing the content of action e-mail. These appear classified as follows:

- Basic Variables
- Managed Equipment Variables

- Entity Type: Port
- Entity Type: Interface, Logical interface



**CAUTION:**

To successfully retrieve Custom attributes, you must first create them. See Edit Custom Attributes on page 89.

You can also configure more limited variables that are slightly more efficient in performance, if not as detailed as those described in the following section.

For example, you can retrieve the following attributes:

```
{RedCell.Config.EquipmentManager_Custom1}
{RedCell.Config.EquipmentManager_Custom2}
{RedCell.Config.EquipmentManager_LastBackup}
{RedCell.Config.EquipmentManager_LastConfigChange} and
{RedCell.Config.EquipmentManager_HealthStatus}
```



**NOTE:**

If the entity does not contain/return these values, then the message [No data for <attribute name>] appears in the email instead.

**Basic Variables**

Attribute	Description	Email Action Variable
Name	The event / alarm name	{Name}
Message	Description from the event	{Message}
Entity Name	The entity (interface, card...) name	{EntityName}
Equipment Manager Name	The name of the equipment, parent or chassis.	{EquipMgrName}
Device IP address	the IP of the device in alarm	{DeviceIP}
Entity Type	Type of entity (Router, and so on)	{EntityType}
Instance ID	An identifier for the event	{InstanceID}
Protocol Type	Of originating alarm (SNMP, syslog, etc.)	{ProtocolType}
Protocol Sub Type	Inform, Trap, [blank] (for internal events)	{ProtocolSubType}
Receive Time		{RecvTime}
Region	The mediation server partition name.	{Region}
Severity	0 - cleared, through 6 - critical, from Alarm Definition	{Severity}
Source IP address	The IP of the component sending the alarm	{SourceIP}

The following section describes variables whose use may have a performance impact.

### Managed Equipment Variables

Attribute	Description	Email Action Variable
Custom 1	Note that although you can re-name any Custom attribute, you must use the variable's original name. For example here, that is {RedCell.Config.Equipm entManager_Custom1}	{RedCell.Config.EquipmentManager_Cu stom1}
Custom 2		{RedCell.Config.EquipmentManager_Cu stom2}
Custom 3		{RedCell.Config.EquipmentManager_Cu stom3}
Custom 4		{RedCell.Config.EquipmentManager_Cu stom4}
Custom 5		{RedCell.Config.EquipmentManager_Cu stom5}
Custom 6		{RedCell.Config.EquipmentManager_Cu stom6}
Custom 7		{RedCell.Config.EquipmentManager_Cu stom7}
Custom 8		{RedCell.Config.EquipmentManager_Cu stom8}
Custom 9		{RedCell.Config.EquipmentManager_Cu stom9}
Custom 10		{RedCell.Config.EquipmentManager_Cu stom10}
Custom 11		{RedCell.Config.EquipmentManager_Cu stom11}
Custom 12		{RedCell.Config.EquipmentManager_Cu stom12}
Custom 13		{RedCell.Config.EquipmentManager_Cu stom13}
Description	Description of the equipment	{RedCell.Config.EquipmentManager_De viceDescription}
DNS Hostname	Hostname of equipment	{RedCell.Config.EquipmentManager_Ho stname}

Attribute	Description	Email Action Variable
Equipment Type	Equipment Type	{RedCell.Config.EquipmentManager_CommonType}
Firmware Version	Version of the equipment's firmware	{RedCell.Config.EquipmentManager_FirmwareVersion}
Hardware Version	Version of the equipment's hardware	{RedCell.Config.EquipmentManager_HardwareVersion}
Last Backup	Last Backup	{RedCell.Config.EquipmentManager_LastBackup}
Last Configuration Change	Last Configuration Change	{RedCell.Config.EquipmentManager_LastConfigChange}
Last Modified	Timestamp of Last Modified	{RedCell.Config.EquipmentManager_LastModified}
Model	Model number of the equipment	{RedCell.Config.EquipmentManager_Model}
Name	Component name	{RedCell.Config.EquipmentManager_Name}
Network Status	Network Status	{RedCell.Config.EquipmentManager_HealthStatus}
Notes	Equipment Notes	{RedCell.Config.EquipmentManager_Notes}
OSVersion	OSVersion	{RedCell.Config.EquipmentManager_OSVersion}
Serial Number	Unique identifier for the equipment	{RedCell.Config.EquipmentManager_SerialNumber}
Software Version	Version of the equipment's software	{RedCell.Config.EquipmentManager_SoftwareVersion}
System Object Id	SNMP based system object identifier	{RedCell.Config.EquipmentManager_SystemObjectID}

### Entity Type: Port

Attribute	Description	Email Action Variable
Custom 1	Note that although you can re-name any Custom attribute, you must use the variable's original name. For example here, that is {RedCell.Config.EquipmentManager_Custom1}	{RedCell.Config.Port_Custom1}
Custom 2		{RedCell.Config.Port_Custom2}
Custom 3		{RedCell.Config.Port_Custom3}

<b>Attribute</b>	<b>Description</b>	<b>Email Action Variable</b>
Custom 4		{RedCell.Config.Port_Custom4}
Encapsulation	Encapsulation	{RedCell.Config.Port_Encapsulation}
Hardware Version	Version of the port's hardware	{RedCell.Config.Port_HardwareVersion}
If Index	SNMP If Index	{RedCell.Config.Port_IfIndex}
MAC Address	“Typically a MAC Address, with the octets separated by a space, colon or dash depending upon the device. Note that the separator is relative when used as part of a query.”	{RedCell.Config.Port_UniqueAddress}
Model	Model number of the port	{RedCell.Config.Port_Model}
MTU	Maximum Transmission Unit	{RedCell.Config.Port_Mtu}
Name	Port name	{RedCell.Config.Port_Name}
Notes	Port Notes	{RedCell.Config.Port_Notes}
Port Description	Description of the port	{RedCell.Config.Port_DeviceDescription}
Port Number	Port Number	{RedCell.Config.Port_PortNumber}
Slot Number	Slot Number	{RedCell.Config.Port_SlotNumber}
Speed	Speed	{RedCell.Config.Port_Speed}
Subnet Mask	SubMask	{RedCell.Config.Port_SubMask}

## Entity Type: Interface, Logical interface

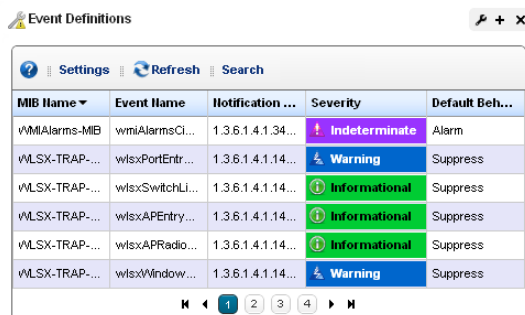
Attribute	Description	Redcell Email Action variable
Custom 1	Note that although you can re-name any Custom attribute, you must use the variable's original name. For example here, that is {RedCell.Config.EquipmentManager_Custom1}	{RedCell.Config.Interface_Custom1}
Custom 2		{RedCell.Config.Interface_Custom2}
Custom 3		{RedCell.Config.Interface_Custom3}
Custom 4		{RedCell.Config.Interface_Custom4}
Encapsulation	Encapsulation	{RedCell.Config.Interface_Encapsulation}
IfIndex	SNMP Interface Index	{RedCell.Config.Interface>IfIndex}
Interface Description	Description of the Interface	{RedCell.Config.Interface_DeviceDescription}
Interface Number	Interface Number	{RedCell.Config.Interface_InterfaceNumber}
Interface Type	Common Interface Type	{RedCell.Config.Interface_CommonType}
MTU	Maximum Transmission Unit	{RedCell.Config.Interface_Mtu}
Name	Interface name	{RedCell.Config.Interface_Name}
Notes	Interface Notes	{RedCell.Config.Interface_Notes}
Port Number	Port Number	{RedCell.Config.Interface_PortNumber}
Slot Number	Slot Number	{RedCell.Config.Interface_SlotNumber}
Subnet Mask	Subnet Mask of the Interface	{RedCell.Config.Interface_SubMask}

Best practice is to clarify such attributes by combining them with others that spell out their source.

# Event Definitions

You can define how the system treats messages (events) coming into the system. Administrators can define event behavior deciding whether it is suppressed, rejected or generates an Alarm. Manage the definitions of events in this portlet.

In this screen, you can configure events that, when correlated as described in Event Processing Rules on page 108, trigger actions.



MIB Name	Event Name	Notification ...	Severity	Default Beh...
vMIBAlarms-MIB	wmiAlarmsCl...	1.3.6.1.4.1.34...	Indeterminate	Alarm
WLSX-TRAP-...	wlsxPortEntr...	1.3.6.1.4.1.14...	Warning	Suppress
WLSX-TRAP-...	wlsxSwitchLi...	1.3.6.1.4.1.14...	Informational	Suppress
WLSX-TRAP-...	wlsxAPEntry...	1.3.6.1.4.1.14...	Informational	Suppress
WLSX-TRAP-...	wlsxAPRadio...	1.3.6.1.4.1.14...	Informational	Suppress
WLSX-TRAP-...	wlsxWindow...	1.3.6.1.4.1.14...	Warning	Suppress

Columns include the *MIB Name*, *Event Name*, *Notification OID*, *Severity* for associated alarms, and *Default Behavior*. See Event Definition Editor for how to alter these. Right-click a selected event definition for the following menu items:

**Edit**—Either open the selected event in Event Definition Editor, or open a details panel for the underlying equipment.

**Set Behavior**—This lets you select from the following options.

*Reject*—Every received message is rejected.

*Suppress*—The message is tracked in Event History and then ignored.

*Alarm*—The message is tracked in Event History and then processed, with Correlated events and Event Processing Rules of any type other than Syslog.

**Set Severity**—Set the alarm severity for the selected event.

**MIB**—This lets you upload a new MIB to your event definitions.

You can also configure an Aging Policy and View events as PDF in this menu. See Redcell > Database Aging Policies (DAP) on page 50, and View as PDF on page 90 for more about those options.

## Event Definition Editor

This editor lets you modify event definitions in the following tabs:

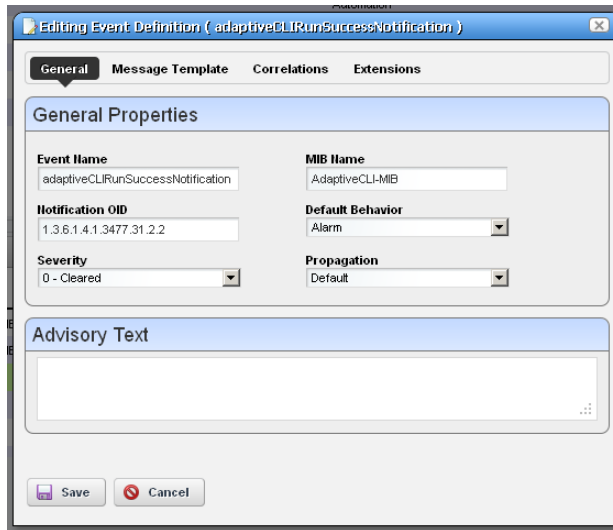
- General
- Message Template
- Correlations

Click *Save* to preserve any modifications you have made, or *Cancel* to abandon them.



## General

This tab manages basics for Event Definitions.



The screenshot shows a dialog box titled "Editing Event Definition ( adaptiveCLIRunSuccessNotification )". It has four tabs: "General", "Message Template", "Correlations", and "Extensions". The "General" tab is active and contains the following fields:

- Event Name:** adaptiveCLIRunSuccessNotification
- Notification OID:** 1.3.6.1.4.1.3477.31.2.2
- Severity:** 0 - Cleared
- MIB Name:** AdaptiveCL-MIB
- Default Behavior:** Alarm
- Propagation:** Default

Below these fields is an "Advisory Text" section with a large text area. At the bottom of the dialog are "Save" and "Cancel" buttons.

It has the following fields:

**Event Name**—A text identifier for the event.

**Notification OID**—The object ID.

**Severity**—The severity of any associated alarm. If a new alarm is a clearing severity, then it closes any existing alarm to which it correlates. Otherwise, if a new alarm severity does not match the existing severity then the existing alarm is closed and a new alarm opened for the new severity.

**MIB Name**—The MIB with which this event is associated.

**Default Behavior**—The options for behavior (*Undefined, Alarm, Suppress, Reject*). *Alarm* means: Process at the mediation server, generate event history and an alarm. *Suppress* means: Process at the mediation server and generate an event (*not* an alarm). *Reject* means: Reject at the mediation server (do not process)

**Propagation**—The propagation behavior for the event (*Default, Impacts subcomponents, Impacts top level, Not service effecting*).

Only service effecting alarms are propagated. By default, events are service-effecting, provided their severity is indeterminate or above. Select the propagation type from the pick list.

An event definition configures “Impact Propagation” (distinct from “Alarm propagation”) based on the event type. Does the event impact the overall device (*Impacts top level*), subcomponents (*Impacts subcomponents*), or just the correlated inventory entity (*Default*)?

*Not Service Effecting* means that alarm propagation ignores alarms for this event. In other words, no impact to associated entities occurs. This also means alarms created for this event type appear as *Not Service Effecting* in the alarm manager—handy to help clean up noisy alarm views since you can filter to conceal these.

Propagation policies configure “Alarm Propagation”—associations based propagation paths to generate calculated alarm states against associated entities like links and services. See Event Processing Rules on page 108 for more about configuring these.

For example, link propagation works like this: If one or both associated endpoints have an impacting alarm, then OpenManage Network Manager generates a calculated alarm for the corresponding link at the highest severity of either endpoint. If both endpoints are clear then the resulting, calculated event is clear. This means alarm correlation removes any existing calculated alarm against the link.

If you upgrade Dell OpenManage Network Manager, all alarms migrated to from previous versions appear as service-effecting, regardless of severity. To alter multiple events’ impact propagation, export the event definitions, and alter the XML export to reflect the kind of propagation desired for events.

Search for the paired `<ImpactPropagation>0</ImpactPropagation>` tags, and alter the numbers within them as follows:

*Default*—0

*Impacts Top Level*—1

*Impacts Subcomponents*—2

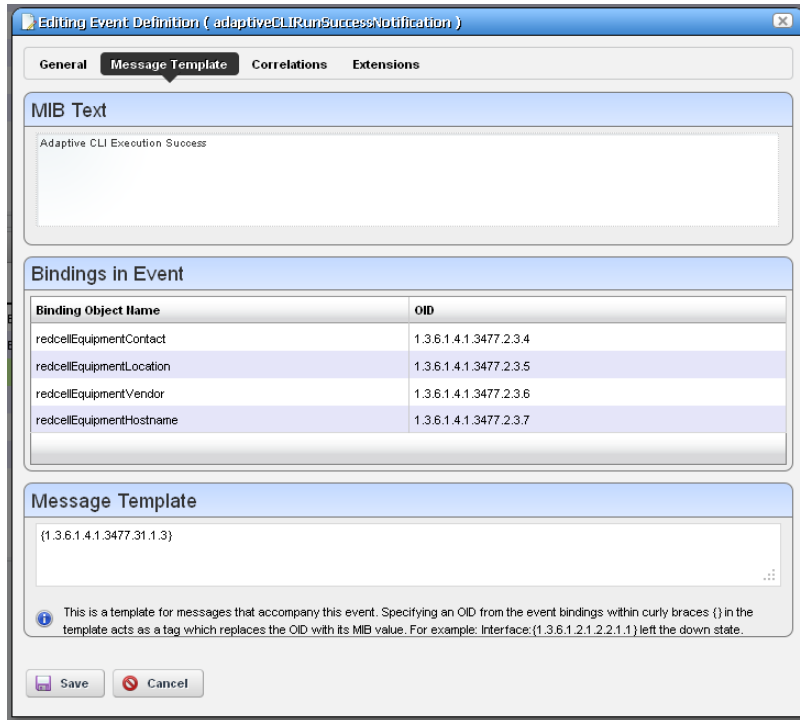
*Not service effecting*—4

Re-import the altered event definition file to update your event definitions.

**Advisory Text**—The *Advisory Text* appears with the event. Configure it in the text box here.

## Message Template

This panel lets you view or alter MIB Text, Bindings and the Message Template for the event selected.



This contains three sections:

**MIB Text**—A read-only reminder of the MIB contents for this OID.

**Bindings in Event**—A read-only reminder of the MIB bindings for this event. This displays the varbind contents of the event, matching the *Binding Object Name* and the *OID* (object identifier).

**Message Template**—A template for messages that accompany this event. Specifying an OID within the curly braces {} in the template acts as a tag which replaces the OID with its MIB value. For example: Interface: {1.3.6.1.2.1.2.2.1.1} left the down state.

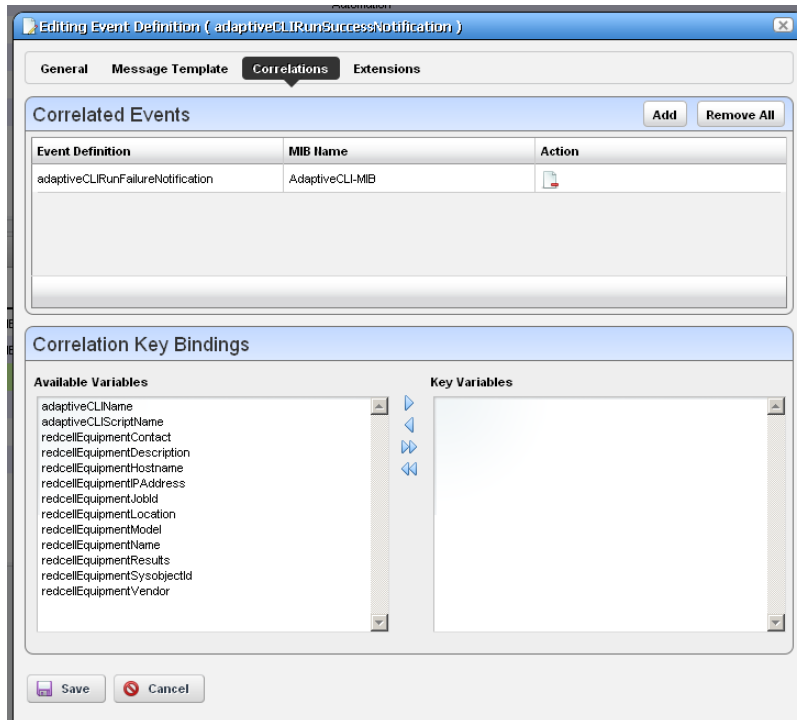
If a message template exists for an existing, correlated alarm and the generated text does not match the original alarm, then Dell OpenManage Network Manager closes the existing alarm, and generates a new one. Leaving this blank transmits the original message.

 **Tip**

Putting an OID in curly brackets amounts to a tag replaced by the MIB text for that OID. Look for OIDs and messages in the MIB browser (as described in MIB Browser on page 188).

## Correlations

This screen lets you configure Correlated Events and Correlation Key Bindings. For example, a link down event could correlate with a link up event, or an alarm with a clear alarm event.



In the Correlated Events panel, click *Add* to display a selector (with filter) to find events to correlate with the one you are editing.

In Correlation Key Bindings, use the right/left arrows to select *Key Variables* from *Available Variables*. The variables considered keys for correlation are the key bindings for the target alarm in the correlation process. This means that if event A is defined to include event B as a correlated event, comparison of the key bindings defined for event B is also considered when comparing a new alarm for event A to an existing alarm for event B.

# Contacts

The contact portlet displays available contacts for your system. There is no expanded version of this portlet.

You can right-click to act on the the selected contact with the following menu items.

**New / Open**—Displays the Contacts Editor, where you can create new contacts or alter existing ones.

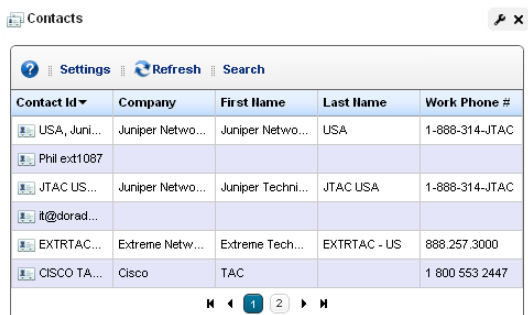
**Details**—Displays a screen with contact-associated alarms, and the information entered in Contacts Editor.

**Visualize**—Displays a mapping of the selected contact’s association to devices. See Chapter 5, Visualize My Network.

**Delete**—Displays a mapping of the selected contact’s association to devices.

**Visualize**—Displays a mapping of the selected contact’s association to devices.

Dell OpenManage Network Manager only retrieves Contact and Location information on initial discovery. You can modify these once the resource is under management. However doing will not modify the any system information on the device.



The screenshot shows a web interface titled "Contacts" with a search bar and a table of contact data. The table has columns for Contact Id, Company, First Name, Last Name, and Work Phone #. There are 6 rows of data, with the first row selected. Below the table is a pagination control showing page 1 of 2.

Contact Id	Company	First Name	Last Name	Work Phone #
USA, Juni...	Juniper Netwo...	Juniper Netwo...	USA	1-888-314-JTAC
Phil ext1 087				
JTAC US...	Juniper Netwo...	Juniper Techni...	JTAC USA	1-888-314-JTAC
it@dorad...				
EXTRTAC...	Extreme Netw...	Extreme Tech...	EXTRTAC - US	888.257.3000
CISCO TA...	Cisco	TAC		1 800 553 2447

## Contacts Editor

This editor has two panels where you can enter contact information (*Name*, *Address*, *Phone*, and so on). Click the tabs at the top of this screen to move between the panels. The *Contact ID*, a unique identifier for the contact in your system, is a required field at the top of the first page.

Click *Save* to preserve your new or modified contact information. Click *Cancel* to leave the contact unmodified.

The image displays two overlapping windows from a software application. The foreground window, titled "Editing Contact ( Silk Contact 608 )", has two tabs: "General" and "Additional Information". The "Additional Information" tab is selected and shows two main sections: "Home Information" and "Other Information".

**Home Information:**

- Home Phone:
- Home Email:
- Home Fax:
- Personal Cell:
- Personal Pager:

**Other Information:**

- Other Phone:
- Other Email:
- Other Pager:
- Other Fax:
- Other Cell:
- Pager Email:

At the bottom of the foreground window are "Save" and "Cancel" buttons. The background window, also titled "Editing Contact ( Silk Contact 608 )", shows the "General" tab with fields for "Contact ID", "Company", "First Name", "Middle Name", "Last Name", "Address", and "City, State". It also has "Save" and "Cancel" buttons at the bottom.

# Locations

In its summary form, the locations portlet displays configured locations in your system.

You can right-click to create, modify or remove (*New*, *Open*, *Delete*) the selected location. See Location Editor description below for more about editing or creating locations.

If you select *Visualize*, a map of the selected location's connection to equipment appears. See Chapter 5, *Visualize My Network* for more.

The *Update Coordinates* option lets you revise a location's longitude and latitude. See *Tag* on page 138 for more.

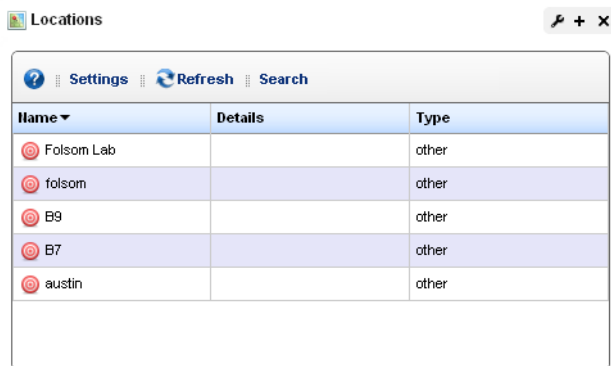
This screen has the following columns:






**[Icon]**—The icon for this location.

**Name**—The name for this location.

**Details**—A description for this location.

**Type**—A designated type for the location.

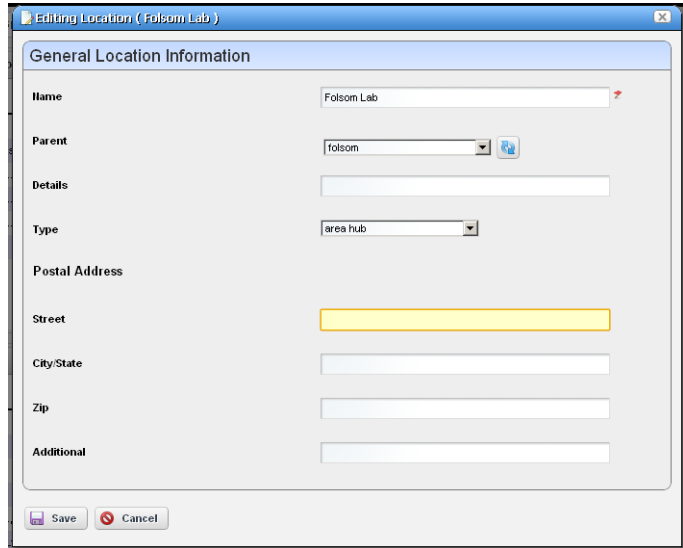


Name ▼	Details	Type
 Folsom Lab		other
 folsom		other
 B9		other
 B7		other
 austin		other

## Location Editor

When you click *New* or *Open*, an editor appears. The *Name* field is mandatory.

**Name**—A unique name for the Location. If you alter the name of an existing location already in use by existing equipment, the editor creates a new location. To change a location name, you must delete the original location and the equipment using it then re-make it. You can change the name of an unused location without deleting anything.



**Parent**—The “parent” of this location (the location to which this location is subordinate). Select a Parent Location from the pick list. The maximum number of levels supported is 15.

**Details**—A text description of the location.

**Type**—Type of location, as selected from the drop-down menu. Available types are: Area Hub, Customer, National Hub, Other, Provider, Regional Hub, and State.

**Postal Address**—The *Street*, *City/State*, *Zip* address of the location.

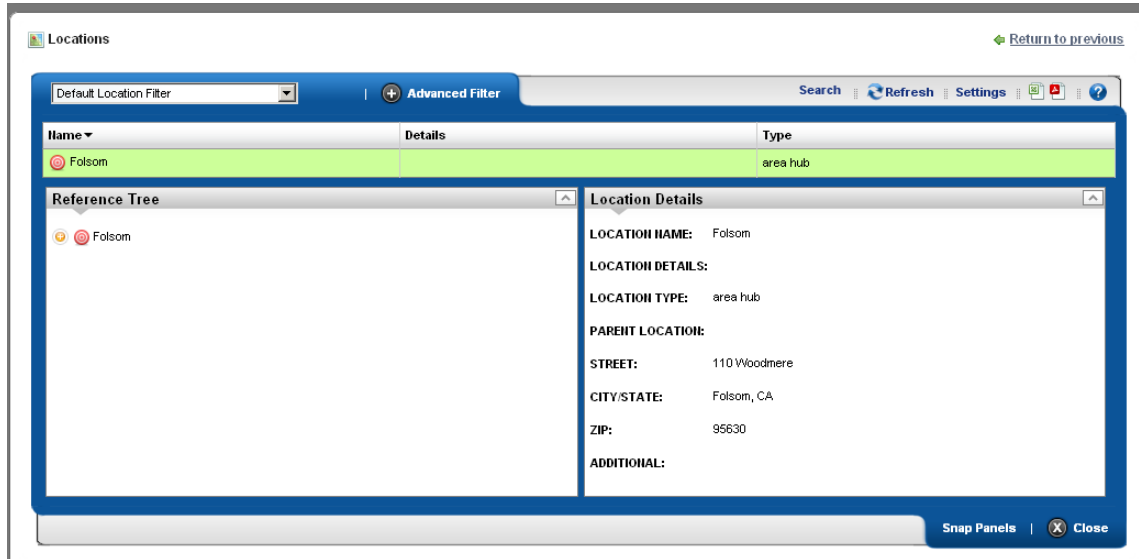
**Additional**—Any optional notes.

Click *Save* to save the Location, or any modifications you have made.



## Expanded Location Portlet

The location portlet displays a list of all locations, with Snap Panels to display a selected location's connection to the network and details.



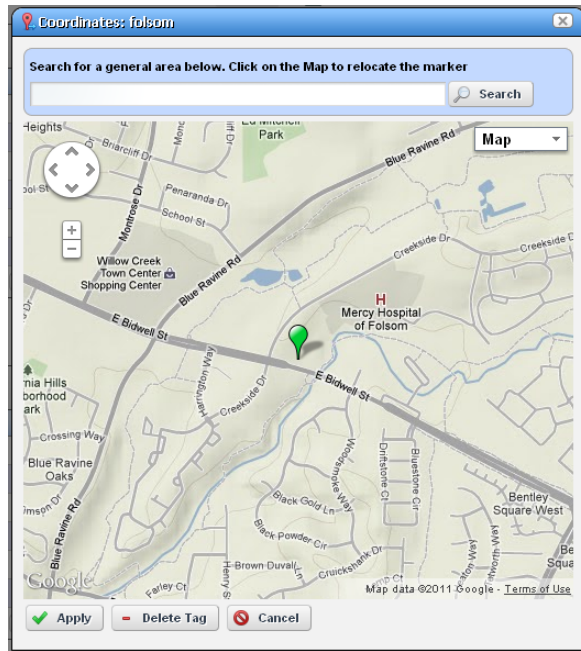
The *New* menu option appears in the expanded location portlet. Click *Settings* to change the column appearance (see *Show / Hide / Reorder Columns* on page 84). This has the same columns as *Locations* on page 135.

## Locations Snap Panels

Selecting a location row displays the *Reference Tree* Snap Panel, with that location's connection to containers (see *Container View* on page 147) and equipment. Click the plus (+) icons to expand the tree. The *Location Details* panel displays what has been configured in the *Location Editor*.

## Tag

When creating a location, Dell OpenManage Network Manager automatically selects the latitude and longitude of the address entered for a location. To update or make these more accurate, select *Update Location* by right-clicking a location in the Locations portlet.



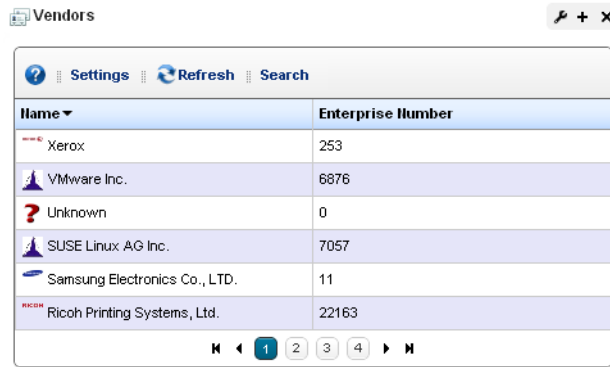
The location created by default is the address entered in the Locations editor. You can also enter the address in the Search field, or click and drag the marker that appears on this screen. Click *Apply* to accept the re-location. A *Delete Tag* button appears when you have created a tag, and lets you remove it. *Cancel* closes the screen.

### Tip

You can zoom in or out on the displayed map with the + and - buttons in the upper left corner of this screen.

# Vendors

In its summary form, this portlet displays the available vendors for network resources.



The screenshot shows a web interface titled "Vendors" with a search bar and a table of vendor data. The table has two columns: "Name" and "Enterprise Number". The rows are as follows:

Name	Enterprise Number
Xerox	253
VMware Inc.	6876
Unknown	0
SUSE Linux AG Inc.	7057
Samsung Electronics Co., LTD.	11
Ricoh Printing Systems, Ltd.	22163

Right-clicking a row lets you do the following:

**New / Edit**—Opens the Vendor Editor where you can configure or re-configure a vendor.

**Details**—Displays a panel showing the alarms, registered models, and identifiers for the selected vendor.

**Visualize**—See a topology of the network filtered to display only the selected vendor, see Chapter 5, Visualize My Network

**Import / Export**—Common menu capabilities described in *Import / Export on page 86*.

This screen has the following columns:

**Vendor Icon**—The icon for this vendor.

**Enterprise Number**—The enterprise number for this vendor.

**Vendor Name**—The name for this vendor.

## Vendor Editor

This editor configures (or re-configures) vendors. It has the following fields:

### General

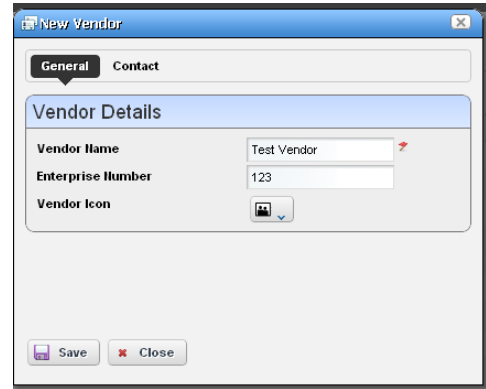
**Vendor Name**—A text identifier for the vendor.

**Enterprise** —A numeric identifier for the vendor.

**Vendor Icon**—Select an icon from the pick list.

### Contact

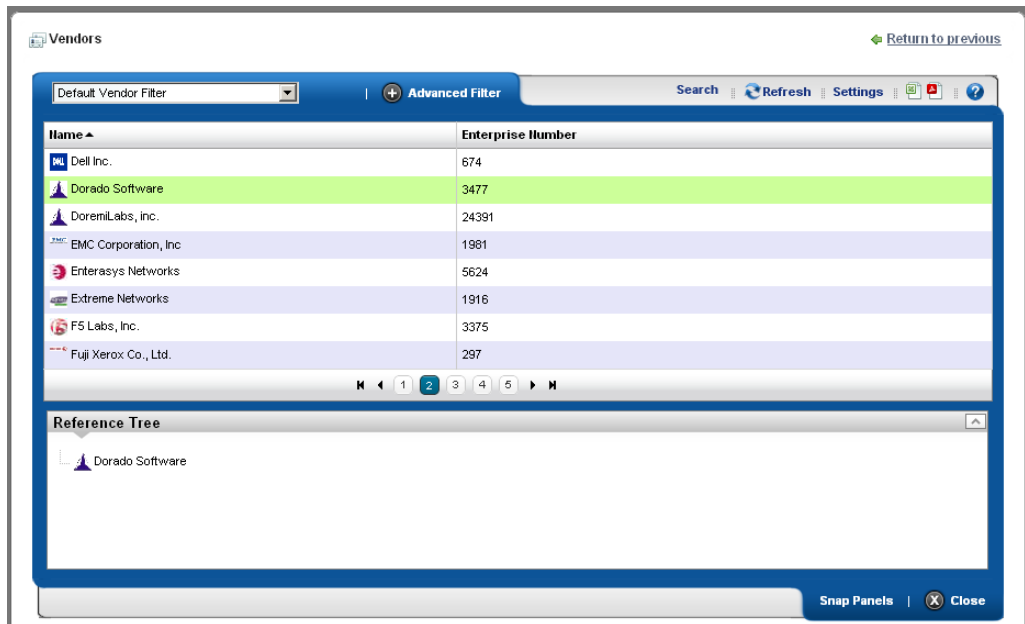
Click the *Add* button to select from contacts in Dell OpenManage Network Manager to associate with this vendor. See *Contacts on page 133* for instructions about configuring contacts.



The screenshot shows a 'New Vendor' dialog box with two tabs: 'General' and 'Contact'. The 'General' tab is selected. Under the heading 'Vendor Details', there are three fields: 'Vendor Name' with the value 'Test Vendor', 'Enterprise Number' with the value '123', and 'Vendor Icon' which is a pick list showing a small icon. At the bottom of the dialog, there are 'Save' and 'Close' buttons.

## Expanded Vendor Portlet

When you expand the Vendor portlet, besides sharing you you can also click *Settings* to configure the columns that appear here (see *Show / Hide / Reorder Columns on page 84*). This screen has the same columns available as the summary screen.



The screenshot shows the 'Vendors' portlet interface. At the top, there is a 'Default Vendor Filter' dropdown and an 'Advanced Filter' button. To the right are 'Search', 'Refresh', and 'Settings' buttons. Below this is a table with two columns: 'Name' and 'Enterprise Number'. The table contains the following data:

Name	Enterprise Number
Dell Inc.	674
Dorado Software	3477
Doremilabs, inc.	24391
EMC Corporation, Inc.	1981
Enterasys Networks	5624
Extreme Networks	1916
F5 Labs, Inc.	3375
Fuji Xerox Co., Ltd.	297

Below the table is a 'Reference Tree' section showing a tree view with 'Dorado Software' selected. At the bottom right of the portlet, there are 'Snap Panels' and 'Close' buttons.

### **Vendors Snap Panel**

The snap panel displays the icon for the selected vendor.



## Resource Management

The Resource management portlets let you manage devices you have discovered or created on your network.

Resource Management portlets let you view device-specific information, both general (name, type, location, contact) and technical (vendor, subcomponents, and so on).

This chapter contains information about the following portlets:

- Authentication
- Container Manager
- Container View
- Discovery Profiles
- Managed Resources
- Ports
- Reports

## Authentication

The authentication summary screen displays credentials used to communicate with and manage devices.

Name	Designated for EMS	Type
XXX	✓	EMC
testipmi	✗	IPMI
test3	✓	EMC
test	✓	Telnet/SSH
TELNET_Altiris Demo	✗	Telnet/SSH
Telnet-Cisco MDS	✓	Telnet/SSH

This portlet displays credentials used in discovery and communication with network resources. The *Name* column identifies the set of credentials, *Designated for EMS* means it is available for all users, and *Type* indicates the protocol for that authentication.

Functions common to many menus, in addition to the Import / Export and Sharing, include the following actions are available in the right-click menu:

**New / Edit**—Opens Authentication Editor, where you can create a new authentication or edit the selected authentication. You cannot change the Authentication Type when you edit an existing authentication.

**Details**—Displays a reference tree, associated equipment, and the configuration created or altered in Authentication Editor.

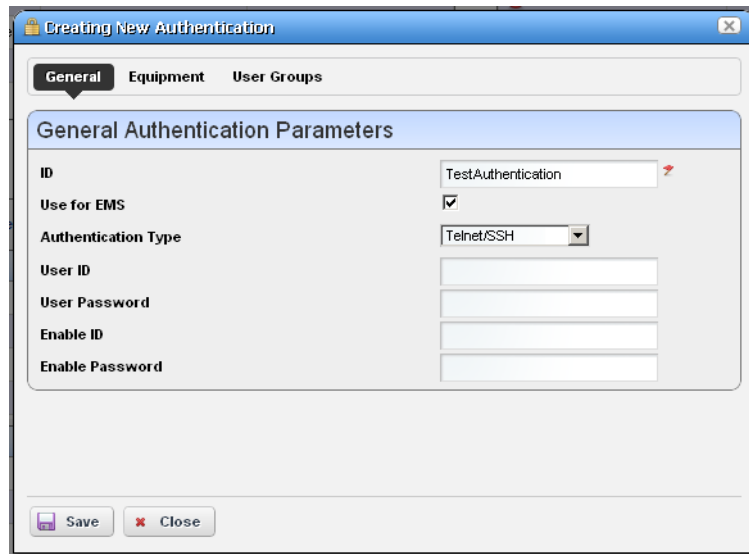
**Audit**—Opens an audit trail viewer for the selected authentication.

**Delete**—Deletes the selected authentication. If it is in use, an error message appears saying that deletion is not allowed.

**Import / Export**—Imports or exports authentications to your Dell OpenManage Network Manager system.

### Authentication Editor

You can right-click and select *New* or *Open* to create or modify credentials for your system. You can also *Delete* and *Share with User* from that right-click menu.



The screenshot shows a window titled "Creating New Authentication" with three tabs: "General", "Equipment", and "User Groups". The "General" tab is selected, displaying "General Authentication Parameters". The fields are as follows:

Field	Value
ID	TestAuthentication
Use for EMS	<input checked="" type="checkbox"/>
Authentication Type	Telnet/SSH
User ID	
User Password	
Enable ID	
Enable Password	

At the bottom of the dialog are "Save" and "Close" buttons.

The fields that appear in this editor vary, depending on the type of authentication. The *ID* (name) for the authentication is mandatory. If you *Add* an existing authentication, for example to Discovery Profiles, you can also configure the Management Interface Parameters like *Timeout*, *Retries*, and *Port* used. If you have an authentication that works for multiple protocols (for example SSH or Telnet), you can also select the *Protocol Type*.

Use the *Equipment* and *User Groups* tabs to associate the authentication you configure here to devices or groups of users.



## Expanded Authentication Portlet

The *Settings* button in the expanded Authentication portlet lets you configure column appearance (see Show / Hide / Reorder Columns on page 84). This offers the same column setup as the summary screen.

The screenshot displays the 'Authentication' portlet interface. At the top, there is a 'Default Authentication Filter' dropdown and an 'Advanced Filter' button. The main table lists authentication filters with columns for Name, Designated for EMS, and Type. The 'qapublic' filter is highlighted in green. Below the table, there are two panels: 'Reference Tree' and 'Associated Equipment'.

Name	Designated for EMS	Type
PowerVault	✓	POWERSVAULT
Printers	✓	HTTP/HTTPS/MBEM
Printers2	✓	HTTP/HTTPS/MBEM
Prod_auth	✓	Telnet/SSH
prod_SNMP	✓	SNMPv1/v2c
pubpriv	✓	SNMPv1/v2c
qapublic	✓	SNMPv1/v2c
qatester/dorado	✗	HTTP/HTTPS/MBEM

**Reference Tree**

- qapublic
  - Resource Profiles
  - This Authentication is associated with the following Equipment
    - JuniperJ2300-10.128.3.16.10.128.3.16
    - M5 JuniperM5-10.128.3.15.10.128.3.15

**Associated Equipment**

Name	IP Address	DNIS Hostname	Vendor
M5 JuniperM5-10.1...	10.128.3.15		Juniper Network...
J JuniperJ2300-1...	10.128.3.16		Juniper Network...

## Authentication Snap Panel

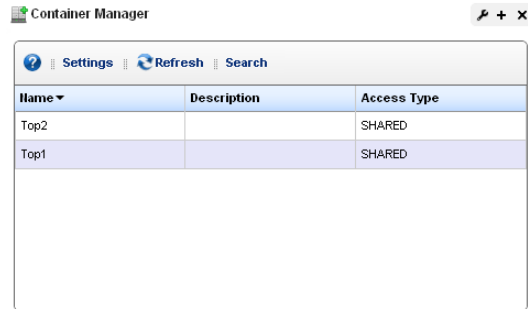
When you select a listed authentication the *Reference Tree* Snap Panel displays a tree of that authentication's connections to Discovery profiles and equipment.

# Container Manager

Container manager lets you create, edit and delete Container tree models displayed in Container Views (described in the next section).

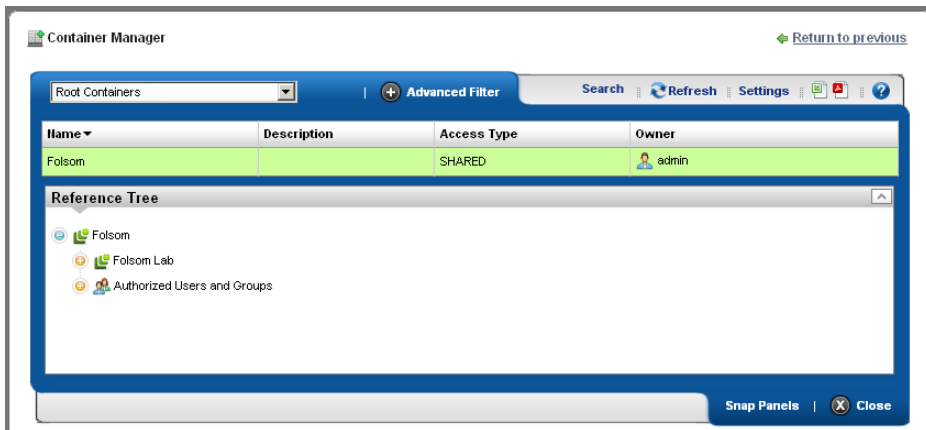
The relationship to users and devices appears in Container Manager Expanded.

Right-click to select from a menu with *New*, *Edit* and *Delete*, and *Refresh Members*. Selecting *New*, or *Edit* displays the Container Editor, described below.



## Container Manager Expanded

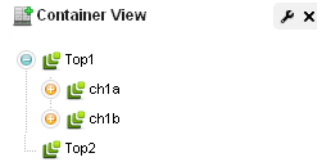
The expanded view displays the same information as the summary view, but displays the selected container's authorized users, creator, owner, and membership in the Reference Tree snap panel.



# Container View

This (non-instanceable) container portlet displays configured containers for Dell OpenManage Network Manager. Because it is non-instanceable, only one can appear on a page.

Expand the container tree by clicking the plus to each container's left. The container selected acts as a filter for a screen's other Dell OpenManage Network Manager portlets. If you select "Folsom" as a location in the container portlet, then only items related to Folsom devices appear in the other portlets on the page. If you select a parent container, that expands the selection to include all child containers' selections. It does not, however select everything. You can configure containers in Container Editor, described in the next section.



## NOTE:

You may have to wait a few moments to see a container's contents accurately.

Portlets that respond to Container or Map Context "filtering" include the following: Audit Trail, Event History, Locations, Vendors, Contacts, Managed Resources, Ports, Authentications, Discovery Profiles, Monitors, Services.

## Tip

If a container displays unexpected results, right-click it to refresh its membership or alarm state.

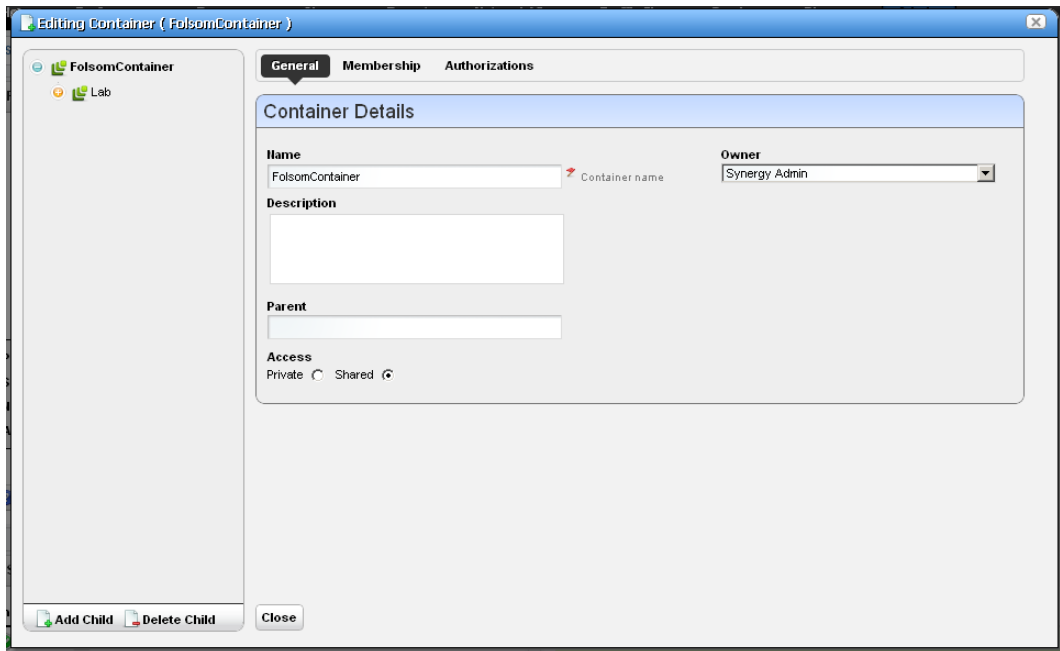
## How To:

### Use Containers

- 1 Create the containers you would like for filtering views of resources. For example, you can create a container for each customer or location.
- 2 Create a page with Managed Resources or other container-filtered portlets (Ports, Alarms and so on).
- 3 Add the Container View portlet to that page.
- 4 Click the container to filter by.
- 5 Observe the other portlets to see resources assigned to the selected container, for example, customer or location.

# Container Editor

This editor lets you create and manage containers. You can also associate user authorizations with container models to specify which groups or users have access to contained items.



In this editor, a tree panel on the left lets you build and navigate the container tree. Click *Add Child* (or *Delete Child*) to create (or remove) a node to / from the node you have selected in the tree. Clicking a node in the tree displays the tabbed panel on the right where you can edit it.

The *Container Details* panel has the following tabs:

- General
- Membership
- Authorizations

Click the labels at the top of the screen to access these.

 **NOTE:**

Alarm states are recalculated and propagated for containers like they are for Visualizations.

## General

This panel has the following fields:

**Name**—The container identifier.

**Description**—A text description of the container.

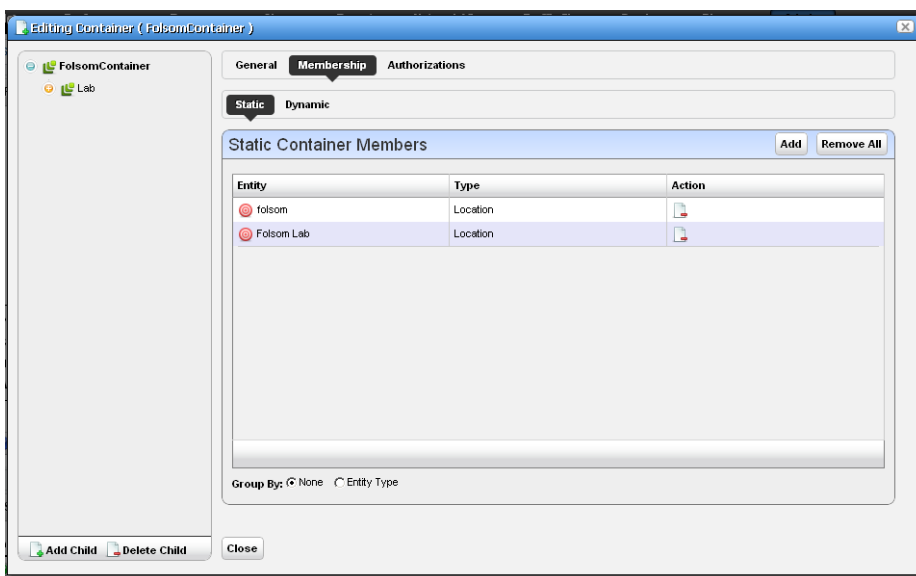
**Parent**—A read-only reminder of the container’s parent, if one exists.

**Access**—Select *Private* (creator only), or *Shared*. A private container is accessible to the container owner alone. *Shared* indicates other users can access a container, but even for *Shared* containers, you must assign Roles to give others access to the container. The *all* role grants access to everyone.

**Owner**—Select an owner for the container. The owner of a container can also change the ownership of the container

## Membership

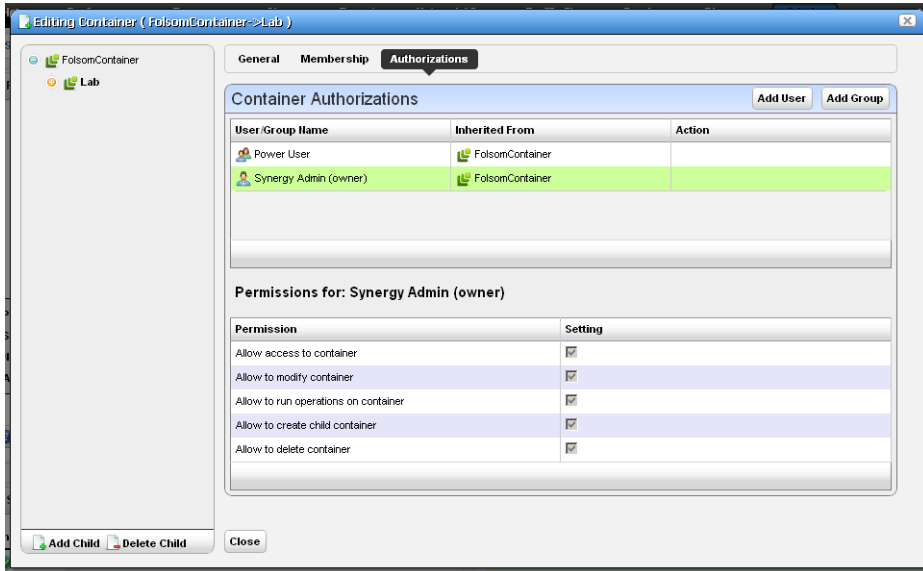
Container membership defines the inventory items that are in a container. You can select either a *Static* membership, which cannot change, or a *Dynamic* one, based on a filter. When Dell OpenManage Network Manager evaluates the filter it adds the resulting items as members in the container.



The sub-tabs at the top of the screen let you edit these types. See Managed Resource Groups on page 162 for more about the specifics of editing these groups. Click *Save* to preserve the membership you have configured. If you *Group By Entity Type* (at the bottom of the screen) rather than *None*, the list of devices appears in a tree, with each node as an entity type. Click the plus (+) to the left of the entity label to expand the tree.

## Authorizations

This tab configures user or group access to the container you are editing. Click *Add User* or *Add Group* to select the users or groups with permission to access the container you are configuring. By default containers are accessible to everyone.



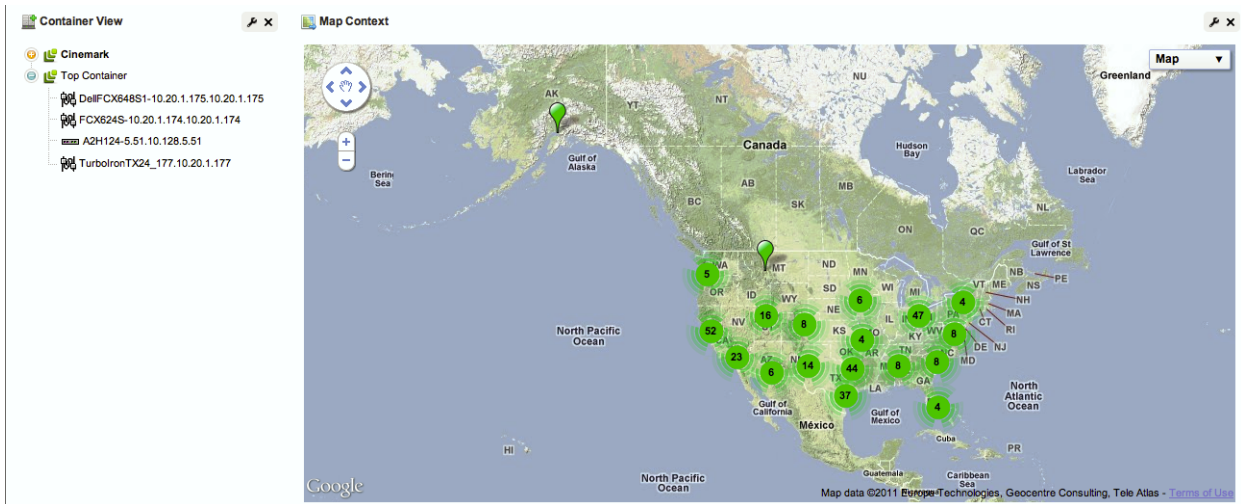
Each entry in the Container Authorizations list specifies the name of the user or group, and whether the entry is inherited or not. A child container by default inherits the authorizations from parent hierarchy, no explicit authorizations for child containers are necessary. Edit any authorizations in the parent.

When editing a child container, click a listed authorized user or group and its permissions appear in the panel at the bottom of this screen.

Clicking *Save* preserves any alterations you have made. Confirm the container is configured as you like by examining it in a Container View portlet.

# Map Context

In addition to displaying filtered-by-container portlets, you can view discovered devices in the *Map Context* portlet, automatically placed by location.

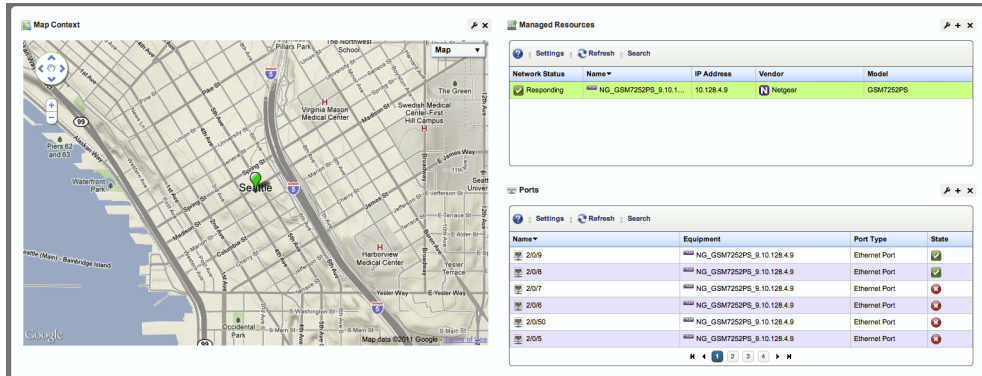


Notice that you can move the center of the map with the arrows in its upper left corner above the zoom in / out (+/-) buttons. The menu in the upper right corner lets you select a *Map* or *Satellite* views, and fine-tune them to include labels, terrain and so on.

You can configure locations with the *Tag* menu item. See *Tag* on page 90 for an explanation.

## Map Context without Containers

If a page has no containers then the Map Context can act like a container too. It displays all tagged resources within the system (see Tag on page 90). Clicking on a tagged item behaves like clicking a Container, confining displayed resources, alarms, and so on, to those for the selected tag.



Each tagged coordinate is cross-correlated with the Alarm State table (if there are alarms against it) and its color reflects the current Alarm state.

# Resource Discovery

The following explains and demonstrates the features included in Resource Discovery. The guide assumes you have full access to all the features (full license) included in the web portal.



## How To:

### Discover Resources

Here are the steps:

- 1 Set up Discovery Profiles for the resources you want to discover.
- 2 Execute the profile
- 3 View the results in the Managed Resources portlet.



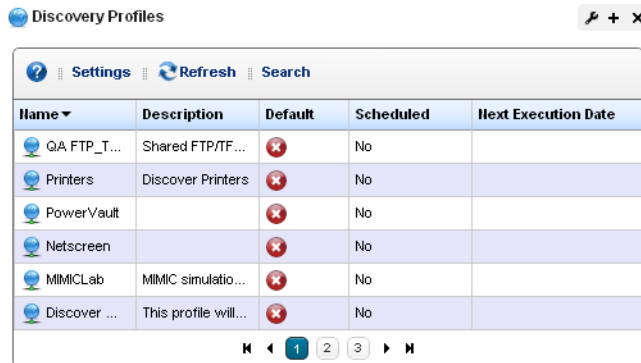
### Tip

Quick Discovery executes the selected *Default* discovery profile.



# Discovery Profiles

The discovery profiles set up equipment discovery for Dell OpenManage Network Manager.



Name	Description	Default	Scheduled	Next Execution Date
QA FTP_T...	Shared FTP/TF...	✘	No	
Printers	Discover Printers	✘	No	
PowerVault		✘	No	
Netscreen		✘	No	
MIMICLab	MIMIC simulatio...	✘	No	
Discover ...	This profile will...	✘	No	

The summary view displays the *Name*, *Description*, *Default* (the green check indicates the default profile), whether the profile is *Scheduled* and *Next Execution Date* for scheduled discovery.

## NOTE:

When Dell OpenManage Network Manager discovers unknown devices, it examines the RFC1213 MIB for hints of the device's capabilities, determining if it looks similar to a layer 3 router or a layer 2 switch. Since some device can do both, Dell OpenManage Network Manager classifies such ambiguous devices as routers.

## Menu Options

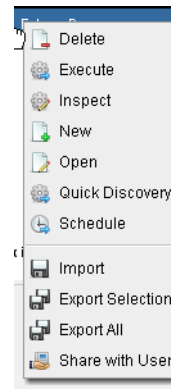
When you right-click a profile, the following menu options appear (in addition to the Common Menu Items):

**New**—Opens Discovery Profile Editor in new profile mode. (see General on page 154)

**Edit**—Opens Discovery Profile Editor.

**Copy**—Opens Discovery Profile Editor, and renames the selected profile as “CopyOf[Original Name]”.

**Execute**—Executes a discovery profile. This also produces an Audit trail (see *Audit Trail / Jobs Screen on page 91*). A message appears indicating the success or failure of discovery execution.



## Tip

Discovery execution continues in the background even when you close the audit trail / jobs screen, but the message indicating success / failure still appears when the discovery process is done.

**Inspect**—Validate the profile’s credentials, and that the device pings, and is licensed for discovery. Described in Inspection on page 159.

**Quick Discovery**—Opens discovery wizard displaying network and authentications. Click the *Execute* button once you open this screen to quickly discover equipment. (See Network on page 156 for more about the screen this displays.)

**Schedule**—Opens schedule editor where you can create and/or modify the schedule for a discovery profile’s execution.

**Audit**—Displays audit trails for the selected profile. See *Audit Trail / Jobs Screen on page 91*.

**Delete**—Deletes a discovery profile, after you confirm deletion. A notification message appears when deletion is completed on the application server.

The remaining menu items include *Import*, *Export Selection*, *Export All* and (if other users exist in the system) *Share with User*.

 **NOTE:**

Dell OpenManage Network Manager discovers Aruba Access points through the controllers to which they connect; discovery does not find stand-alone access points.

## Discovery Profile Editor

This editor lets you create or modify profiles. It has the following sub-sections:

- General
- Network
- Actions
- Inspection
- Results



### How To:

#### Edit Discovery Profiles

Here are the steps that appear in Discovery Profile Editor:

#### General

The General Panel collects all required data for a discovery profile. Dell OpenManage Network Manager validates each field, one at a time. Hints and tooltips appear if you hover your cursor near a field or label.

- 1 **General Parameters**—Set the *Name*, *Description* and a checkbox to indicate whether this profile is the discovery default.

The screenshot shows the 'Editing Discovery Profile (Netscreen)' window with the following details:

- Section 1: Set Discovery Profile General Parameters**
  - Name:** Netscreen (with a red asterisk and the note 'A unique name')
  - Description:** (empty field with the note 'optional')
  - Use as Discovery Default:**  Use as Baseline Default
- Section 2: Set Discovery Profile Options**
  - Discovery Options**
    - Device Naming Format:** Sysname and IP Address
    - Manage by:** IP Address
    - Resolve Hostname(s):**  Attempt to resolve Hostname to IP Address
    - ICMP Ping Device(s):**  Ping devices before authentication.
  - Filtering Options (Not Applicable to Inspection)**
    - Filter by Location:** (empty dropdown)
    - Filter by Vendor:** (empty dropdown)
    - Filter by Device Type:** (empty dropdown)
    - Manage ICMP-only Device(s):**  Manage devices that only respond to Ping
    - Manage Unclassified Device(s):**  Manage device(s) with no registered software installed

Navigation buttons at the bottom: Previous, Next, Save, Inspect, Execute, Close.

- 2 **Profile Options**—Select the *Device Naming Format* (how the device appears in lists, once discovered), whether to *Manage by IP* address or hostname, and check whether to *Resolve Hostname(s)*, *ICMP Ping Device(s)*, *Manage ICMP-only Device(s)*, or *Manage Unclassified Device(s)*. This last checkbox determines whether OpenManage Network Manager attempts to manage devices that have no OpenManage Network Manager device driver installed. If your system’s license permits it, such management may be possible, but more limited than for devices with drivers installed.



**CAUTION:**

If your license limits the number of devices you manage, discovering such “generic” devices may count against that limit.

The Filters (by *Location*, *Vendor*, or *Device Type*) let you narrow the list of devices discovered by the selected item(s). As the screen says, this filtering will not have any impact on the processing that occurs during the Inspection step.

 **NOTE:**

Fields like *Location* query the database for current information, so even though its field may appear empty, Locations may exist. Click the Search button to the right of this field to populate it. Keeping such fields empty until you use them enhances performance.

The buttons at the bottom of the Profile Editor let you navigate through this series of panels. *Previous / Next* move back and forth between screens, *Save* lets you preserve whatever stage you have configured, and close the editor, *Inspect* moves directly to the Inspection screen (described below), and *Execute* triggers the discovery profile and opens the Results panel, displaying message traffic between Dell OpenManage Network Manager and the device(s). Click the “X” in the top right corner of these screens to close them without saving.

 **Tip**

If you discover devices without retrieving their hostnames, and that hostname is needed later, you can run the *Resolve DNS Hostnames* activity to get the hostname. This fetches the DNS hostname and resyncs the device.

## **Network**

The Network Panel collects the network (IP range, hosts, and so on) and the authentication information for the discovery profile.

- 3 After you click *Next*, the *Network* panel appears.

**Network Type and Addresses**—Select the type of entry in the pick list (*IP Address(es)*, *CIDR Address*, *Hostname*, *SNMP Broadcast*, *Subnet*).

The screenshot shows a dialog box titled "Editing Discovery Profile (Netscreen)" with a "Network" tab selected. The main heading is "3. Select Network Type and Address(es)". Below this, there is a dropdown menu for "IP Address(es)" with "172.16.0.1" entered. A prompt below reads "Enter IP Address(es), IP Range(s) and/or Network(s)".

Under the heading "Add Existing Authentication To Resource Discovery", there are several fields:

- "Authentication Name": Telnet/SSH - Netgear
- "Protocol Type": SSH
- "Select Management Interface Parameters":

  - "Timeout": 10
  - "Retries": 1
  - "Port": 22

At the bottom of the dialog, there are buttons for "Apply" (with a green checkmark), "Cancel" (with a red X), "Previous", "Next", "Save", "Inspect", "Execute", and "Close".

The tooltips in the data entry field tell what valid entries look like.

 **NOTE:**

When specifying network addresses using the Subnet type, you must specify the Network address at the beginning of the subnet since Dell OpenManage Network Manager assumes it is the starting IP address for the range. If you specify an address in the middle of the subnetwork then Dell OpenManage Network Manager may discover devices outside of that subnetwork. This also means that IP addresses in the network that precede the specified address are not discovered. To avoid these issues, use the CIDR specification of the network to discover rather than the subnet ID.

- 4 **Authentication**—You can create new, or add existing authentications. See Authentication on page 143 for the way to create such authentications outside the discovery process.

Notice that authentications appear with *Edit / Delete* icons and *Up / Down* arrows on their right. The *Edit* icon opens the authentication editor. Click the arrows to arrange the order in

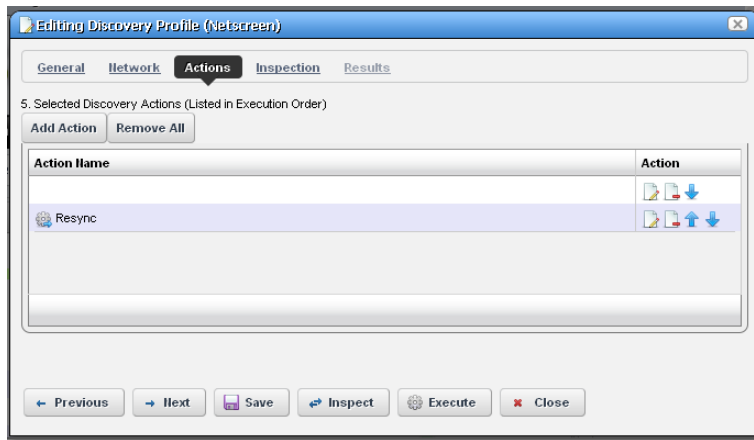
which credentials are tried (top first). Ordering only applies when two credentials are of the same type.

### Tip

If you have imported a discovery profile without importing or creating the authentications it uses, editing authentications is an exercise in frustration. If you cannot import authentications, or have not created them when you do attempt to edit them, the easiest solution is to delete the un-imported un-created authentication the profile refers to and create a new one.

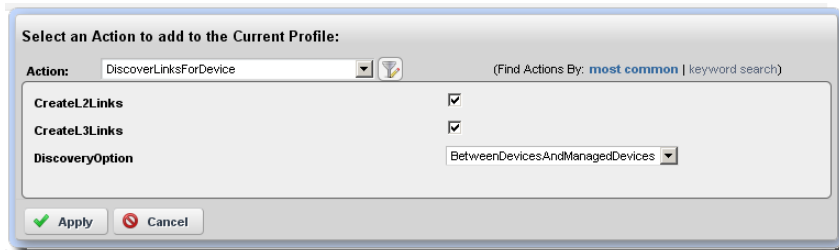
## Actions

- 5 When you click *Next*, the *Actions* panel appears.



You can simply accept the default actions that appear here (like *Resync*, and *Learned MAC* discovery) by clicking *Next* to the *Inspection* portion of discovery, or you can do the following:

**Add Action**—This opens a screen with a selection list of available actions. Click *Apply* to select an action to add to the list for this profile.



Notice the default for this screen displays the *most common* actions, but you can also click *keyword search* in the top right corner to display a search field instead of a pick list with the most common actions. The search results appear in the pick list. When you

select an item, if it has parameters, they appear listed below that item. Use the check-box(es) or pick list to configure these parameters, then click *Apply* to select this action as part of the profile. See Actions on page 116 for more about these.

**Edit, Delete, Move**—These icons appear to the right of each action. If you *Edit* a profile with parameters, you can change them. The screen looks like the one that appears when you *Add* actions. Deleting actions removes them from the list, and the *Move* arrows help arrange the order in which actions appear listed, and are executed. The list of actions the profile executes goes from top-to-bottom.

## Inspection

Using the Inspection Panel is an optional step. If you want to execute the profile after entering the required information on the General and Network panels, you can skip this step, and just click *Execute* at the bottom of the panel.

- Inspection**—This screen lets you preview the discovery profile’s actions and access to devices. If you clicked *Next* rather than *Inspect* at the bottom of the previous screen, click *Start Inspection* in the top right corner of this screen to begin the inspection process that validates the device’s credentials.

6. Inspect Network using current settings (optional)

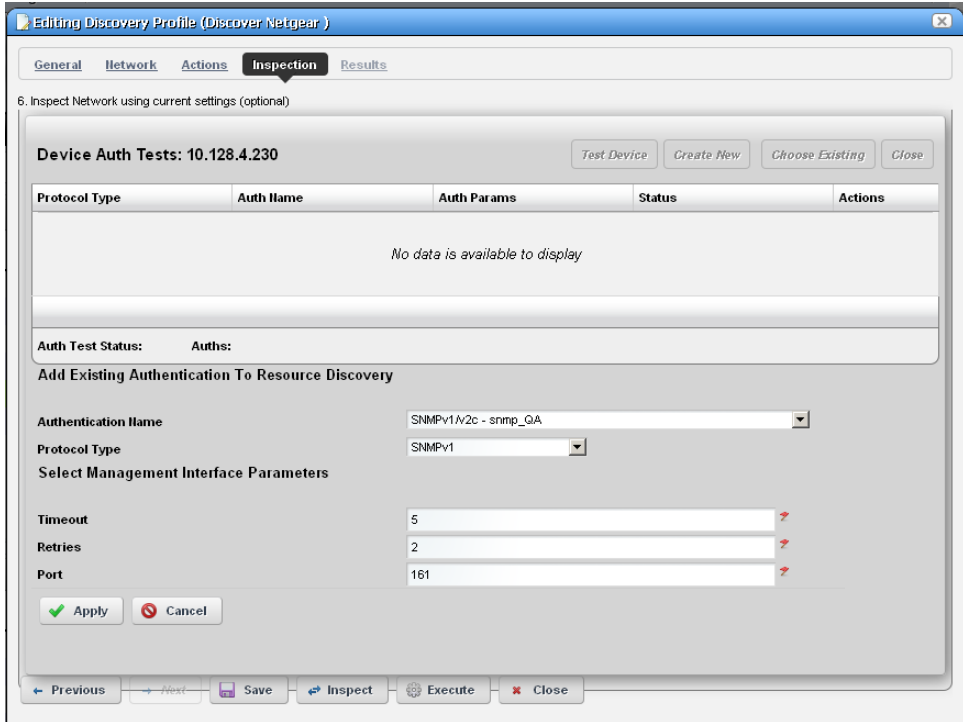
Actions:

Discover	IP Address/ Protocol Type	Hostname/Auth Name	Vendor/Auth Params	Status	Pinged	Licensed
	10.128.4.32			Pending		
	10.128.4.30			Pending		
	10.128.4.25			Pending		
	10.128.4.22			Pending		
	10.128.4.23			Pending		
	10.128.4.48			No Response		
	10.128.4.49			No Response		
	10.128.4.46			No Response		
	10.128.4.28			No Response		
	10.128.4.47			No Response		
	10.128.4.44			No Response		
	10.128.4.26			No Response		
	10.128.4.45			No Response		
	10.128.4.27			No Response		

Inspection Status: Ping: 96 / 210 Hostname: Pending Auths: Pending

Notice that the *Inspection Status* fields at the bottom of the screen indicate the success or failure of Ping, Hostname resolution, and Authentications, and the *Status* column displays whether a valid authentication exists, whether it has been tested, and whether the test is successful.

When authentications are unsuccessful, click the icons to their right to remove or edit them. You can also click the wrench / screwdriver “fix it” icon in the *Discover* column to open an editor where you can revise the authentications for that device.



Clicking *Create New* lets you create new authentications, *Choose Existing* lets you select from existing authentications, *Test Device* lets you try out the authentications you have selected, and *Close* closes this screen. Notice that you can configure new or existing authentications’ port, retry and timeout settings before you click *Apply* (or *Cancel*) in the authentication editor that appears after clicking the “Fix it” button.

- 7 **Save**—Click *Save* to preserve the profile. You can then right-click it to select *Execute*. If you select *Execute* from the profile editor, Dell OpenManage Network Manager does not save the profile to execute later.



## Results

- 8 **Execute**—Clicking *Execute* begins discovery, and the message traffic between Dell OpenManage Network Manager and the device appears on the *Results* screen.  
This produces a standard Audit Trail / Jobs Screen screen displaying the message traffic. See also *Audit Trail / Jobs Screen on page 91* for more about retrieving archives of such screens.
- 9 A message (*Discovery Profile Execute is complete*) appears in the *Messages* at the bottom left of the status bar.
- 10 Click the X in the top right corner of the discovery profile editor to close it.

## Discovery Profiles Expanded

This larger view offers a *Reference Tree* snap panel where you can see the connection between a selected profile and the authentications and discovery tasks it includes.

The screenshot displays the 'Discovery Profiles' interface. At the top, there is a 'Default Resource Profile Filter' dropdown, an 'Advanced Filter' button, and a search bar. Below this is a table with columns: Name, Description, Default, Scheduled, and Next Execution Date. The 'Better Juniper Discovery' profile is highlighted in green. Below the table is a 'Reference Tree' panel showing a hierarchical view of the selected profile's components: Better Juniper Discovery, Authentications (doradof!, qapublic), and Tasks. The interface also includes a 'Return to previous' link, 'Search', 'Refresh', and 'Settings' buttons, and a 'Snap Panels' | 'Close' button at the bottom right.

Name	Description	Default	Scheduled	Next Execution Date
Discover juniper devices	J2300 10.128.3.16 admin@Doradof! J2300 192.16...	✗	No	
Discover IPMI - DISCOVER (Need snmp disc ...	Need to 1- discover as snmp 2- add IPMI MGMT i...	✗	No	
Discover Dell	All Lab Dell devices	✗	No	
Discover Cisco	All LAB cisco Devices	✗	No	
Brocade_Foundry	Brocade/Foundry	✗	No	
Better Juniper Discovery	This discovers Dorado's Juniper	✗	No	
Aruba		✓	No	

In addition to the right-click available in the summary screen, you can also click *Settings* to configure columns.

# Managed Resource Groups

These groups make acting on several devices at once more convenient, making management of groups of devices possible. The summary screen displays columns describing the group *Name*, *Type*, and *Icon*. You can also right-click to do the following:

**New**—Lets you make either a Static Group (one in which you select devices) or a Dynamic Group (one in which a filter selects devices). See details of these screens below.

**Edit**—This opens the same editors as *New*, populated with the information for the selected group.

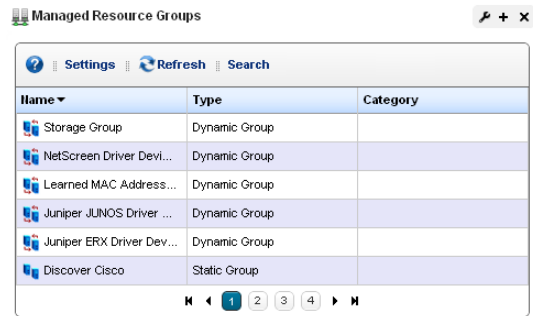
**Edit Resources**—Lets you edit resources associated with the selected group like its location, contact, or whether to manage it by hostname.

**Visualize**—Displays a topology map of the selected group. See Chapter 5, *Visualize My Network* for more.

**Actions**—Select from a sub-menu of actions available for the group.

**Adaptive CLI**—Select from a sub-menu of Adaptive CLI

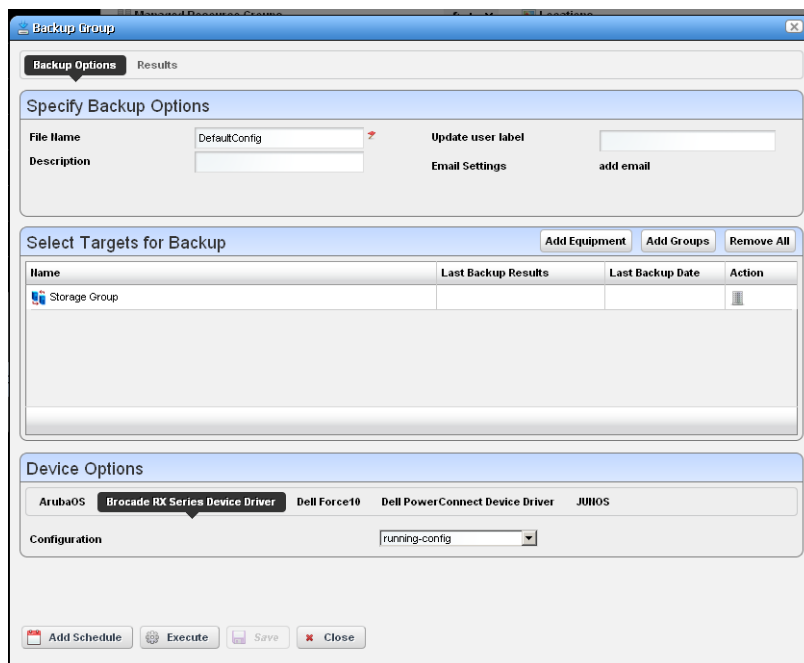
**Change Management**—Elect to run Change Determination process, or any Proscan policies associated with the group. See Chapter 9, *Change Management – ProScan* for an explanation of these. If you want to execute a ProScan policy not already associated with this group, then select *Execute Proscan Policy*. A selection screen appears where you can select a policy and either execute or schedule it.



The screenshot shows a window titled "Managed Resource Groups" with a toolbar containing "Settings", "Refresh", and "Search". Below the toolbar is a table with three columns: "Name", "Type", and "Category". The table contains six rows of data, each with a small icon to the left of the name. At the bottom of the table is a pagination control showing "1" selected out of a total of 4 items.

Name	Type	Category
Storage Group	Dynamic Group	
NetScreen Driver Devi...	Dynamic Group	
Learned MAC Address...	Dynamic Group	
Juniper JUNOS Driver ...	Dynamic Group	
Juniper ERX Driver Dev...	Dynamic Group	
Discover Cisco	Static Group	

**File Management > Backup, Restore, Deploy**— Lets you call on Dell OpenManage Network Manager’s NetConfig configuration file backup, restore and deploy capabilities. See Backup Configurations on page 225 for an example of the steps this follows. See also File Management on page 223 and more about deploying updates to the OS for the selected resource group. See Deploy Firmware on page 238 for details.



When you select a group backup, and the group contains devices of several types, the *Device Options* panel displays a tab for each device type. Select the backup parameters there before executing or scheduling backup.

**Link Discovery**—Discover links between members of the selected group, and others. See New Link on page 175 and Link Discovery on page 176 for details.

**Resync Resources**—Queries the devices in the group to update Dell OpenManage Network Manager’s database.

**Delete**—Remove the selected group from inventory. The devices remain in inventory, but this removes the grouping.

**Import / Export**—Lets you import from or export to file the group configuration.

**Share with User**—Share the group with another user. See Sharing on page 87.

Dell OpenManage Network Manager does not support static groups that include members retrieved by (dynamic) filters. You can configure membership with dynamic resource groups that include group memberships as filter criteria. For example you can create a filter for members of ResourceGroupABC or members of ResourceGroupXYZ.

### Expanded Managed Resource Groups

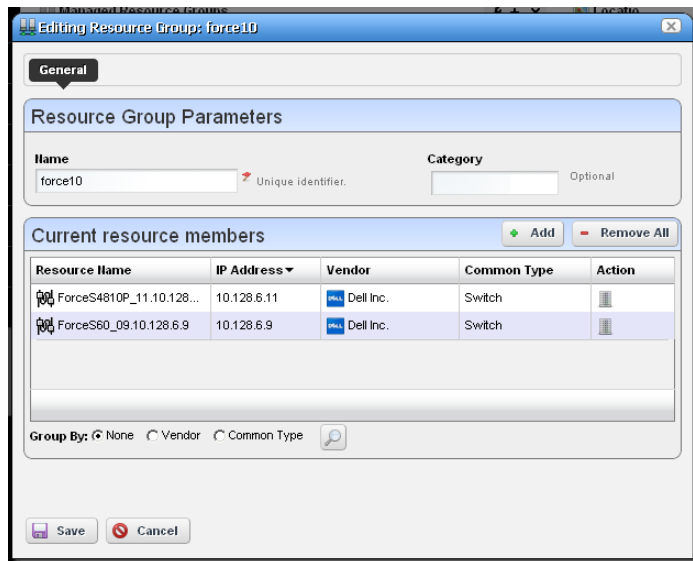
The expanded Managed Resource Groups screen lets you see the summary screen's groups with a Reference Tree snap panel that displays a selected group's connection to its devices and any assigned monitors.

## Static Group

Selecting *Static Group* as the type to create displays a selector screen where you can *Name* and select a *Category* for the group, then search for available resources with a filter. Click *Apply Filter* after you have configured it, and a list of devices fitting its criteria appears. Select device(s) and click *Add Selected*, or simply click *Add All* to add the entire list to your static group. Notice that you can continue to re-use this filter to list devices, and continue to select them.

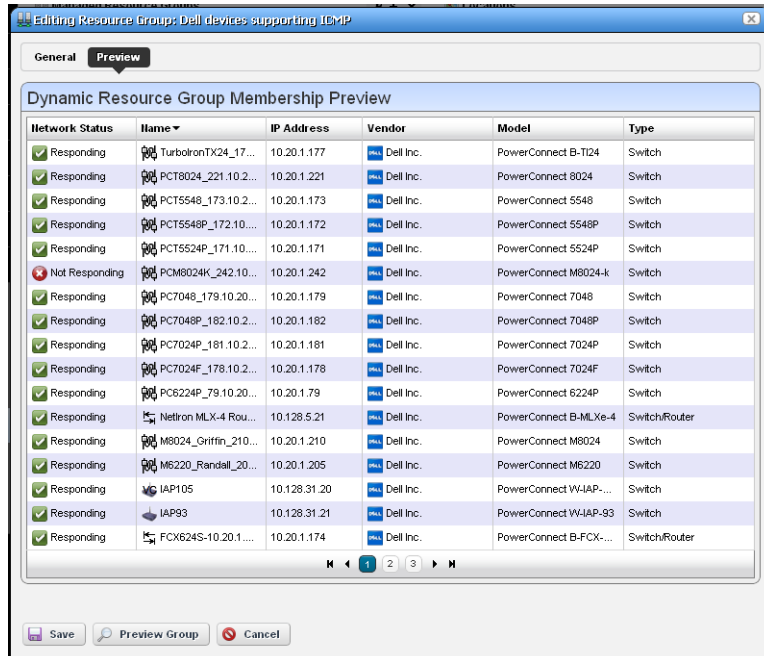
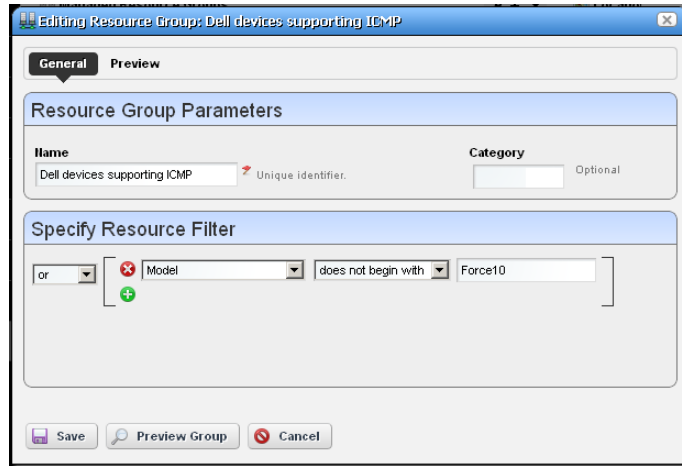
When you select a device, it no longer appears listed. When you click *Done* the subsequent screen displays all devices you have selected. You can click *Add* on this screen to return to the previous screen (or *Remove All* to delete the listed devices from the group). At the bottom of this screen, you can also elect to group devices by *None*, *Vendor* or *Common Type* (Switch, Router, and so on). These last two create “trees” with nodes for each vendor or type. You can also click the magnifying glass to search through listed devices. Clicking *Remove All* removes all devices in the group.

Click *Save* to preserve the group you have configured.



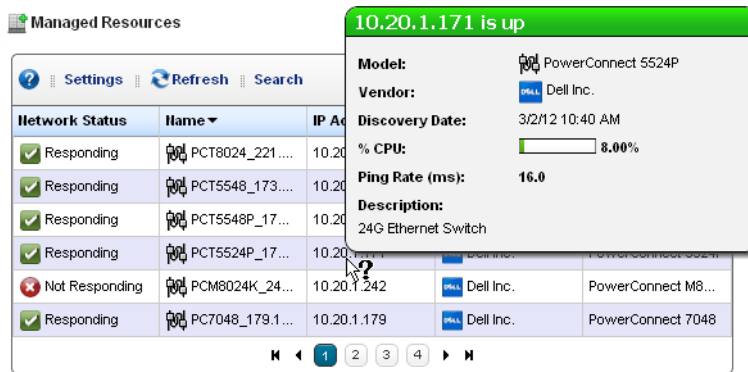
# Dynamic Group

In contrast to Static Groups, Dynamic Groups do not let you select individual equipment. You simply configure a filter, and OpenManage Network Manager creates the group on the fly. After you enter the *Name* and *Category* for the group, create the filter. To see what the group would look like, click *Preview Group*. This opens the *Preview* tab, concealing the *General* tab. To return to *General*, click that at the top of the screen. Click *Save* to preserve the group configuration, or *Cancel* to exit without saving.







# Managed Resources

The *Managed Resources* summary portlet displays the discovered devices on your network, their *Network Status*, *Severity* (of their highest recent alarm), *Equipment Name*, *IP Address*, and *Vendor Name*.



Hovering the cursor over a listed device's IP address produces a popup with its alarm status in the headline (both severity name and color), the % CPU, % Memory, and Ping. See the Managed Resources Expanded section for a description of columns and additional capabilities in that version of the portlet. Icons that appear next to the equipment name have some significance. For example:

Icon	Device Type
	Switch
	Router or Switch/ Router
	Wireless Virtual Controller
	Wireless Access Point

You can schedule actions selected here in addition to executing them immediately. See Schedule Actions on page 186 for more about that. Right-clicking a listed resource can display the following menu items:

**Edit**—This lets you use the following screens:

- General
- Authentication

- Management Interface

Click *Save* to preserve any changes made in these screens to Dell OpenManage Network Manager's database, or *Close* to abandon any changes made in editor screens. Unless the device is a printer, changes to these screens typically make database changes, not changes on the device.

## General

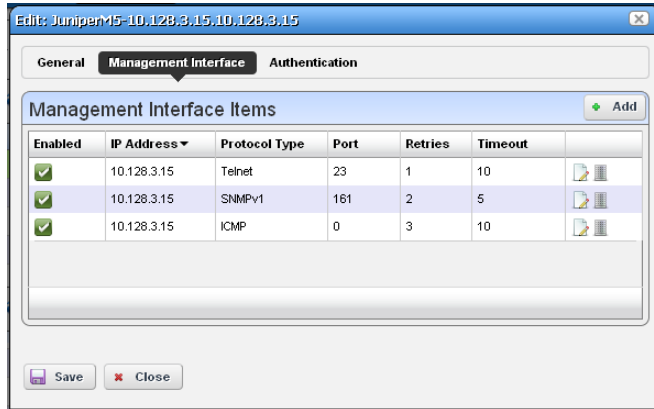
This screen may vary for different kinds of devices. Its *General Details* panel displays the *Name*, *Description*, *Vendor*, *Location*, *Contact*, and *Equipment Icon* for the selected device.

The screenshot shows a web-based configuration interface for a network device. The title bar reads 'Edit: 6248P\_Kinnick\_80.10.20.1.80'. The interface is organized into two main panels. The top panel, 'General Details', contains several fields: 'Equipment Name' (6248P\_Kinnick\_80.10.20.1.80), 'Description' (Powerconnect 6248P, 3.2.0.7, VxWorks 6.5), 'Vendor' (Dell Inc.), 'Location' (Folsom), 'Contact' (Click to Select), 'Equipment Icon' (a small icon), 'Service Tag', and 'Asset Tag'. The bottom panel, 'Extended Details', has three tabs: 'Network', 'Properties', and 'Settings'. The 'Network' tab is selected and shows 'IP Address' (10.20.1.80), 'DNS Hostname', 'Manage By Hostname' (unchecked), and 'Network Status' (Responding). At the bottom of the window are 'Save' and 'Close' buttons.

The *Extended Details* panel includes *Network*, *Properties* and *Settings* tabs. These let you view or alter things like *IP Address*, *DNS Hostname*, *Manage by Hostname*, *Network Status*, *Model* and *Equipment Type*, *Serial Number*, *Software Version* *Firmware* and *Hardware* versions. The *Settings* tab lists the *System Object ID*, *Date created* (the date this managed device entered the database), *Creator* (the user who discovered or created the device), *Install Date*, *Administrative State*, *Operational State*, and any *Notes* about the device.

## Management Interface

This lists the management interfaces for the selected device, including the *IP Address*, *Port*, *Retries*, and *Timeout*.



Notice you can *Add* interfaces with the button in the upper right corner.

## Authentication

This lists the authentications for the selected device. You can *Add* authentications with the button in the upper right corner too. These authentications originate in the portlet described in Authentication on page 143.



**Details**—Displays several panels with detailed resource information. These include *Alarms*, *Performance Indicators* graphs, *Ports*, *Audit Trail*, *Interfaces*, *Associated Link(s)*, *Latest Configurations*, and a *Details* panel with model and other information. A *Network Details* panel displays *VLAN(s) by ID*, *VLAN(s) by Port*, or *STP Data*. Click the button in the upper right corner of the panel to select among those options

The screenshot shows the 'Details' panel for a network device (ForceS4810P\_11.10.128.6.11). The panel is divided into several sections:

- Alarms:** A table with columns for Severity, Date Opened, and Event Name. One alarm is listed: Minor, 3/21/2 10:57 AM, authenticationFailed.
- Performance Indicators:** Two bar charts showing CPU Utilization (7%) and Memory Utilization (6%).
- Ports:** A table with columns for Name and State. It lists ManagementEthernet 0/0 through 5/0.
- Audit Trail:** A table with columns for User ID, Action, Status, and Subject. It shows a series of actions performed by 'admin'.
- Associated Link(s):** A table with columns for Link Name and Link Type. It shows a link for GigabitEthernet 0/47.
- Latest Configurations:** A table with columns for Equi, Fl., Fl., Date Saved, V..., and Fl... It shows two configuration files.
- Details:** A panel with various fields including Equipment Name, Description, IP Address, Alarm Severity, Network Status, DNS Hostname, Manage By Hostname, Location, Contact, Equipment Type, Vendor, Model, System Object ID, Serial Number, Hardware Version, Firmware Version, Software Version, Virtual, Date created, Creator, Discovery Date, Last Modified, Last Backup, Last Configuration Change, Service Tag, and Asset Tag.
- Reference Tree:** A tree view showing the device hierarchy, including Loopbacks, NULL 0, Port Channels, and Slots 0 through 5.
- Monitor Status Summary:** A table with columns for Monitor, Target, and Last Polled. It shows a list of monitored items and their last poll times.

Notice that you can right-click listed interfaces, configuration files, and so on to perform more actions.

**Visualize**—Create a topology map of the selected resources. See Chapter 5, Visualize My Network for more about such maps.

**Actions**—Actions you can initiate here can include things Adaptive CLI Actions (see Chapter 11, Actions and Adaptive CLI), and other actions specific to the selected device.

Actions (including Adaptive CLI) appear in *SHOW*, *CONFIG* and in some cases *MANAGE* categories. The list that appears depends on the device selected. You can also open search field by clicking the magnifying glass at the bottom of this screen. Using that field, the list narrows to actions matching your search string. Select one, and click *Load Selected* to run it manually.

 **NOTE:**

Since menu items appear in alphabetical order, this may be in a different location, depending on the device vendor name.

**Adaptive CLI**—This displays *Adaptive CLIs* related to the selected device, and opens with a screen where you can enter any relevant parameters for those commands. See the previous *Action* menu item’s description, and Chapter 11, Actions and Adaptive CLI for more about these.

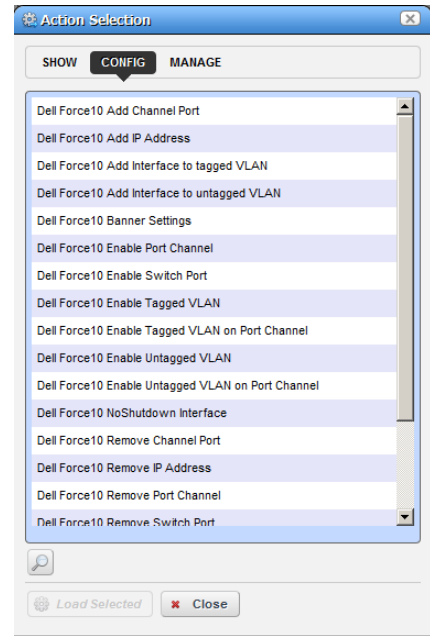
**Change Management**—Run *Change Determination*, or *Execute ProScan* policies for the selected device. See Chapter 9, Change Management – ProScan for more about these capabilities. If you want to execute a ProScan policy not already associated with this device, then select *Execute Proscan Policy*. A selection screen appears where you can select a policy and either execute or schedule it.

**Direct Access**—This opens a sub-menu where you can select the type of available direct cut-through access to the selected device, or ICMP ping that device. See MIB Browser on page 188 and Terminal on page 190 for more the about the available direct access options.

 **NOTE:**

You must have Java installed (and updated) on the client for direct access to function correctly.

**Event Management**—This lets you suppress or update alarms related to the selected resource. You can *Start Alarm Suppression* (*Stop* appears, once you have started suppression), *Stop All Alarm Suppression*, *Schedule Alarm Suppression*, *View Active Suppression(s)*, and *Resync Alarms* (corrects Dell OpenManage Network Manager’s display to match the latest information from the device already in the database). Event Management — This lets you suppress or update alarms related to the selected resource. You can *Start Alarm Suppression* (*Stop* appears, once you have started suppression), *Stop All Alarm Suppression*, *Schedule Alarm Suppression*, *View Active Suppression(s)*, and *Resync Alarms* (corrects Java client’s display to match the latest information from the device already in the database). Alarms

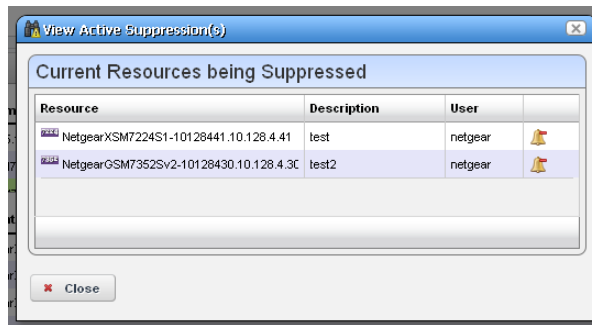


resync for all devices. This corrects the display when the alarm color displayed, either here or in topologies, does not match the highest severity alarm for the device in the alarm portlet. Dell OpenManage Network Manager issues no alerts when resync occurs.

When you *Start* alarm suppression, first enter a description in a subsequent screen, then a Success / Failure message appears confirming suppression has started.

*Schedule* displays a *Parameters* screen where you can describe the scheduled suppression and select a duration and any additional suppression targets. The *Schedule* tab on this screen lets you start suppression at a specific time and configure any recurrence, and termination (*Stopping on*) for the scheduled suppression. The termination can either be a date, a number of occurrences or *Never*.

Deleting, stopping or disabling a schedule does not interrupt suppression, once it has started. You must right click selected devices and select *Stop All Alarm Suppression*. You can also delete suppressions after you select *Event Management > View Active Suppression(s)*.



The viewer lists devices for which alarm suppression is active, their description and configuring user. Click the *Stop Suppression* icon to the right of listed devices to terminate their alarm suppression.

Suppressed events / alarms do not appear in the Alarm display, but, unlike rejected events, the Event History screen can display a record of them.

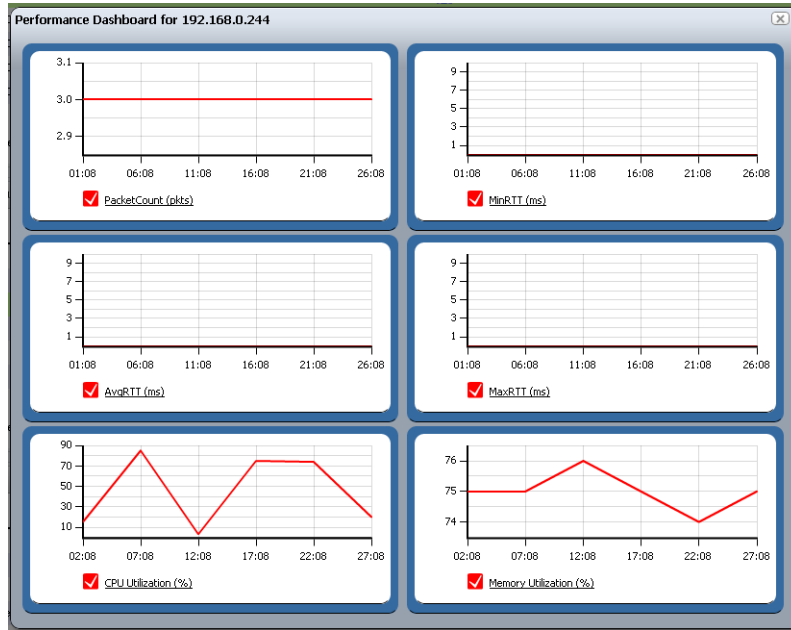
**File Management**—View a current configuration file, compare it to previous backups, backup, restore, import or export a configuration file. You can also deploy firmware to devices from this menu.

If you go to the Configuration Files portlet, you can also edit backed up configuration files. See File Management on page 223 for details.

**Links**—Create a new link or discover links between members of the selected group, and others. See New Link on page 175 and Link Discovery on page 176 for details.

**Performance**—Select from the following options:

*Show Performance*—This displays a dashboard with various performance metrics for the selected device. These can include packet counts, RTT (round-trip time) measurements, and CPU / Memory utilization graphs.



See Dashboard Views on page 277 for more about re-using and managing these capabilities.

*Show Top Talkers*—This displays a *Top Talkers Dashboard* of performance metrics for the selected resource. Use the icon in the top right corner to re-configure the default display. See Dashboard Views on page 277 and Top [Asset] Monitors on page 276 for more information.

*Show Key Metrics*—This lets you see available key metrics for the selected resource, and configure their display.

**Resource Groups**—This lets you add the selected device to new Dynamic or Static groups, or to existing groups. See for Managed Resource Groups on page 162 more about this.

**Resync**—This re-queries the device for more current information.

**Traffic Analyzer**—*Register* or *Unregister* the selected resource for traffic analysis. You can also select *Show Traffic* to see a screen with traffic for the selected device. See Chapter 8, Traffic Flow Analyzer for more about Traffic Flow.

**Delete**—Remove the selected device from inventory.

**View as PDF**—Displays the selected device as an Acrobat pdf. See View as PDF on page 90.

## Managed Resources Expanded

If you click the plus (+) in the upper right corner of the summary screen, this expanded screen appears. As in all such screens, you can limit what appears listed with the filters at the top of the screen. Select the filter from default, seeded filters with the pick list at the top left corner of the screen. You can also create your own custom filter by clicking *Advanced Filter* to the right of this pick list (see Filter Expanded Portlet Displays on page 85 for more).

The screenshot displays the 'Managed Resources' interface. At the top, there is a 'Default Resource Filter' dropdown and an 'Advanced Filter' button. A search bar and 'Refresh' button are also present. Below this is a table with columns: Name, IP Address, Vendor, Model, Type, Firmware Version, Software Version, Last Backup, Location, and Hardware Version. The table lists several Dell switches, with one highlighted in green. Below the table, it indicates '42 item(s) returned'. The interface is divided into three main sections: 'Reference Tree' on the left showing a hierarchy of devices, 'Utilization Summary' in the center with a line graph for CPU, Disk I/O, Memory, and Ping Rate, and 'Bandwidth Utilization' on the right showing a list of interfaces and their bandwidth usage.

The *Settings* button lets you configure the displayed columns and their order.

### Tip

You can select multiple devices by Ctrl-clicking them in the expanded portlet. This lets you do these same tasks on more than one device. You can also perform such tasks on multiple devices with managed resource groups. See Managed Resource Groups on page 162.

The following are available columns:

**Network Status**—The network status of the device.

**Alarm Severity**—The highest open alarm for the device.

**Equipment Name**—The name of the device.

**IP Address**—The IP address of the device.

**Vendor Name**—The vendor for this device.

**Model**—The model of the device.

**Equipment Type**—The type of equipment.

**Firmware Version**—The firmware version of the device.

**Software Version**—The software version of the device.

**Last Backup**—The device’s last backup date.

**Location Name**—The device’s location.

**Hardware Version**—The hardware version for the device.

**Backup Result**—The result the device’s last backup.

**Restore Result**—The result the device’s last restoration.

This screen has several snap panels, some compressed “windowshade” style. Click the title bar for these snap panels to toggle expand / collapse. These display information about the device selected in the list at the top of the panel.

### **Reference Tree**

This displays the device and connected components, tree style.

### **General: Details**

This includes information about the *Equipment Name*, *Vendor*, *Location*, *Contact*, *Icon*, and its *Last Modified* and *Discovery Date*.

### **General: Properties**

This tab includes the *IP Address*, *DNS Hostname*, *Firmware Version*, *Hardware Version*, *Model*, *Serial Number*, *Software Version*, *Managed by Hostname* (if active, this resolves a DNS name rather than use an IP address to manage this resources), and *Equipment Type* information.

### **General: Settings**

This includes the *system Object Id*, *Date Created* (that is, discovered), *Creator* (the user who performed discovery), *Install Date*, *Administrative State* (Locked [Device use is prohibited] Shutting Down [Only existing users can use the device] Unlocked [Normal use of device is permitted]), *Operational State* (Disabled [Inoperable because of a fault, or resources are unavailable] Enabled [Operable and available for use] Active [Device is operable and currently in use with operating capacity available to support further services] Busy [Operable and currently in use with no operating capacity to spare]) OpenManage Network Manager.

## Network Details

This displays network information like *VLAN(s) by ID*, *VLAN(s) by Port* and *STP Data*. Use the pick list in the upper right corner of this snap panel to select which to display.

## Utilization Summary

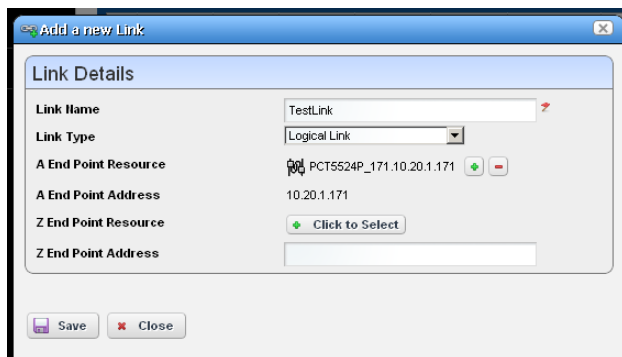
A graph of the device utilization, typically for CPU, Disk I/O, Memory and ping rate.

## Bandwidth Utilization

A graph of the device's bandwidth utilization. Notice that you can change the number of top interfaces graphed, when this is applicable.

# New Link

When you create a new link, the *Link Details* screen appears where you can configure the link.



The screenshot shows a window titled "Add a new Link" with a "Link Details" section. The fields are as follows:

Field	Value
Link Name	TestLink
Link Type	Logical Link
A End Point Resource	PCT5524P_171.10.20.1.171
A End Point Address	10.20.1.171
Z End Point Resource	Click to Select
Z End Point Address	

At the bottom of the dialog are "Save" and "Close" buttons.

This screen has the following fields:

**Link Name**—A text identifier for the link.

**Link Type**—Select the type of link from the pick list.

**A End Point Resource / Address**—Click the plus (+) to select a resource for one end of the link.

When you right-click a selected resource, it automatically appears here. Click the minus (-) to remove it.

**Z End Point Resource / Address**—Click the plus (+) to select a resource for one end of the link.

When you have selected two resources, they automatically appear as A and Z endpoints.

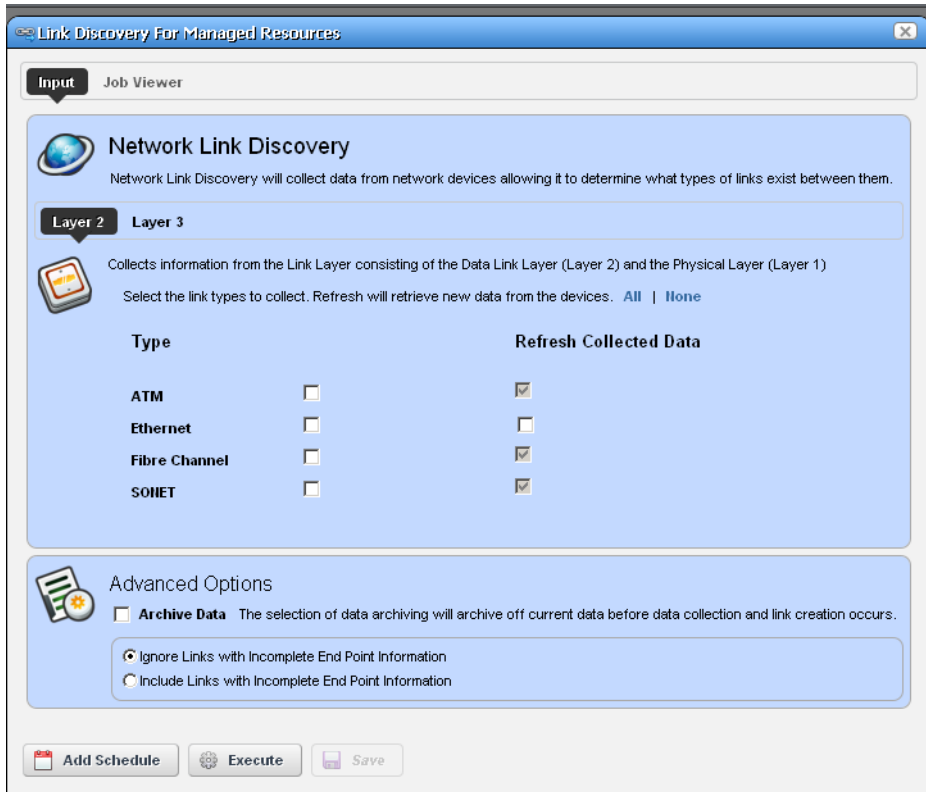


### Tip

Remember, you can only multi-select in the expanded version of the portlet.

# Link Discovery

This is an automated network link discovery feature that you can initiate from individual devices in the Managed Resources portlet, or with the *Link Discovery* button on the home screen. See Link Discovery Prerequisites on page 177 for a list of device features that provide link information. Links discovered can also appear in the screen described in Links in Visualization on page 220.



When you elect to discover links from a right-click menu, the *Network Link Discovery* screen appears. Check the type of links you want to discover or from which you want to refresh collected data. Other options available on this screen include the following:

**Layer 2 / Layer 3** [checkboxes]—Select the layer for which you want to discover links. Depending on the layer selected, the available types appear as checkboxes below this tab selection.

### Tip

Click *All / None* to select all or none of the displayed types for each layer. Remember, selecting more link types consumes more time and processing power.



## Advanced Options

**Archive Data**—Checking this archives current data before collecting information about and discovering links.

**Ignore / Include Links with Incomplete Endpoint Information**—Select the option best suited for your network.

Click *Add Schedule* to schedule link discovery, or *Execute* to run it now (and confirm you are willing to wait for results in a subsequent screen). The *Job Viewer* tab in the link discovery screen displays the message traffic between Dell OpenManage Network Manager and the device(s). See Audit Trail Portlet on page 93 for more about Job Viewer screens.

## Link Discovery Prerequisites

Although Dell OpenManage Network Manager automates link discovery, you must enable the sources for link discovery information on the devices where you do such discovery.

Data sources used to derive links appear listed below. These sources are typically required for the network operations, so if all the sources are disabled, there would be no network to manage in the first place. The more of the sources are enabled, the higher is the quality of links discovered.

Data sources supported:

- IEEE Link Layer Discovery Protocol (LLDP) support
- Cisco Discovery Protocol (CDP) support (reserved for future use)
- Extreme Discovery Protocol (EDP) support (reserved for future use)
- VLAN support
- Spanning Tree Protocol (IEEE STP/RSTP/PVSTP+/PVSTP+) support
- AFT support

# Equipment Details

This screen lets you “drill down” to display equipment details for resources. You can see it by selecting *Details* in the right-click menu for the Managed Resources portlet. You can also install an Equipment Details portlet on a page and use the Container View portlet to select individual devices that appear in it. In that case, you must select an individual device before it displays data.

Details [Return to previous](#)

ForceS4810P\_11.10.128.6.11

### Alarms

Severity	Date Opened	Event Name
Minor	3/2/12 10:57 AM	authenticationFail

### Performance Indicators

**CPU Utilization**  
0% 25% 50% 75% 100%  
7%

**Memory Utilization**  
0% 25% 50% 75% 100%  
8%

### Details

**Equipment Name:** ForceS4810P\_11.10.128.6.11  
Force10 Networks Real Time Operating System, Software Force10 Operating System Version: 1.0 Force10 Application Software Version: 8.3.7.2 Copyright (c) 1999-2011 by Force10 Networks, Inc. Build Time: Sun Aug 7 08:32:10 PDT 2011

**Description:**

**IP Address:** 10.128.6.11

**Alarm Severity:** Minor

**Network Status:**  Responding

**DIIS Hostname:**

**Manage By Hostname:**  False

**Location:** LAB

**Contact:** IT

**Equipment Type:** Switch

**Vendor:** Dell Inc.

**Model:** Force10 S4810

**System Object Id:** 1.3.6.1.4.1.6027.1.3.14

**Serial Number:** HADL112720066

**Hardware Version:**

**Firmware Version:** 8.3.7.2

**Software Version:**

**Virtual:**  Not Virtual

**Date created:** 03/02/2012 10:15

**Creator:** admin

**Discovery Date:** 3/2/12 10:15 AM

**Last Modified:** 3/2/12 10:16 AM

**Last Backup:** 3/5/12 1:31 PM

**Last Configuration Change:**

**Service Tag:**

**Asset Tag:**

### Ports

Name	State
ManagementEthernet 0/0	<input checked="" type="checkbox"/>
ManagementEthernet 1/0	<input checked="" type="checkbox"/>
ManagementEthernet 2/0	<input checked="" type="checkbox"/>
ManagementEthernet 3/0	<input checked="" type="checkbox"/>
ManagementEthernet 4/0	<input checked="" type="checkbox"/>
ManagementEthernet 5/0	<input checked="" type="checkbox"/>

### Audit Trail

User ID	Action	Status	Subject
admin	Adaptiv...	<input checked="" type="checkbox"/>	ForceS...
admin	Equipm...	<input checked="" type="checkbox"/>	ForceS...
admin	File Ma...	<input checked="" type="checkbox"/>	ForceS...
admin	Change...	<input checked="" type="checkbox"/>	ForceS...
admin	File Ma...	<input checked="" type="checkbox"/>	ForceS...
admin	Change...	<input checked="" type="checkbox"/>	ForceS...

### Associated Link(s)

Link Name	Link Type
GigabitEthernet 0/47 (Forc...	Ethernet Link

### Latest Configurations

Equi	Fi...	Fi...	Date Saved	V...	Fi...
Text	D...		3/5/12 1:21 PM	1	6...
Text	Pr...		3/5/12 1:31 PM	1	6...

### Reference Tree

- ForceS4810P\_11.10.128.6.11
  - Loopbacks
  - NULL 0
  - Port Channels
  - Slot 0
  - Slot 1
  - Slot 2
  - Slot 3
  - Slot 4
  - Slot 5
  - Slot 6

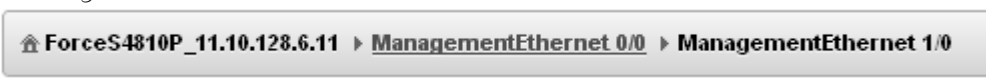
### Monitor Status Summary

Monitor	Target	Last Polled
<input checked="" type="checkbox"/>	ForceS481...	3/6/12 10:41 AM
<input checked="" type="checkbox"/>	Default...	3/5/12 10:39 AM
<input checked="" type="checkbox"/>	Default...	3/6/12 10:39 AM
<input checked="" type="checkbox"/>	ForceS481...	3/5/12 10:39 AM
<input checked="" type="checkbox"/>	Default...	3/6/12 10:40 AM
<input checked="" type="checkbox"/>	NULL 0 (F...	3/5/12 10:38 AM
<input checked="" type="checkbox"/>	Default...	3/6/12 10:41 AM

Details screens are available for a variety of things besides equipment, too. The Equipment Details screen (and others) can have the following sub-panels:

- Performance Indicators
- Interfaces
- Top Configuration Backups (see Top Configuration Backups on page 277)
- Alarms
- Ports
- Details

You can also right-click to open further *Details* screens about some subcomponents like Interfaces and Ports. These display a *Reference Tree* (like Snap Panels (Reference Tree) on page 85) too. You can even right-click nodes in that reference tree to drill down to additional details.



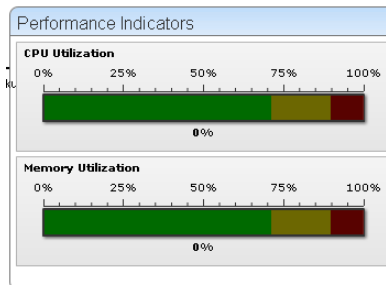
### Tip

Notice the breadcrumb trail at the top of the Equipment Detail panel tracks the levels through which you drill down. You can click a level that appears in this trail to return to a previous screen. If you click *Return to previous* in the upper right corner of the screen, you will return to the original screen from which you selected the basic equipment.

Some fields may be truncated onscreen. Workaround: hover the cursor over the truncated field so the text appears as a tooltip or drill down to see the detail.

## Performance Indicators

These gauges display CPU and Memory Utilization. The numbers indicate percentage of capacity. These rely on Flash.

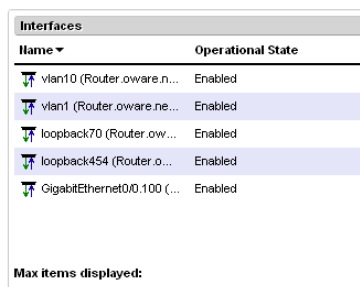


# Interfaces

This panel displays interfaces on the selected device. Notice that you can right-click these to display additional details, or to share this list with another user. You can right-click to *Share* an interface's information, or to open a Interfaces > Details screen.

 **NOTE:**

Some devices populate the ports panel, but not the interfaces panel. This panel is empty for such devices. Interfaces may appear for Force10 Force 10 devices interfaces details can display Port Channels (LAGs), VLANs (SVIs) and Loopbacks.



Name	Operational State
vlan10 (Router.oware.n...	Enabled
vlan1 (Router.oware.ne...	Enabled
loopback70 (Router.ow...	Enabled
loopback454 (Router.o...	Enabled
GigabitEthernet0/0.100 (...)	Enabled

Max items displayed:

## Interfaces > Details

The details available for interfaces can include a *Reference Tree* panel that displays the interface's root equipment and its sub-components. The *Details* panel also appears with the following fields:

**Creator**—The user that created this interface.

**Slot Number**—This interface's type. For example *Loopback*.

**Name**—The interface name.

**Equipment Name**—The name of the equipment that contains the interface.

**Administrative State**—The state of the interface.

**Port Number**—The port for this interface.

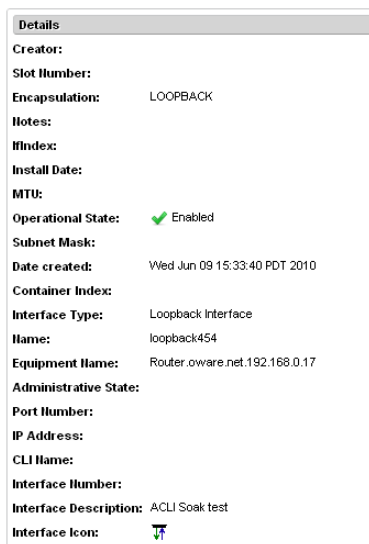
**IP Address**—The interface's IP address.


**CLI Name**—The command line interface name.

**Interface Number**—A numeric identifier for the interface.

**Interface Description**—A text description for the interface.

**Interface Icon**—An icon for the interface.

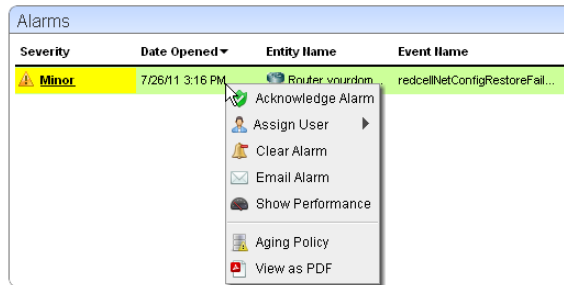


<b>Details</b>	
<b>Creator:</b>	
<b>Slot Number:</b>	
<b>Encapsulation:</b>	LOOPBACK
<b>Notes:</b>	
<b>Index:</b>	
<b>Install Date:</b>	
<b>MTU:</b>	
<b>Operational State:</b>	Enabled
<b>Subnet Mask:</b>	
<b>Date created:</b>	Wed Jun 09 15:33:40 PDT 2010
<b>Container Index:</b>	
<b>Interface Type:</b>	Loopback Interface
<b>Name:</b>	loopback454
<b>Equipment Name:</b>	Router.oware.net:192.168.0.17
<b>Administrative State:</b>	
<b>Port Number:</b>	
<b>IP Address:</b>	
<b>CLI Name:</b>	
<b>Interface Number:</b>	
<b>Interface Description:</b>	ACLI Soak test
<b>Interface Icon:</b>	

# Alarms

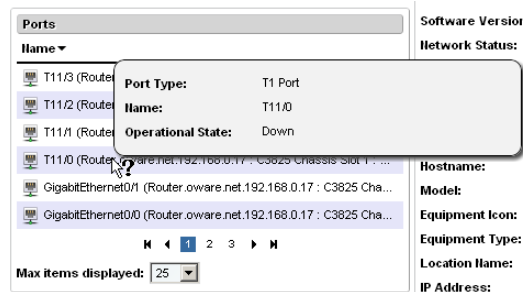
The alarm panel in Equipment Details displays alarms connected to the selected equipment. You can right-click these and *Acknowledge*, *Clear*, or *Email* the selected alarm. You can also *Assign User* and *Share with User*.

Hover the cursor over an alarm and a popup appears with that alarm’s details just as described in Alarms on page 99.



# Ports

This displays the equipment’s ports. If you hover the cursor over a port, you can also see the *Port Type* (for example, Fast Ethernet, T1, and so on), *Name* (port identifier), and *Operational Type* (Up, Down). A column in the summary portlet lists what *Equipment* the port belongs to. The Expanded portlet displays snap panels and additional columns for *Encapsulation*, *IP Address*, *Subnet Mask*, *Port Description*, *8 Date Created*.



## Tip

If the Ports portlet is on the same page as the Managed Resources Proscan portlet, selecting a device in Managed Resources makes its ports appear in the Ports portlet. These can get out of sync, but clicking the browser’s *Refresh* restores the correspondence between a selected device and the ports displayed.

You can also add *Links* to ports with the right-click menu. (See Ports > Links). Existing links appear in the *Reference Tree* snap-in for the selected port in the Expanded Ports portlet. Other snap-ins display port information and any learned MAC address(es) for the port.

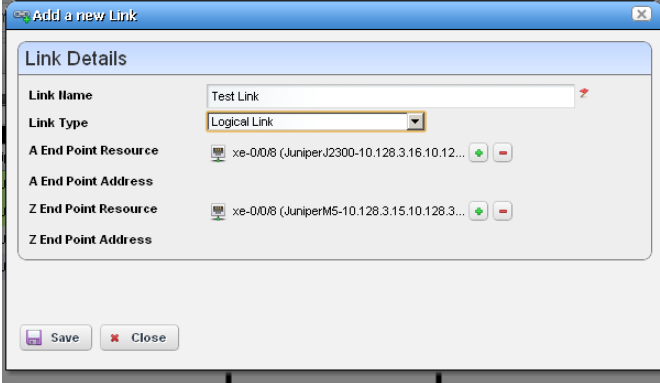
Right-clicking a listed port produces a menu with the following items: *Edit*, *Details*, *Visualize*, *Event Management*, *Links*, *Performance* and *View as PDF*. See Ports on page 191 for more about a portlet exclusively for ports, and Port Editor on page 194 for information about editing them.

## NOTE:

To resync a port, resync the device that contains it.

## Ports > Links

When you add or edit a link, the *Link Details* screen appears.



The screenshot shows a window titled "Add a new Link" with a "Link Details" section. The form contains the following fields:

- Link Name:** A text input field containing "Test Link".
- Link Type:** A dropdown menu with "Logical Link" selected.
- A End Point Resource:** A resource selection field showing "xe-0/0/8 (JuniperJ2300-10.128.3.16.10.12...".
- A End Point Address:** An empty text input field.
- Z End Point Resource:** A resource selection field showing "ve-0/0/8 (JuniperM5-10.128.3.15.10.128.3...".
- Z End Point Address:** An empty text input field.

At the bottom of the dialog are "Save" and "Close" buttons.

It contains the following fields:

**Link Name**—An identifier for the link

**Link Type**—Select the type of link to create in the pick list.

**A / Z Endpoint Resource**—Select a resource for the A or Z endpoint

**A / Z Endpoint Address**—The IP address, if available, for the endpoint.

Click *Save* to preserve your edits, or *Close* to abandon them.

## Ports > Details

You can right-click to *Share* port information, or to open a *Details* screen for the selected port. This includes the device's *Reference Tree* so you can see this port in relation to other parts of the device. It also includes a *Details* panel that can include the following fields:

**Hardware Version**—The port's hardware version

**Port Description**—A text description of the port.

**Model**—A model number.

**Date created**—When the port was discovered.

**Creator**—The logged-in user who discovered it.

**Port Type**—The port's type (T1, Fast Ethernet, and so on).

**Encapsulation**—The port's encapsulation.

**Subnet Mask**—The port's subnet mask.

**Install Date**—The port's installation date.

**In Use**—An indicator use.

**IF Index**—The SNMP MIB designation for the port.

**Container Index**—The SNMP MIB designation for the port's container.

**Slot Number**—The port's slot number.

**Speed**—The port's speed.

**MTU**—The port's MTU.

**Port Icon**—The port's configured icon.

**Learned MAC Addr**—The port's learned MAC address.

**Count**—The port's count.

**CLI Name**—The port's command line interface name.

**Notes**—Any notes recorded about the port.

**Operation Type**—The port's operation type.

**Switch Mode**—Is the port in switch mode?


**Duplex**—Is the port in duplex mode?

**Name**—The port's name.

**Port Number**—The port's number.

**Equipment Name**—The port's equipment name.

**Operational State**—One of following possible values describing the availability of the resource.

Details	
Hardware Version:	
Port Description:	
Model:	
Date created:	
Creator:	
Port Type:	T1 Port
Encapsulation:	
Subnet Mask:	
Install Date:	
In Use:	 Not In Use
IF Index:	
Container Index:	
Slot Number:	
Speed:	
MTU:	
Port Icon:	
Learned MAC Addr:	
Count:	
CLI Name:	
Notes:	
Operation Type:	
Switch Mode:	
Duplex:	
Name:	T11/3
Port Number:	
Equipment Name:	
Operational State:	Down
IP Address:	
MAC Address:	
Administrative State:	

*Disabled*—Inoperable because of a fault, or resources are unavailable.

*Enabled*—Operable and available for use.

*Active*—Device is operable and currently in use with operating capacity available to support further services.

*Busy*—Operable and currently in use with no operating capacity to spare.

**IP Address**—The port's IP address

**Hardware Version**—The port's hardware version

**MAC Address**—The port's Media Access Control (MAC) address.

**Administrative State**—One of the following values:

*Locked*—Device use is prohibited.

*Shutting Down*—Only existing users can use the device.

*Unlocked*—Normal use of device is permitted.



## Details

This panel displays detailed information about the equipment selected. This can include the following fields:

**Serial Number**—The selected resource’s serial number.

**Last Configuration**—The date for the last backed-up configuration file.

**Change**—The date for the last configuration file change.

**System Object ID**—The SysObjectID of the resource.

**Operational State**—One of following possible values, selected from a drop-down menu, describing the availability of the resource.

*Disabled*—Inoperable because of a fault, or resources are unavailable.

*Enabled*—Operable and available for use.

*Active*—Device is operable and currently in use with operating capacity available to support further services.

*Busy*—Operable and currently in use with no operating capacity to spare.

**Install Date**—The date this equipment was installed.

**Notes**—Any notes recorded about the device.

**RTM Category**—The “Right to Manage” category for licensing.


**DNS Hostname**—The DNS name of the resource; this name must be unique.

**Vendor**—The vendor that manufactures/distributes this resource. See the Vendors on page 139 for more information about managing vendors.

**Hardware Version**—This resource’s hardware version.

**Software Version**—The selected resource’s software version.

**Network Status**—The status of the resource in the network. For example: *Responding* means this application can, via some network protocol, get the device to respond. *Not Responding* means the device does not respond to the protocol. *Indeterminate* means the monitoring software has not tried to reach the device or there was some other error which prevented us from determining one of the other two statuses.

Details	
<b>Serial Number:</b>	FTX0916A2H5
<b>Last Configuration Change:</b>	
<b>System Object Id:</b>	1.3.6.1.4.1.9.1.543
<b>Operational State:</b>	✔ Enabled
<b>Install Date:</b>	
<b>Notes:</b>	
<b>RTM Category:</b>	Router
<b>DIS Hostname:</b>	
<b>Vendor Name:</b>	
<b>Hardware Version:</b>	
<b>Software Version:</b>	12.4(7)
<b>Network Status:</b>	● Responding
<b>Creator:</b>	admin
<b>Firmware Version:</b>	12.4(7)
<b>Backup Result:</b>	
<b>Manage By:</b>	False
<b>Hostname:</b>	
<b>Model:</b>	3825
<b>Equipment Icon:</b>	
<b>Equipment Type:</b>	Router
<b>Location Name:</b>	
<b>IP Address:</b>	192.168.0.17
<b>Discovery Date:</b>	06/09/10 02:12 PM
<b>Administrative State:</b>	🔓 Unlocked
<b>Hardware Version:</b>	V01
<b>Last Backup:</b>	07/13/10 04:46 PM
<b>Last Modified:</b>	06/09/10 03:33 PM
<b>Equipment Name:</b>	Router.oware.net.192.168.0.17
<b>Alarm Severity:</b>	
<b>Restore Result:</b>	
<b>Description:</b>	Cisco IOS Software, 3800 Software (C3825-ADVENTERPRISEK9-M), Version 12.4(7), RELEASE SOFTWARE (fc6) Technical Support: <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> Copyright (c) 1986-2006 by Cisco

The appearance of *Network Status* depends on the default ICMP monitor (see Resource Monitors on page 245. If you exclude this equipment from the monitor or disable it (for example, for performance reasons) then a status may appear, but it is not meaningful.

**Creator**—The logged in user that created this record in the database.

**Firmware Version**—This resource's firmware version.

**Backup Result**—The result of any attempted configuration file backup for this resource.

**Managed By Hostname**—True/false. True means DNS rather IP address is how OpenManage Network Manager manages this resources.

**Model**—The resource's model number.

**Equipment Icon**—The resource's icon (typically related to the Vendor).

**Equipment Type**—The resource's type. For example *Router*.

**Location Name**—The resource's location.

**IP Address**—The resource's IP address.

**Discovery Date**—When the resource was discovered.

**Administrative State**—One of three descriptive values. The options are:

**Locked**—Device use is prohibited.

**Shutting Down**—Only existing users can use the device.

**Unlocked**—Normal use of device is permitted.

**Hardware Version**—The resource's hardware version.

**Last Backup**—When the resource's configuration was last backed up.

**Last Modified**—When the resource's configuration was last modified.

**Equipment Name**—The resource's name on the network.

**Alarm Severity**—The most severe alarm on the resource.

**Restore Result**—The result of any attempted restoration of configuration for this resource.

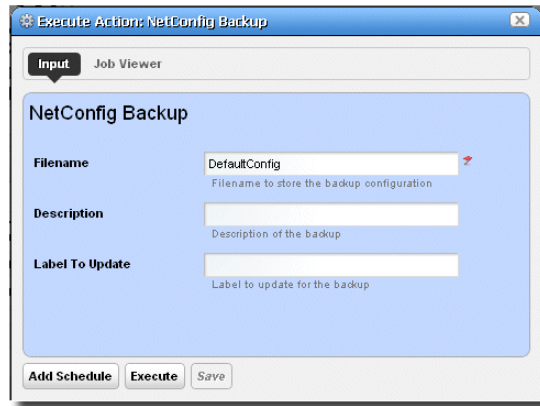
**Description**—A text description of the device.



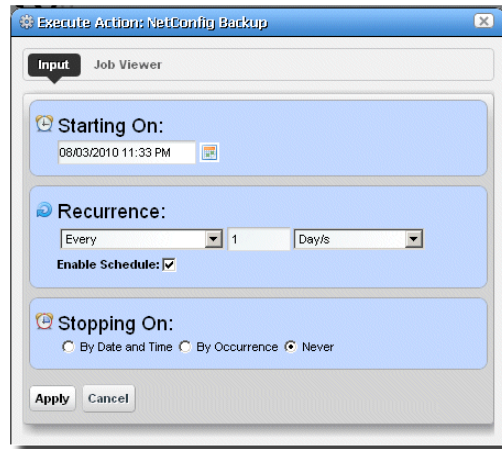
## How To: Schedule Actions

To schedule an action triggered from a right-click menu (for example from Managed Resources) rather than execute it immediately, follow these steps.

- 1 Select the action in the right-click menu. For example: Netconfig Backup.



- 2 Rather than clicking *Execute*, click *Add Schedule*.
- 3 The schedule panel appears.



- 4 Once you click *Apply* on this panel, the previous panel returns, the *Add Schedule* button now appearing as *Edit Schedule*.
- 5 If you click *Save*, Dell OpenManage Network Manager creates a scheduled item around the activity and its data. A row also appears in the screen described in Schedules Portlet on page 95 for this schedule.
- 6 When you have scheduled something from the *Add Schedule* button, clicking *Apply* in the schedule panel returns you to the previous screen.
- 7 If you click *Execute* in that previous screen, the action begins, and audit trail panel appears, displaying the running job for the activity. If you have attached a Schedule, Dell OpenManage Network Manager also saves the activity as a scheduled item in the Schedules Portlet.

# Direct Access

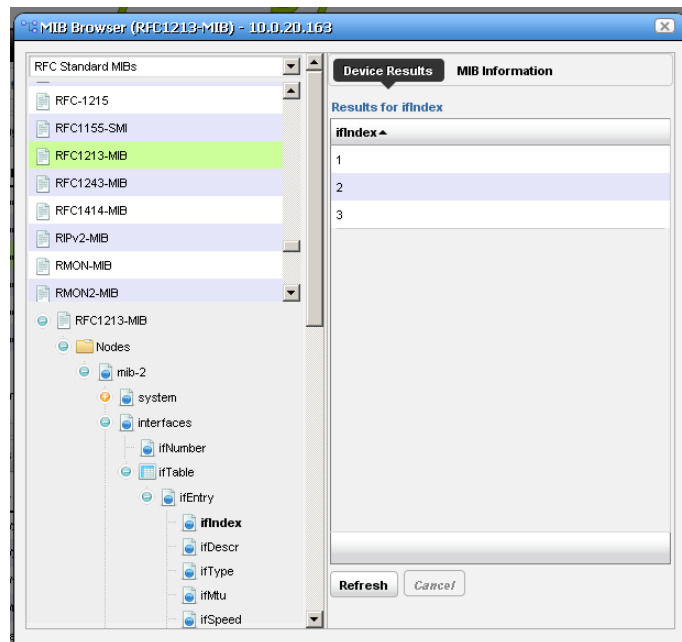
Direct access provides less-mediated access to the device in the following ways:

- MIB Browser
- Terminal
- Ping (ICMP)
- 

The following sections describe those direct options in more detail.

## MIB Browser

As part of the *Direct Access* menu, the *MIB Browser* lets you examine SNMP data available about devices.

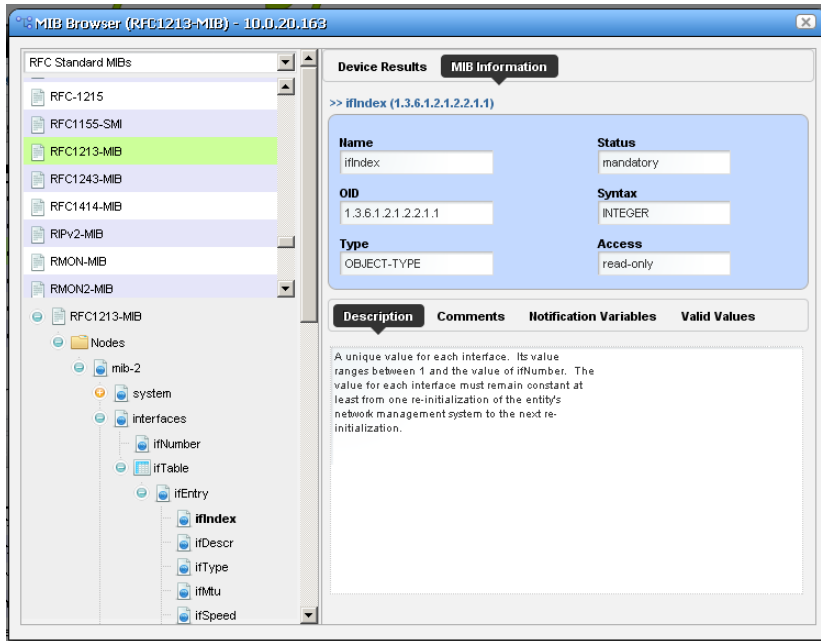


The screen that opens when you select this option displays MIBs available in Dell OpenManage Network Manager in a tree on the left. Notice that a pick list at the top of the left column narrows what appears in the tree.

 **NOTE:**

A progress bar at the bottom of this screen indicates a query for the selected information is in progress. Use the menu described in Event Definitions on page 128 for loading new MIBs.

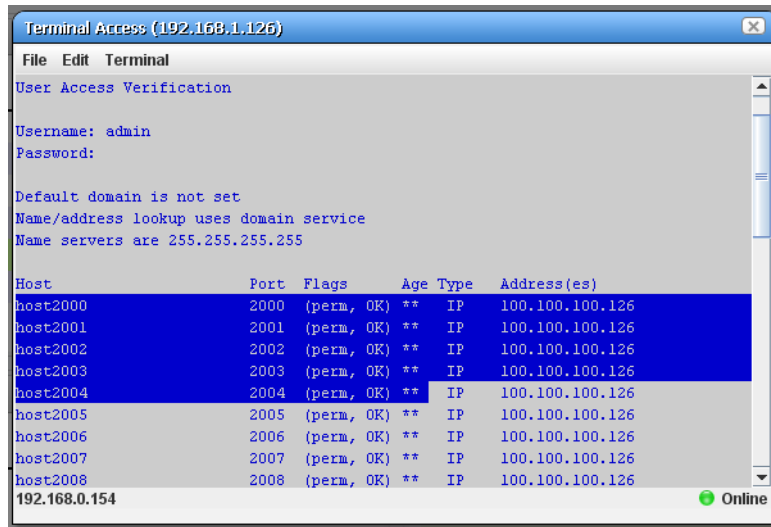
Select a MIB and expand it to see the contents for a selected node appear on the right. In addition to the *Device Results* tab, which displays what the currently selected device uses from the MIB, the *MIB Information* tab displays the parameters available for the selected node.



Notice that the *Description*, *Comments*, *Notification Variables*, and *Valid Values* tabs appear at the bottom of this screen.

# Terminal

This opens a terminal shell connected to the selected device.



A green icon in the lower right corner indicates the device is online, while the IP address of the device appears in title bar. The IP address of Dell OpenManage Network Manager’s server also appears in the lower left corner, when the connection is active.

The following menus appear for your terminal session:


**File**—This menu lets you *Connect* or *Disconnect* to the device.

**Edit**—This menu lets you *Copy* or *Paste* text within the terminal session. Click and drag to select text.

**Terminal**—This menu lets you set *Foreground* and *Background* colors, as well as configuring the *Font* and *Buffer* sizes. *Reset Terminal* restores the defaults.

 **NOTE:**

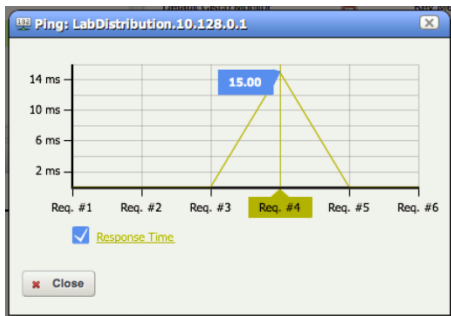
Terminal is now an applet that requires a Java Runtime Environment be installed and associated to the browser as a plug-in on the client machine.

 **Tip**

You can cut and paste from the Direct Access terminal.

Telnet sessions are synchronous. You cannot interrupt a command in progress with another command you send, unless you have enabled something that periodically prompts for additional commands (for example enabling line continuation prompts).

## Ping (ICMP)



Select this option from the Direct Access menu to initiate ICMP ping, and to display a progress bar, and graph of the selected device's ping responses.

Alternatively, an error message can appear describing the device's lack of response.

When ping responds in less than one millisecond, results appear in a table with < 1ms entries.

## HTTP / HTTPS

Selecting this menu item opens the default browser, connected to the selected device.

An intervening dialog appears advising you about the required network conditions for a successful connection.



## Ports

This summary portlet displays discovered device ports.

Name	Equipment	Port Type	State
lo0	JuniperJ2300-10.128.3.16.10	Other	✓
irb			✓
ip-0/0/0			✓
gr-0/0/0			✓
ge-0/0/3	JuniperJ2300-10.128.3.16.10...	Gigabit Ethernet Port	✓
ge-0/0/2	JuniperJ2300-10.128.3.16.10...	Gigabit Ethernet Port	✓

This displays a list of ports, with columns for *Port Icon*, *Equipment Name*, *Name*, *Type* and *Encapsulation*. Hover your cursor over the **Name** column, and a popup appears adding the port's *Date Created* and *Operational State* information. Right-clicking offers a subset of the actions listed in Managed Resources on page 166. You can also create links. See Ports > Links on page 182. See Port Editor on page 194 for details of the editor specifically for ports.

## Port Details

This screen displays all the port's settings that have been retrieved, including a Reference Tree of logical interfaces below the port, a Learned MAC Address panel, Alarms related to the port, and other Details.

**Reference Tree**

- FastEthernet4/0
  - FastEthernet4/0.10
  - FastEthernet4/0.11
  - FastEthernet4/0.21

**Alarms**

Date Opened	Entity Name	Device IP
No data is available to display		

Max items returned: 25

**Learned MAC Address**

Learned MAC Addr...	Last Observed
No data is available to display	

**Learned MAC Address Details:**

- Hardware Version:
- Port Description:
- Model:
- Date created: Fri Sep 10 10:29:14 PDT 2010
- Creator: Cisco Device Driver
- Port Type: Fast Ethernet Port
- Encapsulation: 802.1Q Virtual LAN
- Subnet Mask: 255.255.255.240
- Install Date: Not Available
- In Use: Not In Use
- If Index: 6
- Container Index: 0
- Slot Number: 4
- Speed: 100000000
- MTU: 1500
- Port Icon:
- Learned MAC Addr Count: 0
- CLI Name: FastEthernet4/0
- Notes:
- Operation Type: Routed
- Switch Mode: Not Applicable
- Duplex: Half
- Name: FastEthernet4/0
- Port Number: 0
- Equipment Name: Router.10.128.2.135
- Operational State: Down
- IP Address: 10.80.1.2
- MAC Address: 00307b542070
- Administrative State: Down

In Details, fields describing the following for the selected port: *Hardware Version, Port Description, Model, Date Created* (typically, this is the date discovered), *Creator, Port Type, Encapsulation, Subnet Mask, Install Date, In Use, If Index, Container Index, Slot Number, Speed, MTU* (maximum transmission unit), *Port Icon, Learned MAC Addr, Count, CLI Name, Notes, Operation Type, Switch Mode, Duplex, Name, Port Number, Equipment Name, Operational State, IP Address, MAC address, Administrative State*. See Port Details on page 192 and Managed Resources Expanded on page 173 for an explanation of some of these fields.



## Ports Expanded

Clicking the plus (+) in the upper right corner of the summary screen displays this expanded view of available ports.

The screenshot displays the 'Ports' expanded view. At the top, there is a 'Default Port Filter' dropdown and an 'Advanced Filter' button. A search bar, refresh button, and settings icon are also present. The main table lists the following ports:

Name	Equipment	Port Type	Encapsulation	IP Address	Subnet Mask	State	Port Description	Date created
at-0/0/0	M5 JuniperMS-10...	ATM Port	ATM-PVC			✖		Mon Aug 15 09:01:...
at-0/0/1	M5 JuniperMS-10...	ATM Port	ATM-PVC			✖		Mon Aug 15 09:01:...
e1-0/0/0	JuniperJ2300-...	Other	ppp			✔	created by Sally M...	Mon Aug 15 09:02:...
e1-0/0/1	JuniperJ2300-...	Other	ppp			✔		Mon Aug 15 09:02:...
fe-0/1/0	M5 JuniperMS-10...	Fast Ethernet Port	Ethernet			✔		Mon Aug 15 09:01:...
fe-0/1/1	M5 JuniperMS-10...	Fast Ethernet Port	Ethernet			✔		Mon Aug 15 09:01:...
fe-0/1/2	M5 JuniperMS-10...	Fast Ethernet Port	vlan-ccc			✔		Mon Aug 15 09:01:...
fe-0/1/3	M5 JuniperMS-10...	Fast Ethernet Port	Ethernet			✖		Mon Aug 15 09:01:...

Below the table, there are three panels:

- Reference Tree:** A tree view showing the hierarchy of interfaces. The selected port 'fe-0/1/2' is highlighted in blue. Other visible nodes include fe-0/1/2.512, fe-0/1/2.513, fe-0/1/2.514, fe-0/1/2.515, fe-0/1/2.516, and fe-0/1/2.517.
- Model:** Displays details for the selected port: NAME: fe-0/1/2, MODEL: 4x F/E, 100 BASE-TX, MAC ADDRESS: 0090696atc21.
- Learned MAC Address:** A table with columns 'Learned MAC Address', 'ID', and 'Last Observed'. It currently displays 'No data is available to display'.

At the bottom right, there are buttons for 'Snap Panels' and 'Close'.

The *Settings* button lets you configure columns that appear and their order. The available columns for this view include many related to the attributes that appear in Port Details on page 192, above. This screen also includes a *Reference Tree* displaying a tree of the selected port's relationship to logical interfaces and monitors.

## Port Editor

When you right-click a port, and select *Edit* this screen appears.

It has the following fields:

### General Details

**Name**—An identifier for the port.

**Port Description**—A text description for the port.

**Install Date**—The date this port was installed.

**Model**—The port's model.

**Date created**—The date this port was created.

### Port Details - Properties

**IP Address**—The IP address for the port.

**MAC Address**—The port's Media Access Control (MAC) address.

**Hardware Version**—The port's hardware version.

**Port Type**—The type of port.

**Administrative State**—One of three descriptive values. The options are:

*Locked*—Device use is prohibited.

*Shutting Down*—Only existing users can use the device.

*Unlocked*—Normal use of device is permitted.

**Operational State**—One of the following values:

*Down*—Inoperable because of a fault, or resources are unavailable.

*Dormant*—The port is dormant.

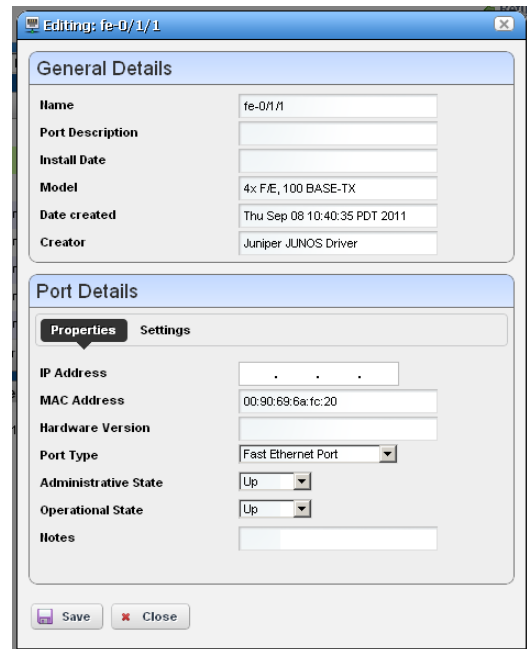
*Not Present*—The port is absent.

*Up*—Operable and available for use.

*Unknown*—Status is unknown.

*Testing*—Status is testing.

**Notes**—Any notes recorded about the device.



The screenshot shows a window titled "Editing: fe-0/1/1". It is divided into two main sections: "General Details" and "Port Details".

**General Details:**

- Name: fe-0/1/1
- Port Description: (empty text box)
- Install Date: (empty text box)
- Model: 4x FE, 100 BASE-TX
- Date created: Thu Sep 08 10:40:35 PDT 2011
- Creator: Juniper JUNOS Driver

**Port Details:**

There are two tabs: "Properties" (selected) and "Settings".

- IP Address: (empty text box)
- MAC Address: 00:90:69:6a:fc:20
- Hardware Version: (empty text box)
- Port Type: Fast Ethernet Port (dropdown menu)
- Administrative State: Up (dropdown menu)
- Operational State: Up (dropdown menu)
- Notes: (empty text box)

At the bottom of the window are "Save" and "Close" buttons.

## Port Details - Settings

**Encapsulation**—An identifier for the port.

**MTU**—The size of the maximum transmission unit.

**Speed**—The port's speed.

**Subnet Mask**—Any subnet mask associated with the port.

**In Use** —Checked if the port is in use.

**IF Index**—The port's SNMP If Index number.



**NOTE:**

The polling frequency is once-an-hour. This is not configurable.

# Report Templates

Report Templates are the basis of reports. This portlet displays the *Template Name*, *Description*, and *Type* in columns.

Right-clicking in this portlet lets you create a *New* template, *Edit* a selected template (see Report Template Editors for information about subsequent screens), view *Details* or *Delete* a selected template. You can also *Import* / *Export* report templates to files.

Template Name	Description	Type
Subnet Template	Default Template for Subnets	Table
Software Inventory Change Template	Default Template for Software Inventor...	Table
Port Template	Default Template for Ports	Table
Pool Template	Pool Statistics	Table
Pool Allocation Template	Allocation Report Template	Table
Netconfig Backup Template	Default NetConfig Backup Template	Table

The expanded Report Templates portlet also includes a Reference Tree snap panel displaying a tree for selected templates connecting them to Report Groups and specific reports.



## How To:

### Create a Report Template

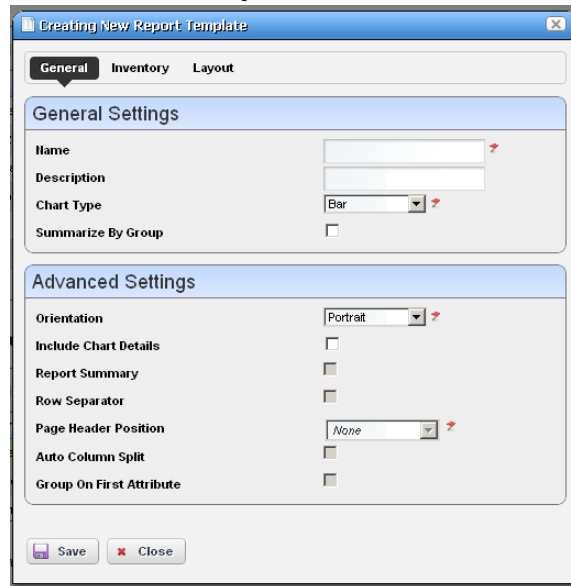
The following steps create a report template:

- 1 In the Report Templates portlet, right-click and select *New* Table template.
- 2 Name the template (for example: Test Amigopod Report)
- 3 In the *Source* tab, select an inventory source (for example: Inventory resources [A - DD] Amigopod).

- 4 Select *Inventory Columns* by clicking the arrow(s) between *Available* and *Selected* columns. (for example: Amigopod: Administrative State, Amigopod: DNS Hostname, Amigopod: Equipment Name, Amigopod:IP Address)
- 5 In the *Layout* tab, configure the column order (top is first, bottom is last).
- 6 Notice you can also configure the font size, color, alignment, and so on when you select a column in this tab.
- 7 Click *Save*. You have successfully created a template.

## Report Template Editors

Dell OpenManage Network Manager has several report template editors. Creating a *New* template, can make *Comparison*, *Table* and *Trend* templates.



This editor has General, Inventory, and Layout tabs.

You can edit any but pre-existing templates, whether they have reports attached to them or not. Consider this example:

Template T has three columns; A, B and C. Someone creates a report R against Template T, executes the report, saves the data as a historical report H1. Two weeks later, someone modifies the Template T, removing column C, adding column D.

When executing report R against the revised Template T', the report now shows columns A, B and D. User saves the report as historical report H2. Here, H1 only has data for columns A, B and C. H2 has data for columns A, B and D.

If you view H1 you see Template T' is in use and this template creates a report with columns A, B and D. Unfortunately, H1 only has data for columns A, B and C, so the report created has data for columns A and B only. Column D is empty. When viewing H2 you can see Template T' is in use and can create a report with columns A, B and D. H2 has data for columns A, B and D, so all data appears.

## General

The following are fields that appear on these screens. Not all screens have all fields.

### General Settings

**Name**—An identifier for the template.

**Description**—An optional description of the template.

**Chart Type**—Select from the available alternatives (*column, line*).

**Summarize by Group**—Group similar results together.

### Advanced Settings

**Orientation**—Select from *Portrait* and *Landscape*

**Include Chart Details**—Enables the following fields

**Report Summary**—Enable a report summary

**Row Separator**—Display a row separator.

**Page Header Position**—Select *none, top, bottom* or *both*.

**Auto Column Split**—Enable automatic column splitting. This automatically aligns the columns equally on the report providing the column widths that are most proportional.

**Group on First Attribute**—Create a report that groups rows based on the first reported attribute. This creates groups of items in the report whenever the left most column's value changes.

For example, with disabled, a report looks like this:

Device Name	Gig/e Port Name	Health Status
M5	ge/0/0/1	Up
M5	ge/0/0/2	Down
M5	ge/0/0/3	Up
M5	ge/0/0/4	Unknown
M18	ge/0/1/1	Up
M18	ge/0/1/2	Starting
M18	ge/0/1/3	Up

M18                    ge/0/1/4                    Down

The same report looks like this with *Group on First Attribute* enabled:

Device Name   Gig/e Port Name   Health Status

M5

	ge/0/0/1	Up
	ge/0/0/2	Down
	ge/0/0/3	Up
	ge/0/0/4	Unknown

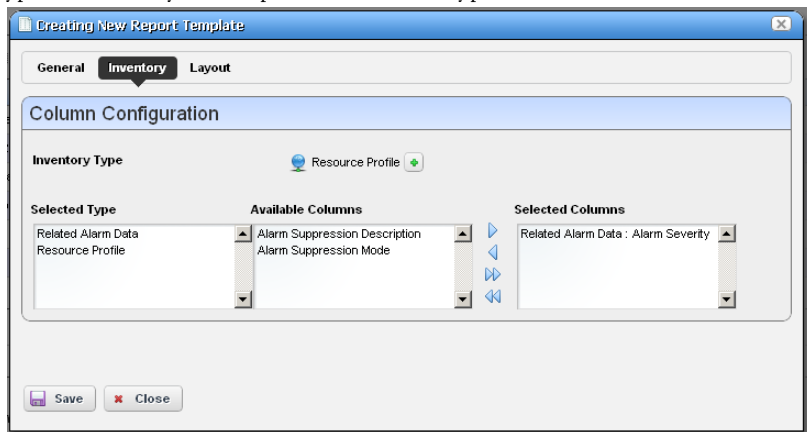
M18

	ge/0/1/1	Up
	ge/0/1/2	Starting
	ge/0/1/3	Up
	ge/0/1/4	Down

The Inventory and Layout tabs are common to all editors.

## Inventory

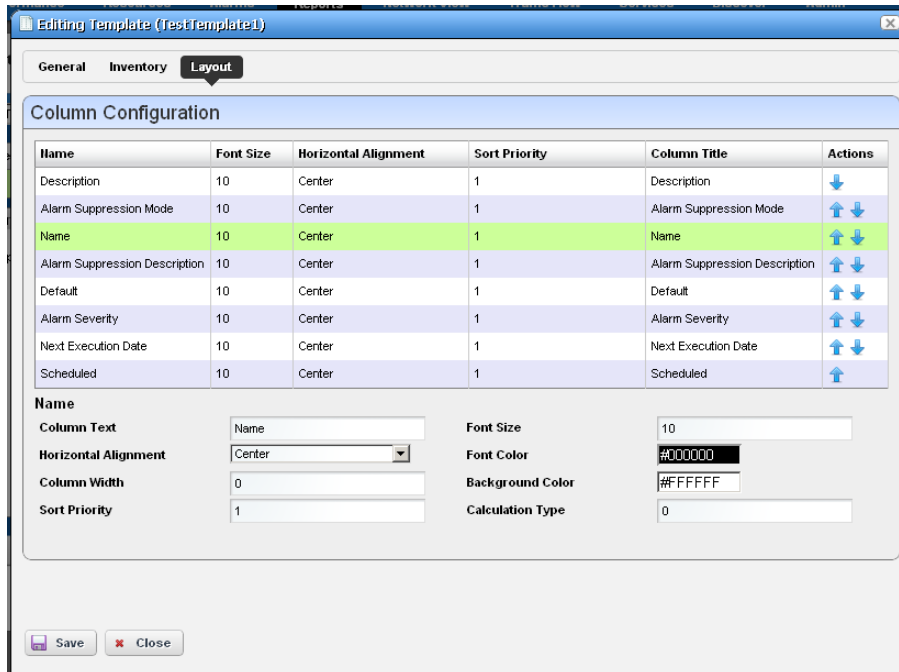
Select the type of inventory for a report, and its data types in this screen.



Click the green plus (+) to select the *Inventory Type*. The types of data available for that inventory type appear in the leftmost column in this screen. Click on a *Selected Type* to see its *Available Columns*. Click the arrows to move columns from *Available* to *Selected*. The *Selected Columns* appear in the template's report.

## Layout

This tab outlines the column layout for the template.



Click on the up/down arrows on the right of each row to re-order data columns. Click to select a row, and the editor panel at the bottom of the screen appears. It has the following fields:

**Column Text**—The column label.

**Horizontal Alignment**—*Right, Left, Center* (the default).

**Column Width**—The column width in characters.

**Sort Priority**—Configures report sorting. Define the attribute sort order here. You can sort within a sort, so you can sort on Name and then by Location and then by IP Address, and so on. The number configures the sort group, so 1 sorts, then 2 within 1, then 3, and so on.

**Font Size**—The data's font size.

**Font / Background Color**—The color for the text/background. Click the field to open a color chooser.

**Calculation Type**—How to calculate for summarizing the numeric data. Select from the available options (*Average, High, Low, Sum*).

Click *Save* to preserve any template you have configured, or *Close* to close the editor screens without saving.

## Reports

This portlet's summary screen lists the available reports that you can run with Dell OpenManage Network Manager.

Report Name	Report Template	Title
Software Change Report	Software Inventory Change Templ...	Software Inventory Change Report
Juniper ISIS Information	Juniper ISIS Template	ISIS
Juniper Bootp Interfaces	Juniper Bootp Interface Template	Bootp Interfaces
Juniper Bootp	Juniper Bootp Template	Bootp Servers
Juniper BGP Information	Juniper BGP Template	BGP
Juniper BGP Groups	Juniper BGP Group Template	BGP Groups

The report *Icon, Name, Template,* and *Subtitle* appear in the columns in this summary screen. Generally speaking, the report selects the target equipment, and the template configures the layout and attributes reported.

 **NOTE:**

If the Interface details panel is empty, then the Interface reports will have no contents. Some devices have ports, but no interfaces. Use the Ports report for such devices.

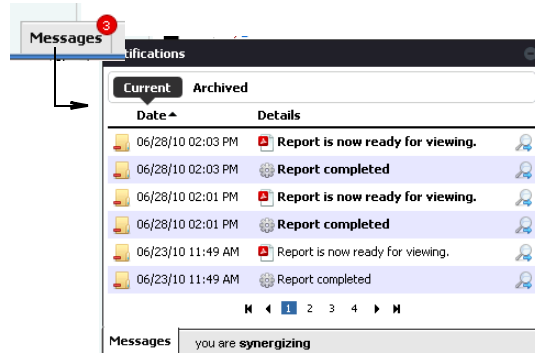
Right-click a selected report to do the following:

**New / Edit / Copy** — This opens the Report Editor, described below, to configure a new report, edit or copy an existing, selected report. *Copy* automatically renames the selected report.

**Schedule**— Opens a scheduler screen to automate report creation.



**Execute Report**—When you execute a report, a numbered message notification appears, and a link to the report appears in the *Messages* panel to notify you the report is ready for viewing. Click the magnifying glass to the right of the notification to view either the audit trail or the report.



**NOTE:**

Reports with lots of data may take a long time to appear without much indication that they are in process. This is an artifact of the Acrobat plug-in, and outside the scope of Dell OpenManage Network Manager to influence. Acrobat also produces an error if a report has too much data to display meaningfully.

**Execute Report (Advanced)**—Also lets you schedule reports.

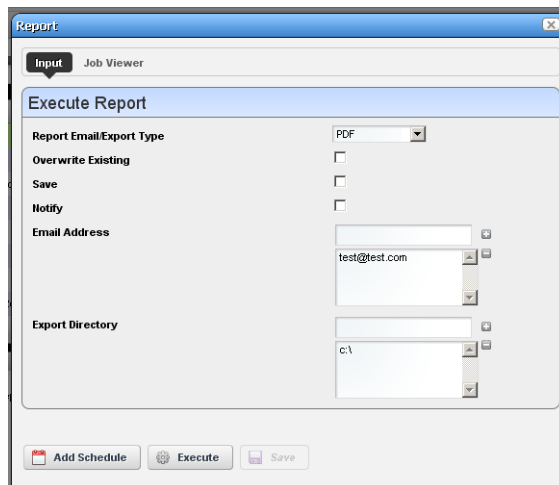
**Aging Policy**—If you automate report generation, you may also want to configure a Database Aging Policy to insure the volume of reports does not overwhelm your storage capacity. See Redcell > Database Aging Policies (DAP) on page 50 for more about doing that.

**Delete**—Removes the selected report from the list display

**Delete History**—Removes the selected report’s history.

To change reports’ appearance and contents, you must configure their Report Templates. Also, see Branding Reports on page 206 for instructions about changing the default report logo.

When you *View or Execute Report (Advanced)*, by right clicking either a listed report or a historical instance of that report, a configuration screen appears that lets you select several parameters.



These include the following:

**Report Email / Export Type**—Select the export file type from the pick list. Options include *CSV*, *HTML*, *PDF*, *XLS*, and *XLSM*.

**Overwrite Existing**—Check to activate overwriting any existing report.

**Save**—Check to activate saving the report to the database.

**Notify**—Check to activate emitting a notification event.

**Email Address**—Enter an e-mail destination for the generated report, and click the plus (+) to list it. You can enter several such e-mails.

**Export Directory**—Enter directory destinations for saved reports as you would e-mail destinations.x

Click *Add Schedule* to schedule the report for future or repeated execution, *Execute* to run the report immediately, or *Save* to preserve this report's configuration. The *Job Viewer* tab displays the report's progress if you click *Execute*.

## Expanded Reports Portlet

Clicking the plus (+) icon displays the expanded portlet, which adds *Add / Remove Column* to the menu options available in the summary screen.

The screenshot shows the 'Reports' portlet interface. At the top, there is a 'User Filter' dropdown, an 'Advanced Filter' button, and a 'Return to previous' link. Below this is a table with three columns: 'Report Name', 'Report Template', and 'Title'. The table lists several reports, with 'Juniper LDP Information' highlighted in green. Below the table, it indicates '16 item(s) returned' and shows pagination controls. At the bottom, there are two snap panels: 'Reference Tree' and 'Report History'. The 'Reference Tree' shows a tree structure with 'Juniper LDP Information' selected. The 'Report History' panel displays a table with columns for 'Run Date', 'Row Count', 'User', and 'Version', showing a single entry for '8/1/11 10:42 AM' with a row count of 0, run by 'admin', and version 1.

Report Name	Report Template	Title
Juniper BGP Groups	Juniper BGP Group Template	BGP Groups
Juniper BGP Information	Juniper BGP Template	BGP
Juniper Bootp	Juniper Bootp Template	Bootp Servers
Juniper Bootp Interfaces	Juniper Bootp Interface Template	Bootp Interfaces
Juniper ISIS Information	Juniper ISIS Template	ISIS
Juniper ISIS Interfaces	Juniper ISIS Interface Template	ISIS Interfaces
Juniper LDP Information	Juniper LDP Template	LDP
Juniper LDP Interfaces	Juniper LDP Interface Template	LDP Interfaces

Run Date	Row Count	User	Version
8/1/11 10:42 AM	0	admin	1

Available columns are the same as the summary screen's. The *Reference Tree* snap panel displays the selected report's connection to devices, historical reports and any report template. Right-click to view the reports in the Historical Reports node.

## Reports Snap Panels

The Snap Panels for reports display a Reference Tree of connections between the selected report and target equipment, and between the report and any Report Template.

The *Report History* Snap Panel displays the selected report's *Run Date*, *Row Count* and the *User* who ran the report. Right-click a row in this panel, and you can *Delete*, *Print* (the report history) or *Export* (the report history), *View* (the report) or *View (Advanced)*. If you *View* the report, a message with a link to the report appears in the bottom left of the screen.



## How To:

### Generate a Report

The following steps configure, then generate, a report.

- 1 In the Reports portlet, right-click and select *New*.
- 2 *Name* the report (for example: Test Powerconnect Router Report)
- 3 Enter a title / subtitle for the report (“Powerconnect Routers”)
- 4 Select a template for the report in the pick list. (For example, the template configured in How to: Create a Report Template.)



#### Tip

If you create a template, the first report you create after making that template automatically selects the newly created template.

- 5 In the *Filters* tab, you can create a filter to confine the reports input to certain devices, locations, and so on. (Here, select the existing All Powerconnect Routers filter)
- 6 Click *Save*.
- 7 Locate the newly created report in the Reports portlet.
- 8 Right-click and select *Execute*.
- 9 Click the *My Alerts* panel in the lower left corner of the portal.
- 10 Click the magnifying glass icon to the right of the *Report is now ready for viewing* message.
- 11 The report appears onscreen.
- 12 Hover your cursor over the lower right corner of the report to see a set of icons that let you expand, zoom out and in, save, or print the report.



#### NOTE:

Some reports may appear pre-seeded in the portlet that are not supported by your package. For example, pool reports may appear for programmatic restrictions on pooled assets like IP addresses, or Route Targets not supported.

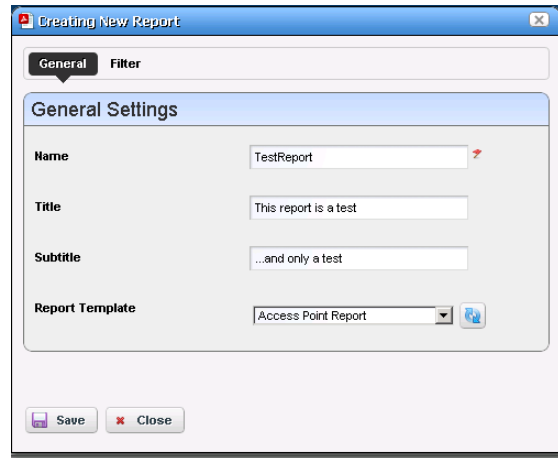
## Report Editor

This editor configures reports, and their targets. It has the following screens and fields:

- General
- Filter

## General

This screen configures the *Name*, *Title* (displayed text in the report), *Subtitle*, and lets you select the *Report Template* for the report (see Report Templates on page 195 for more about them)



The screenshot shows a window titled "Creating New Report" with a "General" tab selected. The "General Settings" section contains the following fields:

- Name:** Text input field containing "TestReport".
- Title:** Text input field containing "This report is a test".
- Subtitle:** Text input field containing "...and only a test".
- Report Template:** A dropdown menu showing "Access Point Report" with a blue icon to its right.

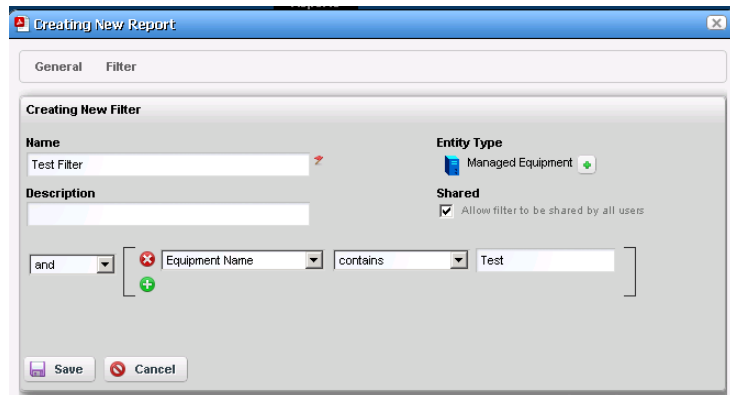
At the bottom of the dialog are "Save" and "Close" buttons.

## Filter

This screen configures a filter to retrieve devices that are the source of the report.

Click *Add Filter* in the filter panel to select an existing filter, create a new filter, or copy an existing filter. When you create a new filter, you must enter a *Name* and optionally a *Description* for it, select an *Entity Type* with the green plus (+), and elect whether this filter is

available to other users (*Shared*). See How to: Filter Expanded Portlet Displays on page 85 for instructions about configuring the filter itself in the lower portion of this screen.



The screenshot shows the "Filter" tab of the "Creating New Report" dialog. The "Creating New Filter" section includes:

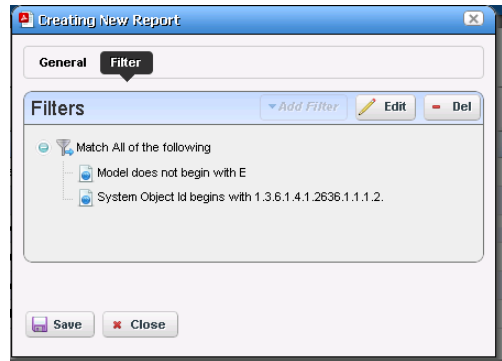
- Name:** Text input field containing "Test Filter".
- Description:** Text input field.
- Entity Type:** A dropdown menu showing "Managed Equipment" with a green plus (+) icon to its right.
- Shared:** A checked checkbox with the label "Allow filter to be shared by all users".
- Filter Rule:** A visual representation of a filter rule: "and" (dropdown) followed by a list of conditions: "Equipment Name" (dropdown) "contains" (dropdown) "Test" (text input). A green plus (+) icon is to the left of the list, and a red minus (-) icon is to the right.

At the bottom are "Save" and "Cancel" buttons.

Once you have configured or selected a filter, the *Filter* panel displays its characteristics in tree form. Click *Edit* to re-open the editor, or *Del* to remove the filter.

 **NOTE:**

Filters appear only for the entity type of your Report template.



## Branding Reports

Reports come with a default logo, but you can change that, as is illustrated in the above screen. Put the .png, .jpg or .gif graphic file with your desired logo in `owareapps\redcell\images` on the application server. In the `owareapps\installprops\lib\installed.properties` file, alter this property:

```
redcell.report.branding.image=<filename_here>
```

No need to include the path, just use the file name.

 **CAUTION:**

You must create images that are no taller than 50 pixels, and no wider than 50 pixels.

## Visualize My Network

The Visualize My Network portlet displays discovered devices, mapping them in relationship to each other. It also lets you store and retrieve views you have arranged, as well as configure the default view (see VIEW DETAILS on page 213 for more about these capabilities).



### How To:

#### Create a Visualization

Creating a topology map of devices or services is as simple as right-clicking the item(s) you want to map, and selecting *Visualize*.

You can also save different topologies after you configure them. See VIEW DETAILS on page 213 for more about that.

You can fine-tune the appearance of what you see with the tools described in Configuring Views and what follows.

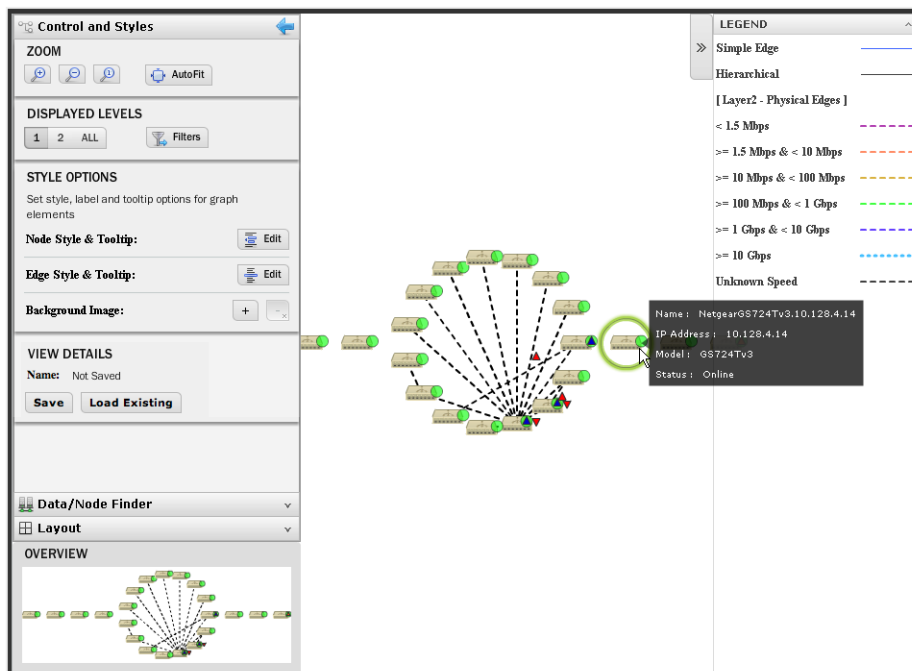


### Tip

If you do not see what you expect, make sure you have refreshed your browser so cached images do not interfere with current ones.

## Configuring Views

Click and drag displayed portions of this screen to see other parts of the topology. To move the display more, click in the OVERVIEW panel. You can also expand / collapse the panels on the left of the screen by clicking their title bars. (Figures below display them expanded.)



Hover the cursor over an icon or link between icons to see a small screen describing its contents and alarm state. Click an icon to highlight it (or click its name in the GRAPH INVENTORY tab list) and its connections to the network. See Alarms in Visualizations / Topologies on page 219 for more about the alarm states indicated by icons in topology.

### ⚠ CAUTION:

If you have installed a firewall on the application server, ports 80 and 8080 must both be open for topology to work.

Click the double arrows in the upper right corner to open the *Legend* for this screen, which describes the link colors and their meaning. Hover the cursor over a link to see its type described. See Icons on page 215 for an explanation of the icons that appear in these screens.

The screen to the left of the map displays the following panels:

- Control and Styles (which includes VIEW DETAILS)
- Data / Node Finder
- Layout

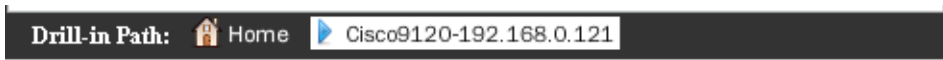


- OVERVIEW

Click on the title bars when these appear collapsed on the left of the screen to expand them. Click the blue left arrow at the top of them to re-collapse them.

In addition to the screen components immediately displayed, you can right-click an icon or component, and *Drill in* or *Expand* a device to see its subcomponents. If you expand, then its subcomponents appear on screen with the rest of the topology. If you *Expand w/o Filtering*, then any filtering you have applied in the Data / Node Finder tab does not apply to the subcomponents that appear. If you drill in, other components do not appear. Finally, you can select Actions to execute. The Layout selected in determines the arrangement of such expansions or drill-ins.

When you drill in, the path back to the top level appears below the topology.



Click the level where you want to “drill out,” or click *Home* to go to the top level.

Right-clicking a device can also let you select available Adaptive CLI Actions to execute on the selected device or component.

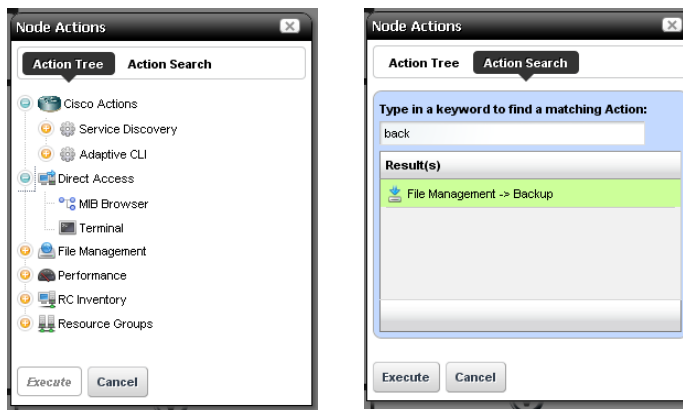
If you right click the blank area of the screen, you can *Export* it as either an image or GML (graphic markup language), or print the displayed topology.

 NOTE:

Because Topology uses Adobe Flash, menu items appear for that software when you right-click nodes. This includes *Settings*, *Global Settings* and *About Flash* menu items. The text below does not discuss these.

## Actions

Available Node Actions mirror the kinds of menu items available in Managed Resources on page 166.



The *Action Tree* panel displays the available actions. The *Action Search* panel lets you enter a desired action and search for it. Select an action and click *Execute* to implement it. Click *Cancel* to dismiss this screen without running any action.

## Control and Styles

- ZOOM
- DISPLAYED LEVELS
- STYLE OPTIONS
- VIEW DETAILS

### ZOOM

Click the + or - icons to zoom in or out. The *1* icon returns to the original default magnification (100%). The *Autofit* icon zooms to fit all devices in the topology.

### DISPLAYED LEVELS

Clicking *1* displays the top level. Clicking *2* displays the top level and the one below it. Clicking *All* displays all discovered levels, from device to interface.



#### Tip

The fewer levels displayed, the more quickly the display appears.

Clicking the *Filter* button opens a screen that lets you further tune the Topology display. It includes the following:

#### Level 1 Filters

Excluded Association Types (*Contact*, *Vendor*, *Location*) lets you turn off those icons. When these are activated, the icons disappear.

#### Level 2 Filters

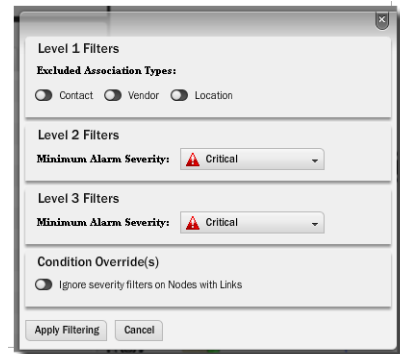
Select a *Minimum Alarm Severity* to display from the pick list. When you select a severity, then only resources with that alarm level or greater appear in the topology display.

#### Level 3 Filters

Select a *Minimum Alarm Severity* to display from the pick list. This restricts the display on a lower level than *Level 2*.

#### Condition Override(s)

When active, this excludes level expands on nodes with links that do not match the severity filters.

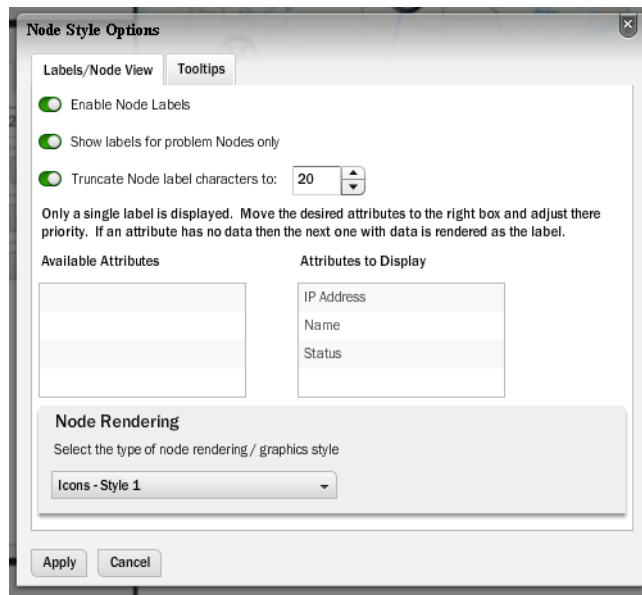


Click the *Apply Filtering* button to implement your configuration, or *Cancel* to dismiss this screen without applying it.

## STYLE OPTIONS

This tab's options configure node and line appearance. It displays the following when you click buttons in this panel. Notice the first two have Tooltips tabs in addition to the first one you see:

**Node Style Options**—Configure how nodes appear in topology.

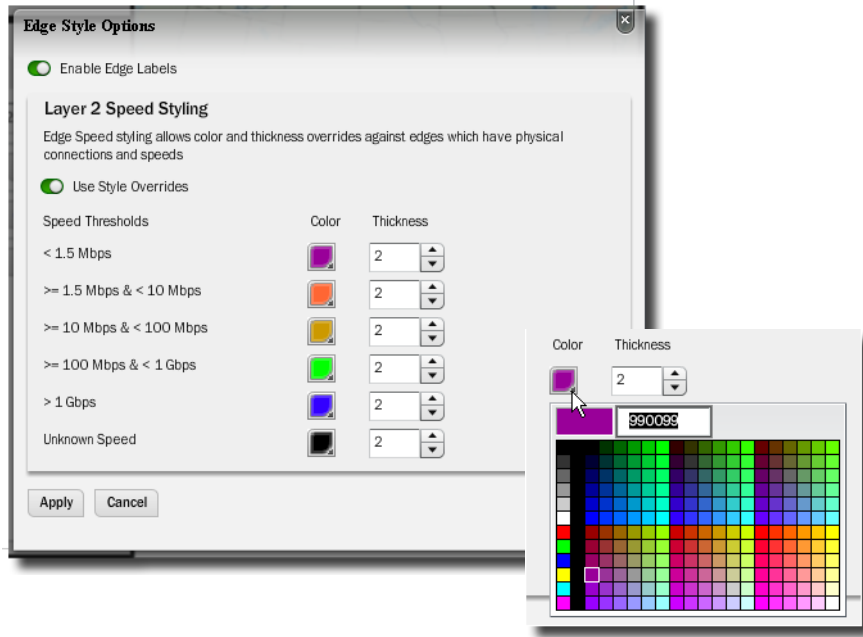


In the *Label / Node View* tab, you can elect to *Enable Node Labels* so labels appear next to icons in topology. Select the attributes in the middle panel. You can also elect to *Show Labels for Problem Nodes Only*, and *Truncate Node Label Characters* (and select the maximum number of characters).

Click to move attributes from *Attributes to Display* (all appear by default) to *Available Attributes* to conceal attributes you do not want displayed.

The *Node Rendering* pick list lets you select from several styles of icon that appear in topology. These include two icon styles (*Style 1*, the default, and *Style 2*), colored *Circles* (the color is the associated alarm color), and *Labels Only*. This last style overrides any previous selection to display labels only for problem nodes.

**Edge Style Options**—This lets you configure the colors on connections between icons.



First, click to *Enable Edge Labels*. To have the edge reflect speeds, you can then elect *Layer 2 Speed Styling* (enable *Use Style Overrides*). Select colors for speeds by clicking the lower right corner of the colored boxes that appear next to speed range labels. You can also configure the thickness of the edge next to that color selector. Click *Apply* to enable your configuration, or *Cancel* to abandon it and close this options screen.

 **NOTE:**

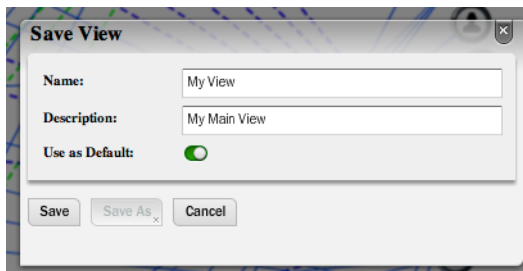
Revising colors does not mean the revision appears in the legend

**Background Image**—Click the + to select an image, typically a map, that you want to appear in the background, or the - to remove an existing one. Click and drag icons to locations on that image after it has appeared onscreen.

The selector looks for images on the machine where the browser is located. The size and appearance of images depends on the resolution of the monitor and the layout of the page in the browser. For example, setting the screen to 1280 by 1024 pixel resolution, with a one-column layout for the page where topology appears, a background graphic can be as large as 800 x 650 pixels.

## VIEW DETAILS

This panel displays the saved status of the current View, and has buttons to let you *Save* or *Load Existing* saved views. The View *Name* defaults to *Not Saved* when the display has not yet been saved. Clicking *Save* displays a screen where you can *Name* and enter a *Description* for the view you are saving. You can also configure a saved view for Dell OpenManage Network Manager to *Use as Default*, so it appears by default whenever you see a topology view.

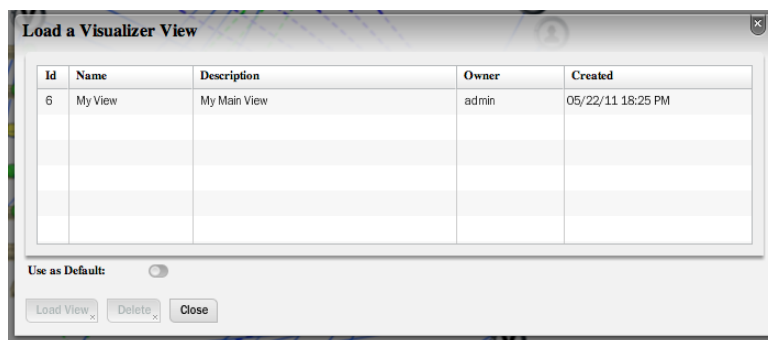


The 'Save View' dialog box contains the following fields and controls:

- Name:** Text input field containing 'My View'.
- Description:** Text input field containing 'My Main View'.
- Use as Default:** A toggle switch that is currently turned on (green).
- Buttons:** 'Save', 'Save As', and 'Cancel'.

Saving preserves Views and current Layout, Level, Node/Edge Settings, Top Level graphic elements, Name, Description, Owner, Dates and Filters.

Clicking *Load Existing* loads other saved views selected from a screen that also lets you *Delete* a selected view. Users who do not own the retrieved view can save a copy. Deletion is only possible for views you own.



The 'Load a Visualizer View' dialog box displays a table of saved views and includes the following controls:

Id	Name	Description	Owner	Created
6	My View	My Main View	admin	05/22/11 18:25 PM

Below the table, there is a 'Use as Default' toggle switch (currently off) and three buttons: 'Load View', 'Delete', and 'Close'.

If you delete the default view and do not set a new one, then the Network View defaults to its original settings.



### CAUTION:

Deleting views is not confirmed.

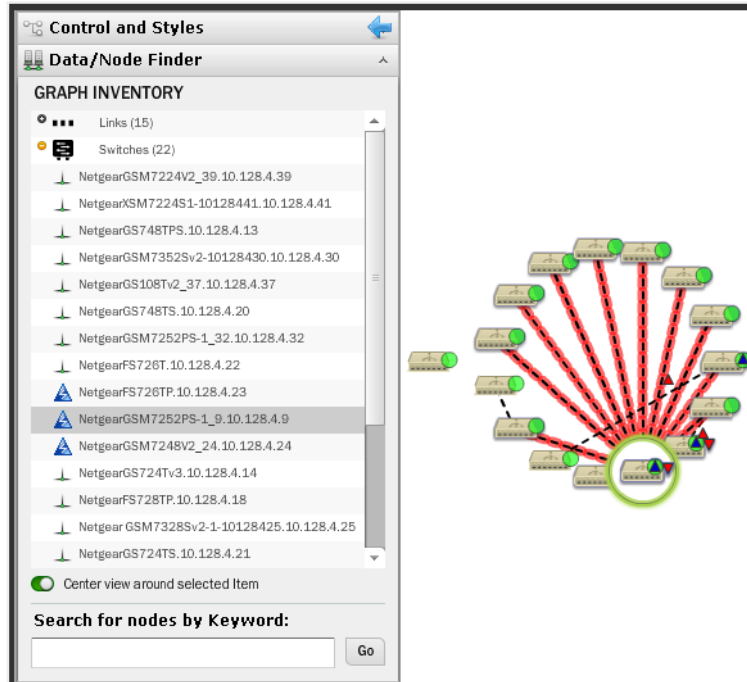
The saved label appears in the title bar the next time you open the view.

## Data / Node Finder

This screen offers additional topology information to help you locate specific resources within the visualization you have produced.

## GRAPH INVENTORY

This displays a legend of icon types followed by a count (in parentheses) of how many of each appear in the topology. The switch at the bottom of this panel centers the display around the selected icon.



Click the plus (+) to the left of the inventory category icons to display a list of devices in that category in the topology. Click on a list item to highlight that device and its network connection in the topology view. A circle highlights the device and a colored glow highlights its network connection(s). Notice that the listed inventory changes if you drill in.





### Tip

To make sure the selection appears in your view, select *Center view around selected item* at the bottom of this panel.

This tab also lets you *Search for nodes by keyword*. Search results highlight specific items within the topology.

## Icons

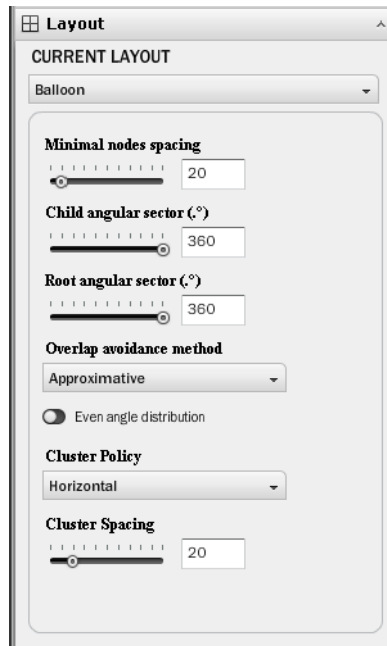
The the icons next to listed devices mean the following:

Icon	Type	Explanation
	Alarm	This shows the alarm state of the devices listed. In a composite list, like appears in Inventory, it shows the highest alarm state.
	Indeterminate	No alarm information is available for this device.
	Status	Green means the device is Online, red means Offline, and yellow means indeterminate.
	Topology Alarm Triangle	These appear next to the device icons. The upward pointing triangle indicates the icon attached is a top-level device. The color in the circle is connection status color described above. The color in the triangle the device's alarm state. If the triangle points down, it indicates the triangle's alarm state color comes from a "child" component of the node.

In the GRAPH INVENTORY tab (not the topology), the icons to the left of the devices are alarm icons, and their color reflects the highest alarm state on that device. Icons that appear on the right in the summary tree view displays the highest alarm severity for that type of device.

# Layout

The layout tab lets you select and configure the type of automated node layout that appears in the topology display.



Under CURRENT LAYOUT, use the pick list to select the type of layout. The fields and selectors that appear below depend on the selection. Here are the available layouts, and the fields that go with them:

## Balloon

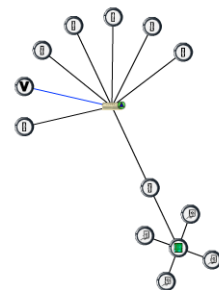
Balloon layouts display links between managed objects in a balloon tree structure. The root is typically whatever device you have expanded or drilled into.

You can specify the following in the settings for this layout:

**Minimal nodes spacing**– Use the slider to determine how close nodes are to each other.

**Child / Root angular sector (.o)**– Use the slider to determine the angular sector. The root sector determines how much of an arc around that root the child nodes fill, and the child sector determines the orientation around the child nodes.

**Overlap avoidance method**– Select *Approximate* or *Deterministic*.





**Even angle distribution**—Enable even angle distribution of nodes.

**Cluster Policy**—Select *Vertical* or *Horizontal*. This determines the (automated) orientation of the topology. Remember, you can click and drag device icons.

**Cluster Spacing**—Use the slider to determine the spacing between icons not in child / parent hierarchy.

## Orthogonal

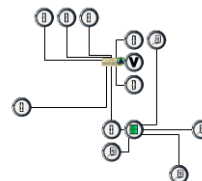
Orthogonal connections include right angles. You can specify the following settings for such layouts

**Minimal nodes spacing**—Use the slider to configure the node spacing.

**Use pseudo-orthogonal edges**—Enable pseudo-orthogonal edges that have non-right angles.

**Cluster Policy**—Select *Vertical* or *Horizontal*. This determines the (automated) orientation of the topology. Remember, you can click and drag device icons.

**Cluster Spacing**—Use the slider to determine the spacing between icons not in child / parent hierarchy.



## Radial

Radial layouts arrange nodes in concentric rings.

**Minimal concentric rings radius** —Use the slider to determine the concentric ring spacing.

**Minimal nodes spacing**—Use the slider to determine the nodes spacing.

**Angular sector (.o)**—Use the slider to determine the arc where child nodes appear.

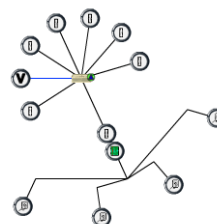
**Overlap avoidance method**—Select *Approximate* or *Deterministic*.

**Root node selection policy**—Select *Most weighted (for general graphs)*, *Manual (for general graphs)* or *Directed (only for tree graphs)*.

**Link drawing type**—Select from *Straight*, *Straight polyline*, *Curved polyline*, *Orthogonal polyline*, *Orthogonal curved*.

**Cluster Policy**—Select *Vertical* or *Horizontal*. This determines the (automated) orientation of the topology. Remember, you can click and drag device icons.

**Cluster Spacing**—Use the slider to determine the spacing between icons not in child / parent hierarchy.



## Circular

Circular layouts arrange all nodes in a circle.

**Minimal circle radius** – Use the slider to determine the radius of the circle.

**Minimal nodes spacing**– Use the slider to determine the nodes spacing.

**Wedge Angle**–Use the slider to determine the arc where child nodes appear.

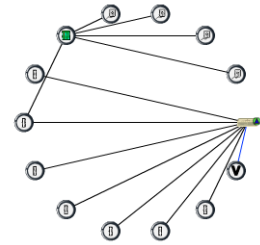
**Overlap avoidance method**–Select *Approximate* or *Deterministic*.

**Root node selection policy**–Select *Most weighted* (for general graphs), *Manual* (for general graphs) or *Directed* (only for tree graphs).

**Link drawing type**– Select from *Straight*, *Straight polyline*, *Curved polyline*, *Orthogonal polyline*, or *Orthogonal curved*.

**Cluster Policy**–Select *Vertical* or *Horizontal*. This determines the (automated) orientation of the topology. Remember, you can click and drag device icons.

**Cluster Spacing**—Use the slider to determine the spacing between icons not in child / parent hierarchy.



## Hierarchical-Cyclic

This arranges connections in a hierarchy. Use the following settings to alter its appearance.

**Distance between levels**– Use the slider to determine the distance between levels.

**Distance between nodes**– Use the slider to determine the distance between nodes.

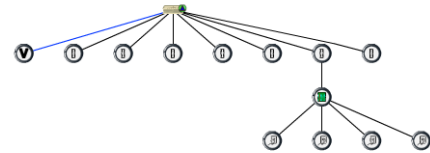
**Orientation**–Select from *Top to Bottom*, *Bottom to Top*, *Left to Right* or *Right to Left*.

**Draw edges from**–Select from *Node Center* or *Node Side*.

**Link drawing type**–Select from *Straight*, *Straight polyline*, *Curved polyline*, *Orthogonal polyline* or *Orthogonal curved*.

**Cluster Policy**–Select from *Horizontal* or *Vertical*.

**Cluster Spacing**—Use the slider to determine the spacing between icons not in child / parent hierarchy.



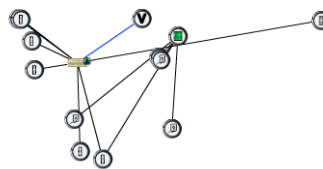
## Basic Spring

Basic Spring is an algorithm attempts to produce a natural layout that optimizes a spread out topology.

**Optimal Edge Length**—Use the slider to determine the distance between nodes.

**Cluster Policy**—Select from *Horizontal* or *Vertical*.

**Cluster Spacing**—Use the slider to determine the spacing between icons not in child / parent hierarchy.



## OVERVIEW

This displays a thumbnail of the entire topology that appears in the larger screen to the right. Click a location to move the larger view to center on it.

## Alarms in Visualizations / Topologies

Colored circles and triangles appear next to topology nodes to indicate its network status (circles) or the alarm state of the device (triangles, apex points up) or the alarm state of its child entities (off-center triangles, apex points down). For information about the alarm, hover your cursor over the triangle, and a popup appears describing the device, whether the alarm is on the device or a “child,” and what is its severity.



The alarms indicated are like alarms described in the portlet Alarms on page 99.

### NOTE:

The displayed alarms in the Alarms portlet may not be up to date, or may differ from those within Visualizations. Resyncing alarms and/or refreshing the browser resolves this difference.

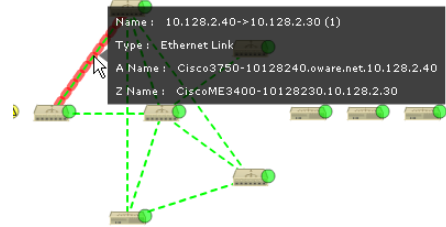
# Links in Visualization

When you have discovered links between devices in your network (see Link Discovery on page 176), they appear in the visualization.

Hover the cursor over a link, and a panel appears with the link information (*Name*, *Type* (for example: Ethernet), *A / Z Names* for the endpoints).

 **NOTE:**

Dell OpenManage Network Manager currently does not support displaying one-ended links.



## File Servers

You must configure FTP and/or TFTP file servers to push and pull configuration files to and from devices, or to deploy firmware updates. With this portlet you can switch between internal and external file server mode, and *Show* or *Hide* not applicable File Servers depending on the file server mode by checking/unchecking the *Show All Servers* check box. When this is unchecked, only the relevant file server(s) appear onscreen.

File Server Mode: <input type="radio"/> Internal <input checked="" type="radio"/> External				
Enabled	Name	Description	IP Address	TFTP Enabled
<input checked="" type="checkbox"/>	Julia's FTP		192.168.1.31	<input checked="" type="checkbox"/>

Right clicking a file server, or the empty list space lets you do the following:

**New**—Displays the File Server Editor screen.

**Edit**—Displays the selected File Server in the File Server Editor screen.

**Disable**—Disables the selected file server. When file servers are disabled, they are not used in a Backup, Restore or Deploy operation. This too appears only for External File Servers.

**Enable**—Activates the selected file server. Again, exposed for External file Servers only.

**Test**—Tests the selected file server by sending and retrieving a file.

**Delete**—Removes the selected file server from the list. This appears for External File Servers only.

### NOTE:

You can select whether Dell OpenManage Network Manager is in *Internal* or *External File Server Mode* with the radio buttons at the top of this portlet. Checking *Show All Servers* displays the internal file server.

### CAUTION:

Port conflicts prevent having an external file server and internal file server operate on the same machine.

Columns in this manager identify the server, and describe whether it is enabled, and has TFTP enabled.

# File Server Editor

This editor lets you configure new and existing file servers.

The screenshot shows a window titled "Editing: koss (File Server)". It has two tabs: "General" (selected) and "Test". The "General" tab is divided into three sections: "General Parameters", "Server Type", and "Authentication Settings".

- General Parameters:** Includes fields for "Name" (koss) and "Description" (Jorns external file server). There is a checked "Enabled" checkbox.
- Server Type:** Includes radio buttons for "FTP Server" and "Secure FTP/SCP Server" (selected). There is a checked "TFTP Support" checkbox.
- Authentication Settings:** Includes fields for "IP Address" (192.168.0.118), "External IP Address" (.), "Net Mask" (255.255.255.0), "Login" (admin), and "Password" (\*\*\*\*\*).

At the bottom of the window are buttons for "Save", "Cancel", and "Test".

This is where you specify the *Name*, whether the server is *Enabled*, whether the connection is secure (*Secure FTP/SCP Server*), supports TFTP, internal and external (optional) IP addresses, and Net Masks, and the login and password for the file server. Once you have configured a server, you can test the file server credentials by clicking on the *Test* button at the bottom of the screen. Click *Save* to preserve your changes.

## Tip

FTP servers typically must be on the same side of the firewall as the devices with which they communicate. If you have several such servers, the specified *Net Mask* also determines which server communicates with devices in which portion of the network.

Notice that you can now configure an IP address used by Dell OpenManage Network Manager, and another *External IP Address* used by the devices. If you configure multiple file servers, Dell OpenManage Network Manager selects the server with the *Net Mask* whose subnet is closest to the device(s) with which it communicates.



# File Management

In addition to letting you back up and restore configuration files, and deploy firmware updates to devices, this menu manages viewing and comparing configuration files backed up from the selected devices. Details about these capabilities appear below.

*Compare* and *View* options have the following limitations:

- If you select a config file that is a single file, without any historical precedent, no comparison option appears on the menu since the selected version does not have a prior version.
- If you select a single config file of version two or higher, comparison is an option. When selected, OpenManage Network Manager automatically compares against the prior version for that device and file name.
- If you select two config files of any version, compares is between those two versions.
- If you select three or more config files, no comparison option appears.
- The *View* option appears for a single selection only, and only lets you view files that are not binary.

## Tip

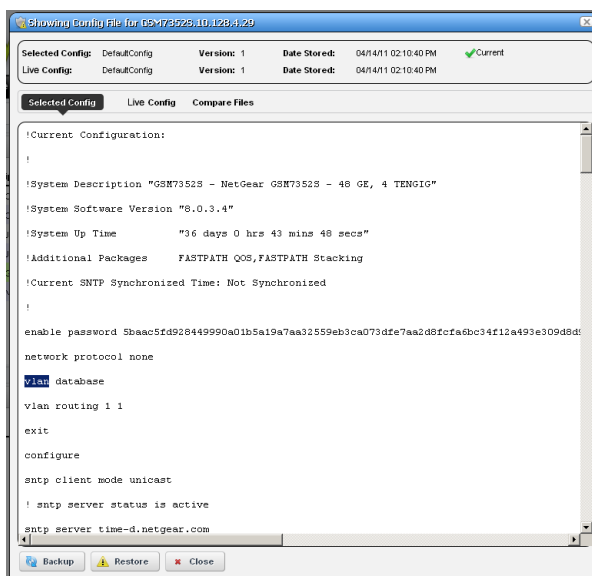
The icon to the left of the *File Name* listed in the portlet lets you know whether a configuration file is binary (  ), and not viewable, or text (  ), and viewable.

The file management menu contains the following:

**View / Edit**— This opens a panel displaying the configuration file's contents. Use the browser's *Find* function (as demonstrated on the right) to locate specific text within the Config File. You can also select and copy text within this screen.

Notice that *Selected Config* and *Live Config* (current) version and storage dates appear at the top of this screen. When you perform a backup that differs from the config that is *Labeled Current*, that label changes to *Live Config* if changes are detected.

*Selected Config* appears when you open this screen from the Configuration Files Portlet, but *Live Config / Current Config* appear side-by-side when you open this screen from the Managed Resources portlet.



You can also compare two different configurations (*Selected Config* and *Labeled Current / Live Config*) in the tabs that appear on this screen, with the *Compare Files* tab at the top.

Close the screen with the buttons at its bottom. Notice you can also *Backup* or *Restore* what you are viewing with buttons at the bottom of the screen.

**Assign Labels**—Use this option to select an existing label or create a new one. You cannot assign System labels (*Current*, *Compliant*, and so on).

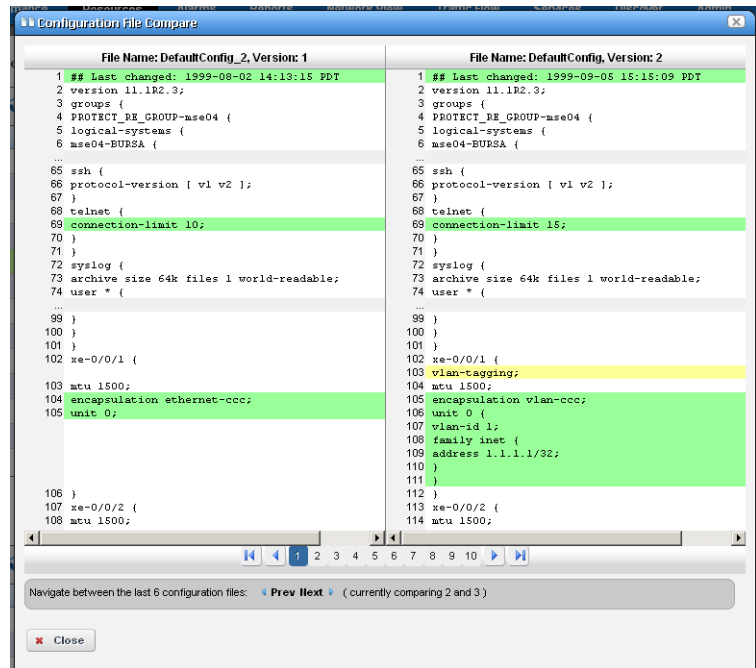
**Compare Current v. Previous / to Label / Selected**—You can compare configurations by right-clicking a device, or two devices then selecting *Compare*. If you right click a single device with a previous backup, then the comparison is between the latest and next-to-latest backup. If it does not have a previous backup, then the menu offers to compare to a designated label. You can compare two different *Selected* devices too. Ctrl+click to select two different devices before you *Compare*.

Notice that the *Prev / Next* buttons at the bottom of this screen cycle through as many as five previous configuration files.

The comparison screen appears with the configurations side-by-side (note the file names in the title bar of this screen).

Lines that differ between the two configurations appear highlighted green. Lines that are missing in one, but that appear in another appear highlighted red. Added lines appear highlighted in yellow. Use the right/left arrows to page through the side-by-side comparison.

The page numbers and beginning / forward / back / end arrows help you navigate between pages of pairs of files. Notice also that if you have more than two such files, a panel appears at





the bottom that lets you navigate between adjacent pairs of such files (1 and 2, 2 and 3, 3 and 4, and so on). Click the Prev / Next links to move between pairs of files.

### Tip

You can use the browser's "Find" function (typically initiated by Ctrl+F) to locate text within these views.

**Backup / Restore**—Select these to backup or restore a configuration file. See *How to: Backup Configurations* on page 225 or *Restore Configurations* on page 227 for step-by-step instructions.

**Deploy**—Select this option to deploy an OS Image (firmware). See *Deploy Firmware* on page 238 for more.

### NOTE:

Some devices, including the Dell Force10 C-Series and E-Series, will allow then drop telnet connections during deployment or file restoration when you select restart as part of the process. This can take from six to eight minutes, though it can take as long as fifteen minutes for a fully populated chassis. During that time, you can ping the device; however, Dell OpenManage Network Manager cannot log in to the device until the reboot is complete.

Restoring configurations to Dell Force 10 devices may produce errors when individual commands already exist in the running config and cannot be overwritten. Dell OpenManage Network Manager ignores such errors and reports success by default since the errors indicate a command was not applied, not that restoration was unsuccessful. Best practice is to restore to startup config to avoid these errors, especially when scheduling backup or backing up a group on such devices.

**Export / Import** —Export lets you save a local copy of the selected config file. Import opens a screen that lets you select a locally-accessible file to store, view, compare and deploy.

### Tip

You can see configuration files in the *Latest Configurations* portion of the Details screen for a device or in the Configuration Files or Top Configuration Backups portlets.



## How To:

### Backup Configurations

Dell OpenManage Network Manager simplifies backing up devices so you always have their configuration files, even if the one on the device becomes corrupted or out-of-date.

### Tip

You can back up several devices at once for what amounts to a "group operation." Select more than one device by Ctrl+clicking in the expanded portlet, then right-click as outlined below. You must expand portlets to multi-select.

Here are the steps to back up a device:

- 1 Make sure you have configured an FTP or TFTP server to handle the backup. See *Netrestore File Servers* on page 70.
- 2 Right-click a device in the *Managed Resources* portlet.
- 3 Select *File Management > Backup*.
- 4 Configure the subsequent *Backup Device* screen.

**Specify Backup Options**

File Name: DefaultConfig  
Description:   
Update user label:   
Email Settings: [add email](#)

**Select Targets for Backup** Add Equipment Add Groups Remove All

Name	Last Backup Results	Last Backup Date	Action
Cisco7206-1921681138.192.168.1			

**Device Options**

Add Schedule Execute Save Close

This screen lets you configure the following:

**File Name**—A text identifier for the file

**Description**—A text identifier for the file

**Update User Label**—A text identifier for the file. Entering such a label creates it, and makes it available for later restoration, comparison, and so on.

**Email Settings**—Click *add email* to configure an email notification about this backup.

**Select Targets for Backup**—This screen defaults to the device you selected in *Managed Resources*. You can also click the *Add Equipment* to add individual devices, or *Add Groups* to add groups, or *Remove All* to manage devices that appear in this list of targets.

**Device Options**—This portion of the *Backup Options* screen displays detailed configuration options available for the selected target. For example, you could select between backing up the running-config and the startup-config.

- 5 Click one of the buttons at the bottom of the screen to initiate the next backup action.

*Add Schedule* opens the scheduling screen to let you automate the backup you have configured on a specified date, time, or repetition. See *Scheduling Actions* on page 369.

*Execute* performs the backup immediately. The *Results* tab in this screen opens, displaying the message traffic between Dell OpenManage Network Manager and the device(s). See *Audit Trail Portlet* on page 93.

*Save* preserves this configuration without scheduling or executing it.

*Close* closes this screen without saving the configured restoration.



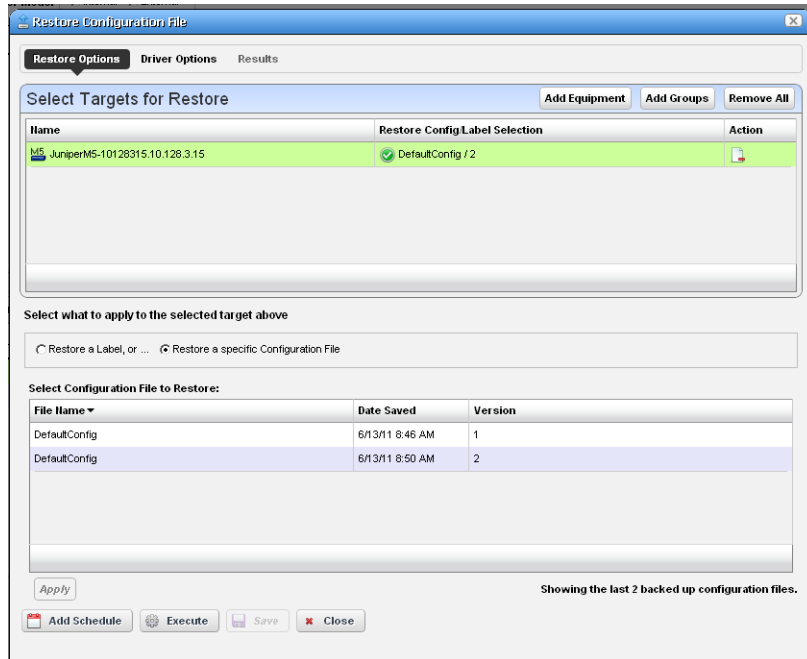
## How To:

### Restore Configurations

The following are the steps to restore a config file to a device:

- 1 Make sure you have configured an FTP or TFTP server to handle the backup. See *Netrestore File Servers* on page 70.
- 2 Right-click a device in the *Managed Resources* portlet.
- 3 Select *File Management > Restore*.

- 4 Configure the subsequent *Restore Device* screen.



This screen lets you configure the following:

**Select Targets for Restore**—This portion of the screen lets you *Add Equipment*, *Add Groups*, or *Remove All* target devices. Listed targets and their *Restore Config / Label Selection*. Click the icon in the *Action* column to remove the listed target.

**Select what to apply to the selected target**—This portion of the screen lets you select either a label (like *Current*, *Compliant* and so on—a selector listing available labels appears onscreen once you click this option), or *Restore a specific Configuration File*. The latter lists available files and lets you click to select. Click *Apply* to configure the selected target, or *Apply to All* to configure all targets.

- 5 Click one of the buttons at the bottom of the screen to initiate the next backup action.

*Add Schedule* opens the scheduling screen to let you automate the restoration you have configured on a specified date, time, or repetition. See *Scheduling Actions* on page 369.

*Execute* performs the restoration immediately. The *Results* tab in this screen opens, displaying the message traffic between Dell OpenManage Network Manager and the device(s). See *Audit Trail Portlet* on page 93.

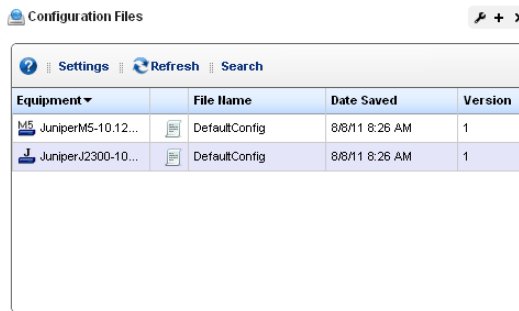
*Save* preserves this configuration without scheduling or executing it.

*Close* closes this screen without saving the configured restoration.

# Configuration Files

One place backed up configuration files can appear is in this portlet. Right-clicking offers you the following options (all options listed may not be available):

**View / Edit**—See or edit the backed up configuration file, if it is not a binary file. See File Management on page 223 and Configuration File Editor on page 231 for a description of these capabilities.



Equipment	File Name	Date Saved	Version
M5 JuniperM5-10.12...	DefaultConfig	8/8/11 8:26 AM	1
J JuniperJ2300-10...	DefaultConfig	8/8/11 8:26 AM	1

**Compare to Label / Compare Selected**—Compare labeled configuration files to the current selection. See File Management on page 223 for a description of this capability. You can create labels when you back up a config file, or you can compare to the default labels (*Change Determination, Current, Compliant*). If you select two configuration files in the expanded portlet, you can also *Compare Selected*.

**Promote**—Makes the selected config file available for mass deployment. This is a useful way to make a “pattern” configuration file to deploy to several devices. See Image Repository on page 233 for additional information about how to do this.

**Backup / Restore**—Back up the device (again) related to the selected file, or restore the selected file.

**Archive**—Save the selected file to disk, and optionally delete it from this list.

**Import / Export**—Export the selected config file to disk, or import it from disk.

**Delete**—Removes the file from the Dell OpenManage Network Manager database without exporting it.

**Aging Policy**—Opens the Aging Policy selector. See Redcell > Database Aging Policies (DAP) on page 50 for more about these.

You can also import and export a selected config file.

## Tip

You cannot select multiple lines in most summary portlets. This is the one exception. You do not need to open Configuration Files Expanded to select multiple lines.

## Configuration Files Expanded

The Expanded portlet lets you filter the list of displayed configuration files, and displays the *File Type, Description, File Size* and whether the configuration file is *Labeled* in columns.

The Labeled column appears with green or red icons depending on whether the config file has a label. When a label applies to a configuration, you cannot *Delete* or *Archive* it.

The screenshot shows the 'Configuration Files' interface. At the top, there's a 'Default Configuration Files Filter' dropdown and an 'Advanced Filter' button. To the right are 'Search', 'Refresh', 'Settings', and other utility icons. Below this is a table with the following data:

Equipment	File Type	File Name	Date Saved	Version	Description	File Size	Labeled
Router:192.168.1.138	Text	DefaultConfig	9/1/11 8:55 AM	1		3 KB	✓
MS JuniperMS-10.128.3.15.1	Text	DefaultConfig	9/1/11 8:55 AM	1		32 KB	✓
JuniperJ2300-10.128.3.1	Text	DefaultConfig	9/1/11 8:55 AM	1		52 KB	✓

Below the table, it says '3 item(s) returned'. There are two side panels:

- Reference Tree:** Shows a tree view with 'DefaultConfig / 1'.
- Labels Using Config File:** Shows a table of labels assigned to the selected file:
 

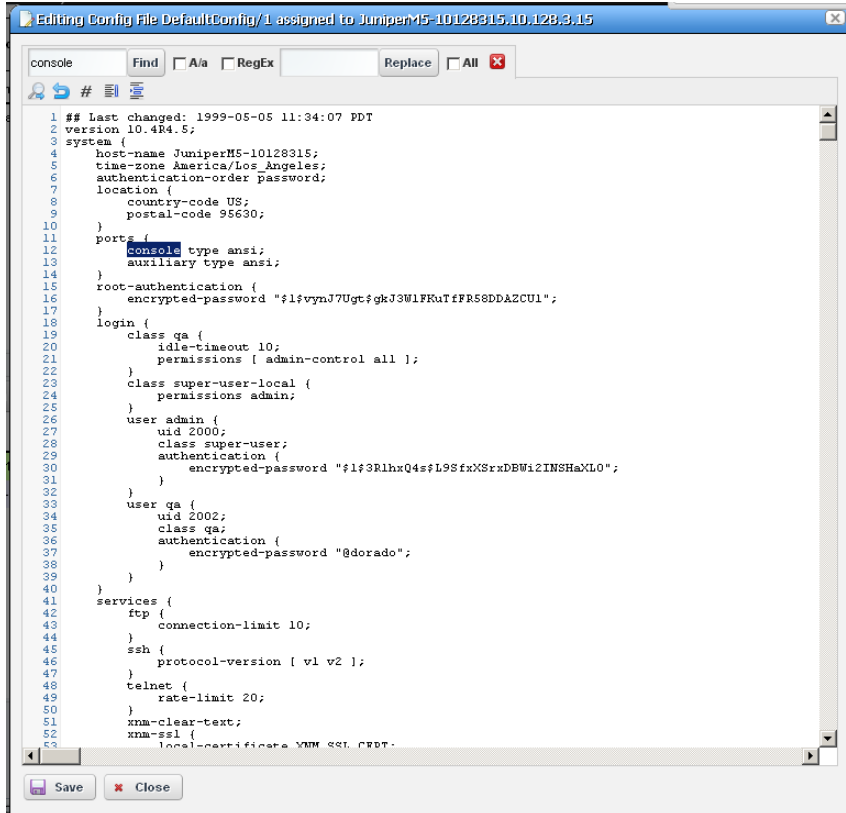
Label	Assigned On
Current	9/1/11 8:55 AM
Change Determ	9/1/11 8:55 AM

At the bottom right of the interface, there are 'Snap Panels' and 'Close' buttons.

The *Labels Using Config File* snap-in displays all labels connected to the selected configuration file, and the date on which that connection was made. The *Reference Tree* displays the configuration file name, and lets you right-click it to access the available operations it supports. To see the most recent configuration files, see *Top Configuration Backups* on page 277.

## Configuration File Editor

This editor lets you manually edit configuration files, and save them to the Dell OpenManage Network Manager database.



When you select a file in the Configuration Files portlet, and right-click to select *Edit*, this screen appears with the following features.

**Find / Replace**—Click the magnifying glass icon to open a text search feature. Notice that you can check *A/a* to make your search case-sensitive, or *RegEx* to use regular expressions to search.

Click the *Find* button to locate text in the config file. Click *Replace* to replace found text, once it is located. Check the *All* checkbox and click *Replace* to bulk replace all instances of the *Find* text.

Click *Save* to preserve your edits, or *Close* to abandon them. Notice that the edited configuration appears listed with the other Configuration Files in the portlet as a different version than the original (the version increments by one every time you edit and save a configuration).

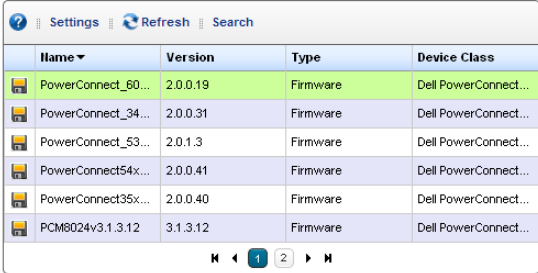




# Image Repository

The Image repository manages firmware updates to deploy to devices in your network, or configurations you want to deploy to several devices.

You must add such files to your Dell OpenManage Network Manager system before you can deploy them. The summary screen listing these images displays their *Name*, *Description*, *File Name*, *Image Type* and *Installed Date*. Right-clicking this screen displays the following menu items:



The screenshot shows the 'Image Repository' window with a table of firmware images. The table has four columns: Name, Version, Type, and Device Class. The first row is highlighted in green.

Name	Version	Type	Device Class
PowerConnect_60...	2.0.0.19	Firmware	Dell PowerConnect...
PowerConnect_34...	2.0.0.31	Firmware	Dell PowerConnect...
PowerConnect_53...	2.0.1.3	Firmware	Dell PowerConnect...
PowerConnect54x...	2.0.0.41	Firmware	Dell PowerConnect...
PowerConnect35x...	2.0.0.40	Firmware	Dell PowerConnect...
PCM8024v3.1.3.12	3.1.3.12	Firmware	Dell PowerConnect...

**New**—Select either *Firmware Image*, or *Configuration Image*. Firmware Image displays the Firmware Image Editor screen. Configuration Images originate from Configuration Files that are promoted to mass restore. See the Configuration Image Editor on page 236 for its functionality.

**Edit**—Displays the selected Firmware image in the Firmware Image Editor screen, or the Configuration Image Editor if the selected line is a configuration image.

**Deploy**—Deploys the selected file to devices, and with the options you select in a subsequent selection screen. For this to function, you must have enabled a server, as described in File Management on page 223.

**Download Firmware For**—Some devices (typically Dell) support downloading firmware from the internet. These devices appear listed in a sub-menu. Select the type for which you want to download OS images, and Dell OpenManage Network Manager automatically downloads them.

**Delete**—Removes the selected OS image / configuration from the list.

## Expanded Image Repository portlet.

When you click the plus, this portlet expands to display the OS images list, a snap panel Reference tree of the connections to devices, and another panel listing the files within the selected image.

Image Repository [Return to previous](#)

Default OS Image Filter | + Advanced Filter Search Refresh Settings

Name	Description	File Name(s)	Version	Installed Date	Type	Device Class	Device Family	Status
TestConfig	This is a test	/hetrestore/hnarc...	1	10/25/11 2:13 PM	Configuration			Invalid Device Cl...
PowerConnect3...	PowerConnect 3...	powerconnect_...	2.0.0.40	9/8/11 11:38 AM	Firmware	Dell PowerConn...	OSVersion	Ready
PCM6348v3.1.5.2a	PowerConnect ...	PCM6348v3.1.5...	3.1.5.2	9/8/11 11:42 AM	Firmware	Dell PowerConn...	OSVersion	Ready
PCM6220v3.1.5.2a	PowerConnect ...	PCM6220v3.1.5...	3.1.5.2	9/8/11 11:41 AM	Firmware	Dell PowerConn...	OSVersion	Ready
PowerConnect_...	PowerConnect 6...	PowerConnect_...	2.0.0.19	9/8/11 11:39 AM	Firmware	Dell PowerConn...	OSVersion	Ready
PowerConnect_...	PowerConnect 3...	PowerConnect_...	2.0.0.31	9/8/11 11:38 AM	Firmware	Dell PowerConn...	OSVersion	Ready
PowerConnect5...	PowerConnect 5...	PowerConnect_...	2.0.0.41	9/8/11 11:39 AM	Firmware	Dell PowerConn...	OSVersion	Ready
PCM8024v3.1.3.12	PowerConnect ...	PCM8024v3.1.3...	3.1.3.12	9/8/11 11:43 AM	Firmware	Dell PowerConn...	OSVersion	Ready

11 item(s) returned

Reference Tree

- PowerConnect35xx\_V20040

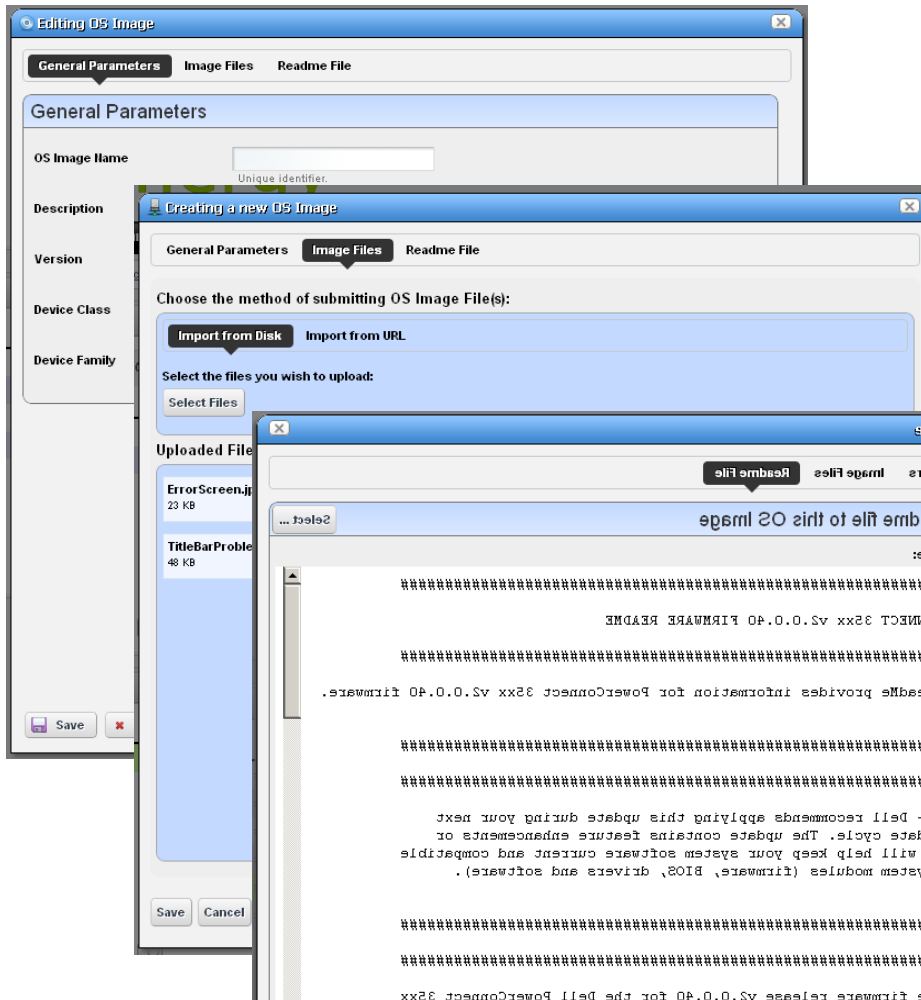
Files

Name	Size
powerconnect_35xx-20040.ros	4 MB
powerconnect_35xx_boot-20000.rtb	512 KB

Snap Panels | Close

# Firmware Image Editor

When you open or create an OS image, its configuration appears in this editor. The *General*



*Parameters* tab contains its *OS Image Name*, *Description*, *Version*, and the *Device Class* and *Device Family*. The *Image Files* tab displays a selector that lets you create new OS Images, retrieving files from the local file system (*Import from Disk*) or a URL (*Import from URL*). Because such images can consist of multiple files, you can import multiple files here. Finally, you can also import a *Readme File* to accompany this image, and view it in that tab.

Click *Save* to preserve the OS Image you have configured, or *Cancel* to exit these screens without saving.

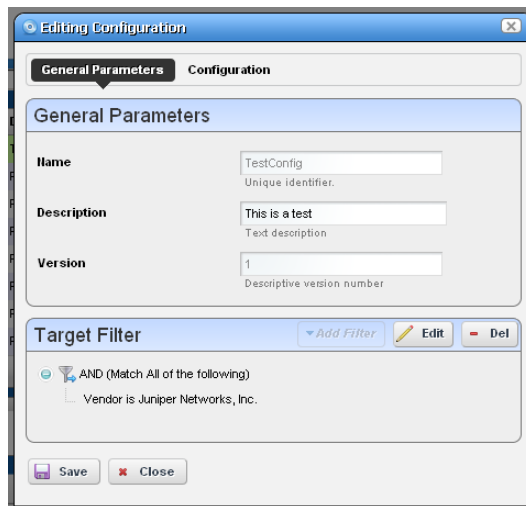
# Configuration Image Editor

This editor appears for new configuration images, or for configurations you *Promote* in the Configuration Files portlet for mass restoration. This screen has the following tabs:

- General Parameters
- Configuration

## General Parameters

In this screen you can name and describe the configuration file, and configure a filter to screen restoration targets.

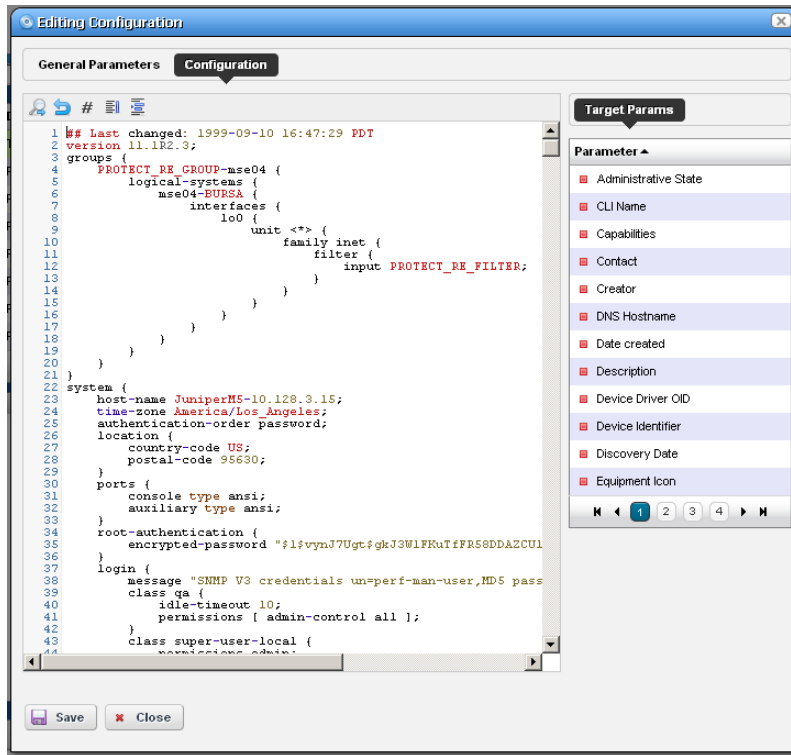


The *Version* field automatically tracks changes to the original.

The *Target Filter* panel lets you configure how this configuration decides which devices to target. When targets fail, restoration skips them.

## Configuration

This panel lets you configure what is restored, and what is variable in mass deployments.



This screen appears without contents when you create a new Configuration Image, but appears with data from any promoted configuration file, if it originated as a promoted config file.

## Target Param

The panel of parameters that appears to the right of this screen lets you insert a value retrieved from Dell OpenManage Network Manager's database into the restored configuration file.

For example, if a Contact appears in the file, delete the specifics retrieved from a particular device's config and double-click the *Target Param* "Contact." Dell OpenManage Network Manager inserts `$_EquipmentManager_RedCell_Config_EquipmentManager_Contact` (a unique identifier for the database's Contact field) wherever you put the cursor.

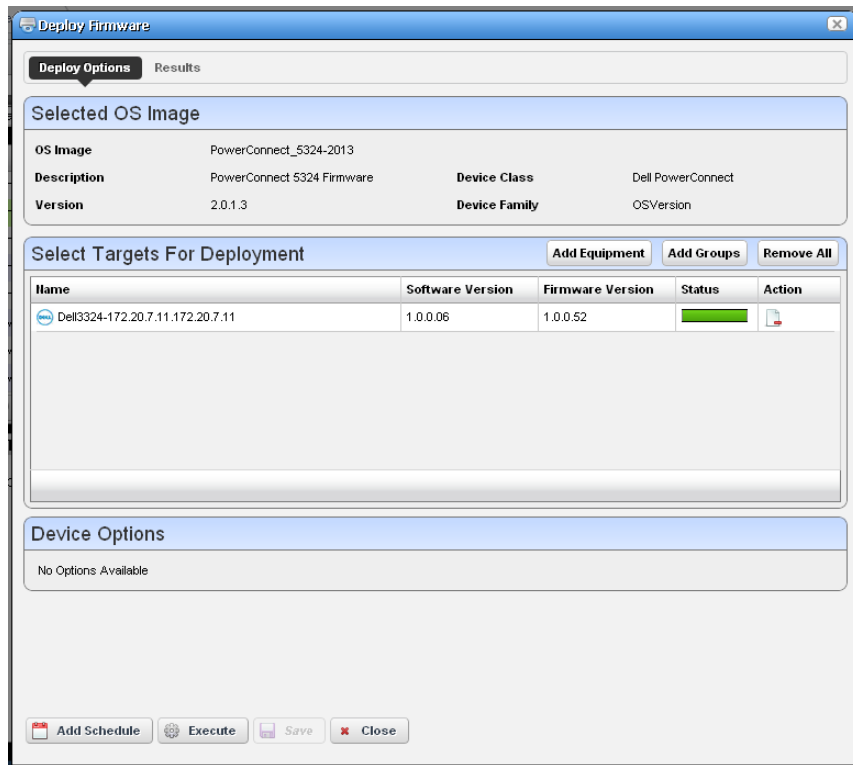
Now, when you deploy this config file to the devices that pass the filter in the General Parameters editor screen, Dell OpenManage Network Manager first updates this parameter with discovered data retrieved from the device before restoring the configuration. This facilitates deploying the same config to many devices while retaining individual Target Params like contacts, DNS Hostname, and so on.

 **NOTE:**

Target Params include all available discover-able parameters. Some may not apply to the specific device or configuration file.

## Deploy Firmware

This screen lets you configure a deployment, whether triggered from resource groups, individual resources, or the Image Repository screen. Deployment validates the selected image is appropriate for the selected devices, or appropriate devices within a group.



Notice you can *Add Schedule* to schedule this deployment rather than *Execute* it immediately. Click *Save* if you schedule this deployment, or *Close* to abandon your edits.



## How To:

### Deploy Firmware

To deploy firmware, follow these steps:

- 1 Make sure you have an FTP / TFTP server correctly configured. See File Management on page 223.
- 2 Right click a device in *Managed Resources* or the groups or Image Repository pages and select *File Management > Deploy*.
- 3 The *Deploy Firmware* screen appears.

You can *Select OS Image* in the top panel, and configure deployment with the following fields:

**OS Image**—Select an image. It must already have been uploaded in the Image Repository.

**Description**—A text description of the image.

**Version**—The image version.

**Device Driver**—The device driver associated with this image.

**Image Type**—A read-only reminder of the type of image.

**Select Targets for Deployment**—Select targets for deploying the image. This defaults to the device right-clicked in *Managed Resources* to initiate this action, or devices that match the selected file you want to deploy. You can then click the *Add Equipment* button (again, restricted to devices that match the deploy file's type). You can also remove devices from the target list with the *Remove All* button. Notice the *Status* column in the table of targets shows whether the OS deployment is supported or not.

#### NOTE:

You can also select devices, then change the OS selection so a potential mismatch will occur. This will likely trigger rejection of the deployment by the device, but is not a recommended experiment.

**Device Options**—The appearance of the *Device Options* panel, at the bottom of this screen, depends on the device selected in the *Targets* panel. These vendor-specific fields let you fine-tune the deployment.

- 4 Click one of the buttons at the bottom of the screen to initiate the next backup action.

*Add Schedule* opens the scheduling screen to let you automate the backup you have configured on a specified date, time, or repetition. See Schedule Actions on page 186.

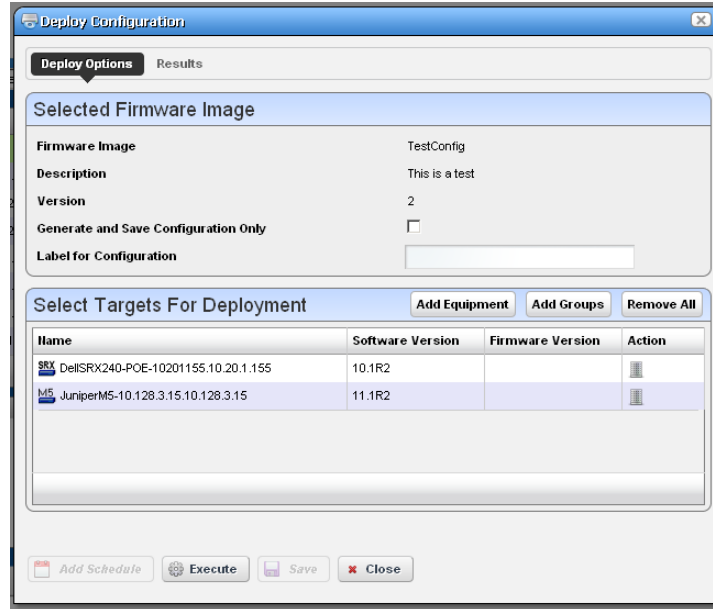
*Execute* performs the backup immediately. The *Results* tab in this screen opens, displaying the message traffic between Dell OpenManage Network Manager and the device(s). See Audit Trail Portlet on page 93.

*Save* preserves this configuration without scheduling or executing it.

*Close* closes this screen without saving the configured backup.

# Deploy Configuration

When you deploy a configuration, a screen appears to configure how that occurs.



It has the following fields:

## Select Firmware Image

**Firmware Image**—The identifier for the image

**Description**—The description for the image

**Version**—The version for the image

**Generate and Save Configuration Only**—Check this if you simply want to configure for later restoration.

**Label for Configuration**—Enter a label name, if applicable.

## Select Targets for Deployment

Use the *Add Equipment* or *Add Groups* buttons to select individual devices or groups of devices (both are possible together). Use *Remove All* to delete all targets, or use the delete icon in the *Action* column to delete individual equipment or groups.

**NOTE:**

The listed targets must still pass the filter set in the editor's General Parameters.





## How To:

### Restore a single configuration to many target devices

The following steps describe restoring a single configuration to many discovered devices without overwriting those devices' essential information.

- 1 Back up a single device's configuration that is nearest to the kind you would like to see generally.
- 2 Right-click this backed up file in the File Management portlet, and *Promote* it so it appears in the Image Repository portlet.
- 3 Right-click > Edit the promoted configuration in the Image Repository.
- 4 Name the file, and, if necessary, configure a filter In the General Parameters tab of the editor.
- 5 In the Configuration tab, locate the parameters you want to preserve in discovered devices when you restore this file. This can include items like the device's DNS Hostname, IP Address, and so on. Delete the file's specifics and double-click to insert the *Target Params* in place of these variables.
- 6 Save the configuration.
- 7 Right-click to deploy this configuration.
- 8 You can check *Generate and save for configuration only* if you simply want to configure deployment for later, and save for now. You can also optionally name a label for the deployed files.
- 9 Select the devices, or groups of devices to which you want to deploy.
- 10 Click *Save*, *Execute* or *Add Schedule* depending on your desired outcome.
- 11 If you click *Execute*, you will have to confirm this action.

When Dell OpenManage Network Manager performs the restoration (deploy), it reads the Target Params from those discovered for each device, inserts those in the config file, then restores it, device by device, skipping any that do not pass the filter set up in step 4.



# Monitoring

This section describes Resource Monitors as they appears in Dell OpenManage Network Manager's web portal. The following describes these monitors:

- OpenManage Network Manager Server Statistics
- Resource Monitors
- Top [Asset] Monitors (pre-configured monitors that come with your installation by default.

Finally, this chapter contains a reminder about scheduling refreshes of monitor target groups. See *Scheduling Refresh Monitor Targets* on page 276.

## Monitors and Discovery

Not all monitors are enabled for devices discovered by default. Typically discovery adds devices only to ICMP (ping) monitoring. If you enable an SNMP monitor during discovery, for example, performance degrades if discovery finds devices with many interfaces that the monitor attempts to process.

To improve performance such behavior is disabled by default so processing occurs only for the ICMP Monitors. To re-enable processing for other monitors during discover (assuming they are enabled), set/create the following property in `owareapps/installprops/lib/installed.properties`:

```
pm.monitor.process.implicit=true
```

By default, this is set to `false`. Monitors automatically refresh all implicit targets when a rule executes independently of discovery in roughly six hour intervals. Alternatively you can select the monitor(s), right mouse click and select *Refresh Monitor* to manually refresh the target.

## How to's

This chapter contains the following step-by-step instructions for these features:

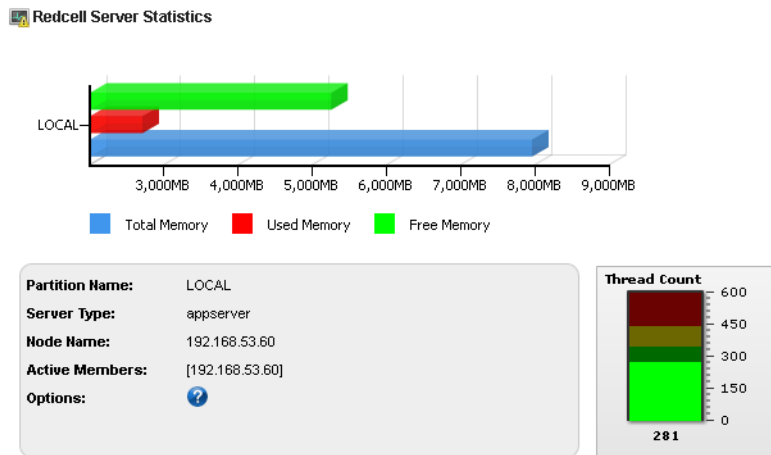
- Create an SNMP Interface Monitor
- Create an ICMP Monitor
- Create a Key Metrics Monitor
- Create a Simple Dashboard View

You can see Performance Options from a variety of locations by right-clicking in Dell OpenManage Network Manager. For example:

- Ports in the Ports portlet
- Interfaces
- Ports / Interfaces in the Details panels lets you *Show Performance*
- Right clicking on any of the above within a Reference tree displays Performance Options.
- All Top [Asset] Monitors right click to offer Performance options.

## OpenManage Network Manager Server Statistics

This summary screen has no expanded view. It displays the statistics for the OpenManage Network Manager application server.



The bar graph displays *Total*, *Used*, and *Free* memory on the server. One such graph appears per server monitored. Hover your cursor over a bar to see its reading in a tooltip. Click the trio of bar graphs related to the server you want to monitor, and its information appears in the text and in the thread count gauge.

The text displays the *Server Type* (appserver), the *Node Name* (typically the IP address of the server providing information), and *Active Members* (more than one appears for a cluster).

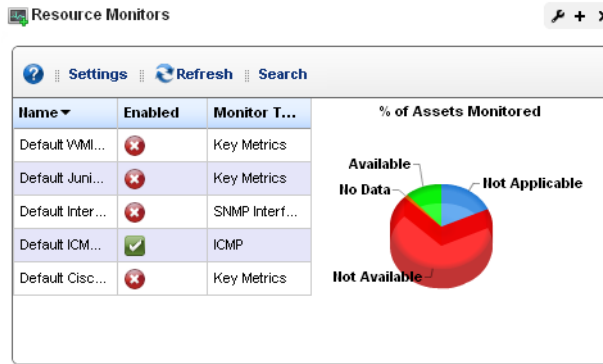
### NOTE:

The graphs in this portlet do not start at zero (0), so the bars may appear out of proportion. The total of Used plus Free memory may appear to be much smaller than the Total Memory bar.

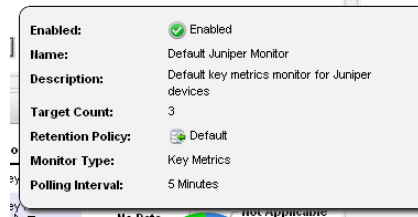
# Resource Monitors

This summary screen displays currently, active performance monitors in brief.

The *Name* column displays the identifier for each monitor instance, *Enable* displays a green check if it is currently enabled, or a red minus if it is disabled.



The *Monitor Type* column typically displays what the monitor covers. Hover your cursor over this column to see a popup with the selected monitor's properties. The popup that appears after this query displays the relevant information for the monitor, including whether it is *Enabled*, *Name*, *Description*, *Target Count*, *Retention Policy*, and *Polling Interval Value*.

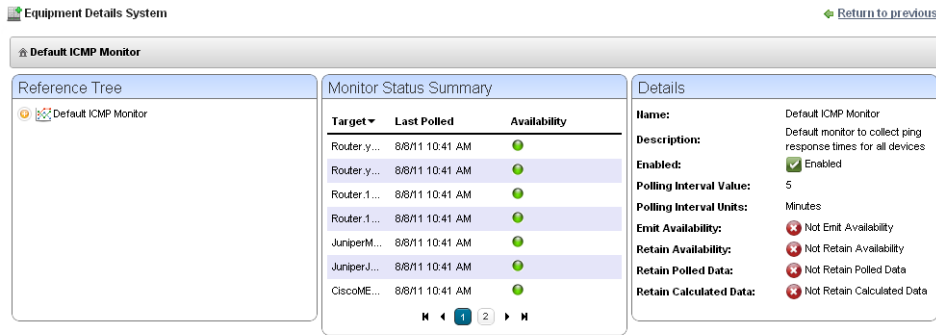


The graph that appears to the right of the monitors displays the aggregate availability information for the enabled monitors. Topics graphed include, *Available*, *Not Available*, *No Data* and *Not Applicable*.

Right-click a listed monitor to do the following (not all menu items appear for all types of monitors):

- New Monitor**—Lets you either create a new monitor of the type you select in the sub-menu, or edits the monitor selected in the portlet. See *Monitor Editor* on page 251 for details.
- New (from Template)**—Opens the Monitor Editor, where you can configure the equipment targets for template monitors, selected in the sub-menu. These templates already have selected attributes and calculations. You can examine exactly what these are in the editor that appears when you select one.
- Edit Monitor**—Opens the Monitor Editor, where you can modify the selected monitor.

**Details**—Opens a Detail panel, with a reference tree, status summary, and general information about the selected monitor.



**Enable / Disable Monitor**—Enables or disables the monitor. Only one of these options appears. Only enabled monitors report data (and demand resources), while disabled monitors do not.

**Refresh Monitor**—Re-query to update any targets for the current monitor. See *Scheduling Refresh Monitor Targets* on page 276 for instructions about automating this.

**Manage Retention Policies**—Select this to manage the data retention policies for the selected monitor. See *Retention Policies* on page 248 for details.

**Delete**—Removes the selected monitor.

## Expanded Resource Monitor

This screen appears when you click the plus in the upper right corner of the summary screen.

The screenshot shows the 'Resource Monitors' interface. At the top, there is a 'Default Active Monitor Filter' dropdown and an 'Advanced Filter' button. A search bar, refresh button, and settings icon are also present. The main area contains a table of monitors with columns for Name, Enabled, Description, Monitor Type, Polling Interval, Target Count, and Retention Policy. Below the table are three snap panels: 'Reference Tree' showing a hierarchy of 'TestACLI Monitor', 'Details' showing configuration for 'TestACLI Monitor', and 'Monitor Status Summary' showing a table of monitor status.

Name	Enabled	Description	Monitor Type	Polling Interval	Target Count	Retention Policy
TestACLI Monitor	<input checked="" type="checkbox"/>		Adaptive CLI	5 Minutes	2	Default
Default VM Monitor	<input checked="" type="checkbox"/>	Default key metrics monito...	Key Metrics	5 Minutes		Default
Default Juniper Monitor	<input checked="" type="checkbox"/>	Default key metrics monito...	Key Metrics	5 Minutes		Default
Default Interface Monitor	<input checked="" type="checkbox"/>	Default monitor to collect b...	SNMP Interfaces	5 Minutes		Default
Default ICMP Monitor	<input checked="" type="checkbox"/>	Default monitor to collect p...	ICMP	5 Minutes	2	Default
Default Cisco Monitor	<input checked="" type="checkbox"/>	Default key metrics monito...	Key Metrics	5 Minutes		Default

**Reference Tree**

- TestACLI Monitor
  - Monitor To Targets
  - Monitor To Trendable Attributes
  - Retention Policy
  - Membership

**Details**

NAME: TestACLI Monitor

DESCRIPTION:

ENABLED:  Enabled

POLLING INTERVAL: 5 Minutes

RETENTION POLICY:  Default

EMIT AVAILABILITY:  Not Emit Availability

RETAIN AVAILABILITY:  Not Retain Availability

RETAIN POLLED DATA:  Retain Polled Data

RETAIN CALCULATED DATA:  Retain Calculated Data

**Monitor Status Summary**

Target	Last Polled	Availability
JuniperMS...	8/15/11 10:19 AM	<input type="checkbox"/>
JuniperJ2...	8/15/11 10:23 AM	<input type="checkbox"/>

As in most expanded views, this one displays a list ordered by the *Name* of the monitor. Click *Settings* to configure the column display. Available columns include those on the summary screen (*Name*, *Enabled*, *Monitor Type*) as well as *Description*, *Poling Interval*, *Target Count* and *Retention Policy*.

## Resource Monitor Snap Panels

When you select a monitor, the Snap Panels at the bottom of the screen display details about it. The *Reference Tree* shows the selected monitor's connection to attributes, groups, retention policies and its membership (the devices monitored).

The *Details* Snap Panel displays the attributes the popup shows when you hover the cursor over the *Monitor Type* column in the summary screen, and adds *Emit Availability* (events), *Retain Availability*, *Retain Polled Data*, and *Retain Calculated Data* parameters.

The *Monitor Status Summary* Snap Panel displays the status of each individual member (*Target*) of the monitor, showing the *Last Polled* time and date, and a title bar and icon indicating *Availability* (green is available, red is not).

Hover the cursor over the Availability icon, and a popup appears with details about availability. If the device is available, the *RTT* (round-trip time) for communication appears in *Avg* (average), *Max* (maximum), and *Min* (minimum) amounts, along with the *PacketCount*. If it is not, an *Error Message* appears instead of the *RTT* and *PacketCount* parameters.

To edit more performance settings and targets than are available here, use the features described in *Dashboard Views* on page 277. You can create and display dashboards by right-clicking items in Managed Resources, selecting *Show Performance*.



### Excluding Attributes from Display

The `show.perf.exclude` property in the `portal-ext.properties` file contains a comma delimited list of the attribute display names to exclude from display. Remember, best practice is to override properties as described in *Overriding Properties* on page 23.

For example,

```
show.perf.exclude=CPU Utilization,AvgRTT
```

If you define this property, the *Show Performance* command creates charts for the listed attributes. This has no impact on manually created dashboards.

#### NOTE:

You must restart tomcat after changing the properties file for the changes to take effect.

## Retention Policies

The basis of all reporting and dashboard presentations is retained data from established monitors. In other words, each monitor provides a simple schema from which you can produce a chart, graph or report.



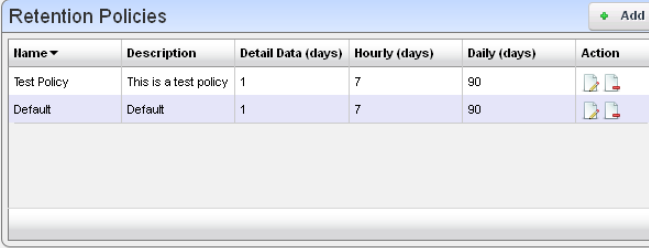
To reduce resource impacts, the scope of retained data may exclude some of the collected data. A monitor may have no retained data and only emit events based on transient results in the execution/calculation.





For example, the application can derive a metric from several collected values and you may opt to retain only the derived result.

All monitors rely on a polling engine which provides runtime mediation activities for distributed device interaction at regular intervals. Monitors may share a retention policy. Data is rolled up hourly and daily into summary data. The retention policy controls how long data is held per roll-up period.

When you manage these policies, you configure how monitored data is retained. When you select *Manage Retention Policies* in the Monitors portlet, first a list of available policies appears.

Clicking the *Add* button at the top of the screen lets you create a new policy, while clicking the *Edit* button to the right of selected, listed policies lets you modify existing policies. The *Delete* button to the right of listed policies removes them from the list.



Name ▼	Description	Detail Data (days)	Hourly (days)	Daily (days)	Action
Test Policy	This is a test policy	1	7	90	 
Default	Default	1	7	90	 

## Editor

Monitors may share a retention policy. The retention policy controls how long data is held per roll-up period. The editor for Retention policies lets you assign characteristics and monitors to them.

The screenshot shows a dialog box titled "General Retention Policy Options". It has two main sections. The top section, "General Retention Policy Options", contains five text input fields: "Policy Name" (Test Policy), "Description" (This is a test policy), "Detail Data (Days)" (1), "Hourly Data (Days)" (7), and "Daily Data (Days)" (90). The bottom section, "Active Monitor Members", contains two list boxes: "Available Monitors" (Default Cisco Monitor, Default ICMP Monitor, Default Interface Monitor, Default VMIL Monitor) and "Selected Monitors" (Default Juniper Monitor). Navigation arrows are between the lists. At the bottom are "Save" and "Cancel" buttons.

### General Retention Policy Options

The editor contains the following fields:

**Policy Name**—A text identifier for the policy.

**Description**—An optional description for the policy.

**Detail / Hourly / Daily Data (Days)**—How many days to retain the selected data.

The amount retained has both a performance and data storage impact. For example, retaining day's information from an active performance SNMP monitor configured with one target's worth of data, retrieved on one minute intervals can consume 0.7 G of database, and require 21 inserts per second.

Traffic flow analysis can process and retain even larger amounts of information. Flows that correlate 50%, polled every minute for a day require roughly 109G of database, and require 4500 inserts per second.

### Active Monitor Members

Select from *Available Monitors* on the left, and click arrows to move the desired monitor(s) to the *Selected Monitors* on the right.

Click *Save* to preserve your edits, and include the monitor as listed among existing Retention Policies, or click *Cancel* to abandon any changes.

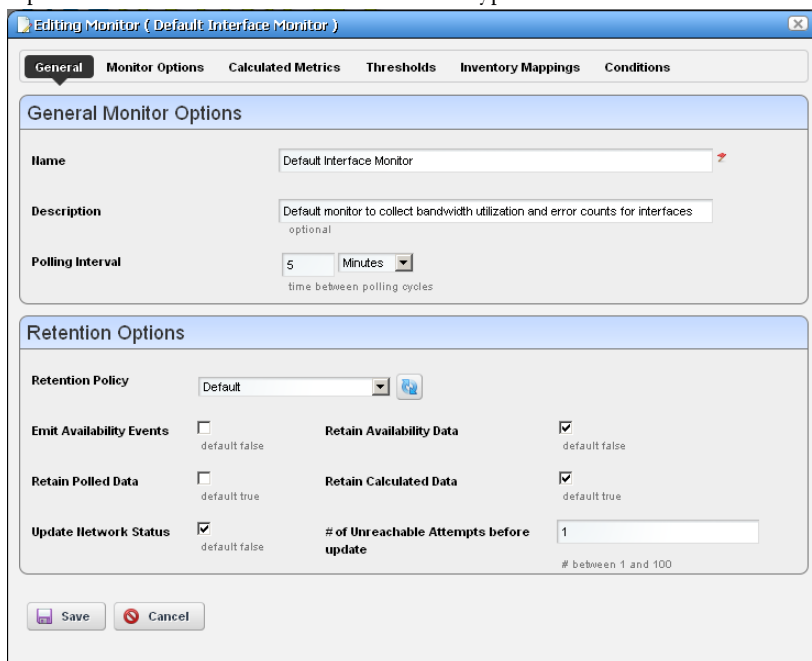
## Monitor Editor

This editor lets you fine-tune the monitor you selected and right-clicked to open the editor. It includes the following panels and fields:

- General
- Monitor Options
- Calculated Metrics
- Thresholds
- Inventory Mappings
- Conditions

### General

The General panel is common to all different monitor types.



The screenshot shows the 'Editing Monitor (Default Interface Monitor)' window. The 'General' tab is selected, showing the following fields:

- Name:** Default Interface Monitor
- Description:** Default monitor to collect bandwidth utilization and error counts for interfaces (optional)
- Polling Interval:** 5 Minutes (time between polling cycles)
- Retention Policy:** Default
- Emit Availability Events:**  (default false)
- Retain Availability Data:**  (default false)
- Retain Polled Data:**  (default true)
- Retain Calculated Data:**  (default true)
- Update Network Status:**  (default false)
- # of Unreachable Attempts before update:** 1 (# between 1 and 100)

Buttons for 'Save' and 'Cancel' are located at the bottom of the window.

### General Monitor Options

**Name**—The identifier for this monitor.

**Description**—A text description for this monitor.

**Polling Interval**—Use these fields to configure how often the monitor polls its target(s).

### **Retention Options**

**Retention Policy**—This configures how long Dell OpenManage Network Manager retains the monitor's data. Manage these by right-clicking in the Resource Monitors portal, and selecting *Retention Policies*. You must make retention policies before you can select them here.

**Enabled**—Check to enable.

**Emit Availability Events**—Check to activate emitting availability events. The monitor does not emit an event until the monitored entity's state has changed. All monitors can generate events on failure to contact the monitored device, port, and so on. For example, by default ICMP monitor updates the network status after a selected number of consecutive failures.

You can configure the monitor to generate an event in addition to updating network status, but Dell OpenManage Network Manager does not like the polling interval to be very small especially when monitoring many devices.

Example: poll every 10 secs for 10,000 devices with Packet Size = 64 bytes, Packet Count = 3 Timeout (secs) = 1, and configure Unreachable attempts = 1 with polling interval = 10 seconds. This polls the device every 10 seconds and emits a “down” event on the first failed attempt.

**Retain Availability Data**—Check to activate. You must Retain availability data to enable alarms. If you define thresholds, you should retain availability data. *Retain availability data* stores the Boolean values of whether availability data was in the range your defined metrics.

**Retain Polled Data**—Check to activate. If you uncheck *Retain polled data* only calculated data remains, you cannot view data retrieved from monitored entities. Turning off *Retain polled data* discards the data as it arrives from the device.

**Retain Calculated Data**—Check to activate. *Retain calculated data* complements *Retain polled data*. If checked, it stores the calculated results which came from the raw poll data received from the device.

**Update Network Status**—Check to activate reporting the network status of the target device(s). The results of this monitor's activity then appear in the Network Status column of the Managed Resources portlet.

Only one monitor—and no monitors on interfaces or child components—should ever update networks status. Any monitors on child components or interfaces are rolled up to the top level device, so status may be erroneously reported. For example the top level device is not necessarily down if the interace is down.

If two monitors report the network status of a single device on different intervals, they must both agree it is down before that state appears in Managed Resources. As long as one monitor says a device is Responding, then that is the state displayed.

If ping fails (an endpoint is down) and update network status is configured, then Dell OpenManage Network Manager tries to ping the switch/router in front of the endpoint to determine if that device is reachable. If that device also failed, then the endpoint's status becomes *indeterminate*.

 **Tip**

For clarity's sake, best practice has only one monitor per device updating network status. By default ICMP monitoring enables *Update Network Status*, and monitors all discovered devices.

 **NOTE:**

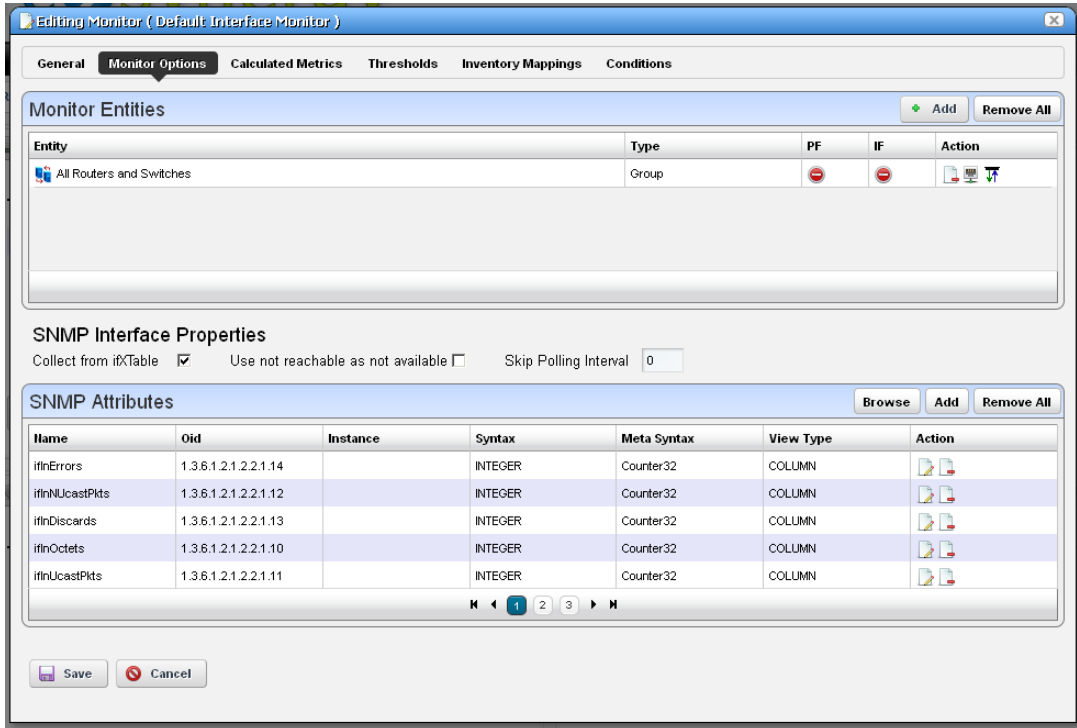
Migrating from previous versions automatically replaces any configured Heartbeats with ICMP monitors with *Update Network Status* enabled. If your previous system had HTTP or SNMP heartbeats, you must manually configure monitors to provide equivalent monitoring in this version.

**# of Unreachable Attempts before update**—The number of attempts to reach the device before Dell OpenManage Network Manager updates the displayed network status of the device. (1-100)

Click *Save* to preserve any edits you make, or *Cancel* to abandon them.

## Monitor Options

Monitor options contains two panels. The entity panel lets you select the monitor targets. The types of monitor entities allowed varies depending on the type of monitor. The second panel contains options specific to the monitor type being edited.

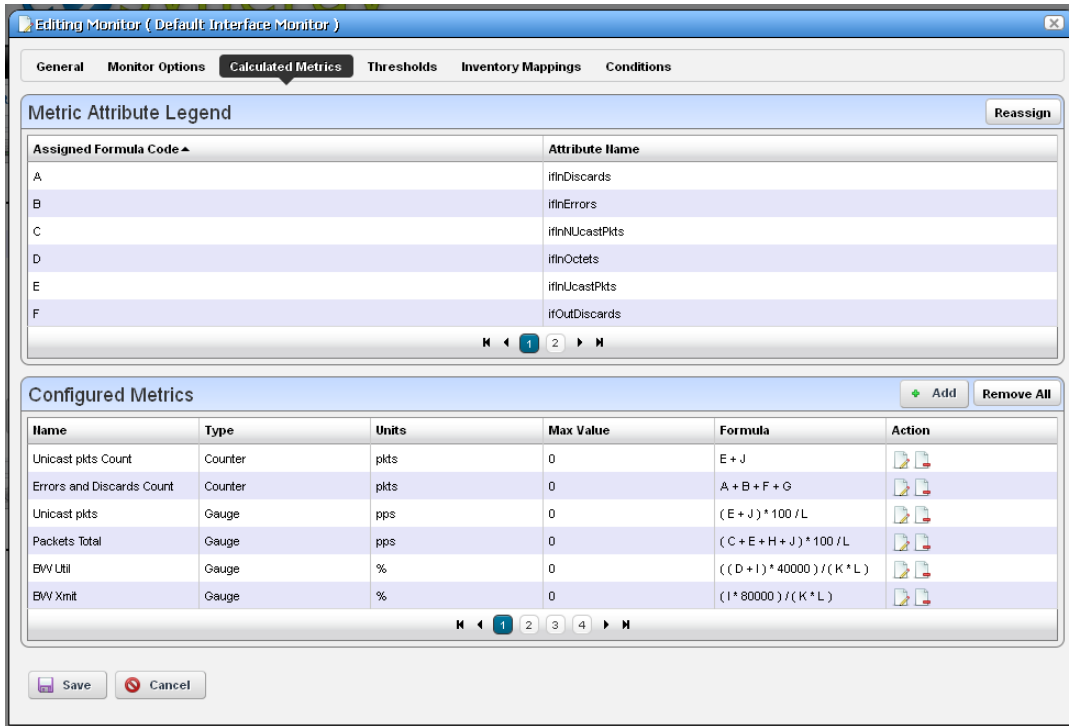


The entity and options panels for the various types of monitors appear below in *Monitor Options Type-Specific Panels* on page 266.

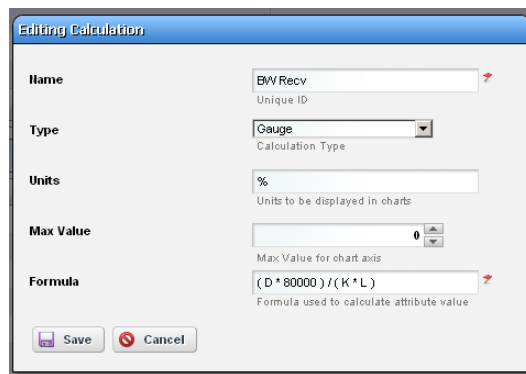
## Calculated Metrics

The calculated metrics panel lets you create attributes that are calculated from existing monitor attributes. The metric attribute legend assigns a letter value to each monitor attribute. The *Reassign* button reassigns the letters. This is useful if some attributes have been deleted and their letters are no longer used.

The *Configured Metrics* table lists the calculated metrics. An edit and delete action appears to the right of each row. The *Add* button creates a new calculated metric and the *Remove All* button deletes all the calculated metrics.



Clicking on the Add button or edit button displays the calculation editor.



This panel contains the following properties:

**Name**—The attribute name to be displayed for the calculation

**Type**—Calculation Type - Gauge or Counter

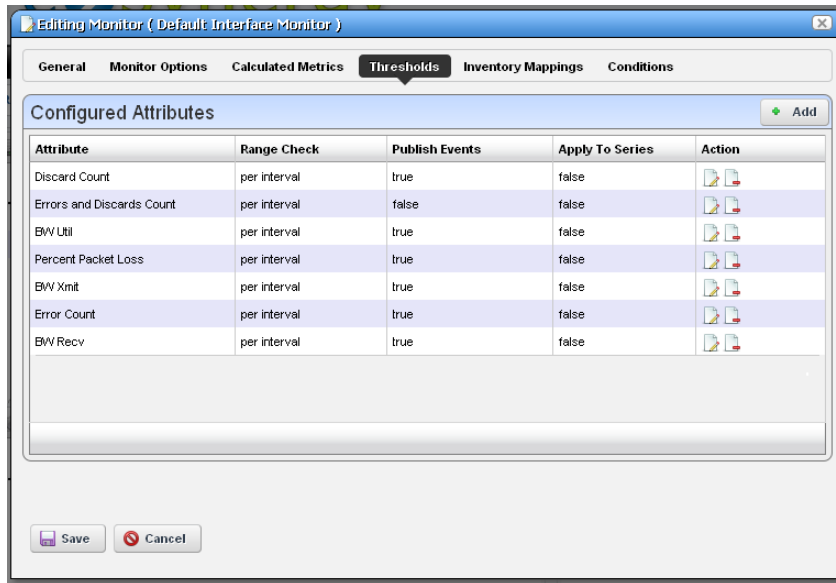
**Units**—Units string to appear in graphs

**Max Value**—Maximum value to be used in graphing (0 = no max)

**Formula**—The formula for the calculation using the assigned formula codes from the metric attribute legend.

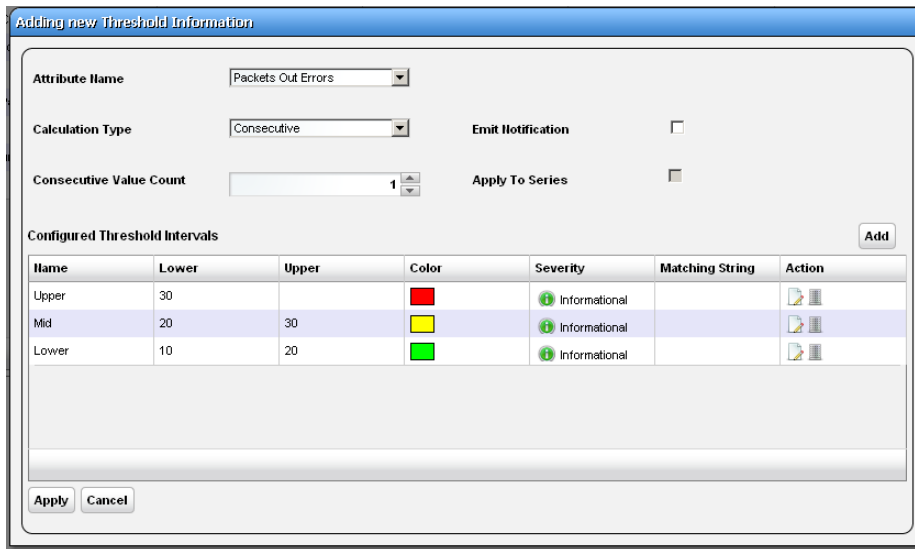
## Thresholds

The thresholds panel allows the user to set threshold intervals on attributes in the monitor. The table lists the attributes for which attributes have been configured. Each row has an edit action and delete action. The Add button allows thresholds to be specified for another attribute. If all monitor attributes have thresholds defined for them the Add button will be disabled.





The *Add* or *Edit* buttons open a threshold editor (blank or with existing, configured thresholds, respectively).




Configure threshold intervals you *Add* at in the editor screen according to the following parameters.

**Attribute Name**—Appears when you click *Add* rather than *Editing* a selected threshold. Use the pick list that appears in this screen to select the attribute for which you are specifying threshold information. When you *Edit*, the name of the attribute appears as a title within the editor screen.

**Calculation Type**—Select from the pick list. Specifies whether the range calculation is to be done based on *Average* or *Consecutive* values.

**Consecutive Value Count**—Select how many consecutive values to consider at once for a range calculation. Typically the larger the number here, the less “flutter” in reporting threshold crossings.

**Emit Notification**—Check to emit an event if the device crosses the configured threshold(s). The notification event contains the threshold-crossing value, as well as which threshold was crossed, and is an alarm at the severity selected when you configure the threshold.

 **Tip**

You can make a set of thresholds for each monitored attribute, so a single monitor can throw different alarms for different attributes. To see available events and their descriptions, view the contents of the RedcellMonitor-MIB in `\owaareapps\performance\mibs`.

**Apply to Series**—Check to enable on composite attributes only. Checking this applies the threshold to individual elements within the series. When it is unchecked, the threshold applies only to aggregate measurements (the overall value of the series), not individual elements within the series.

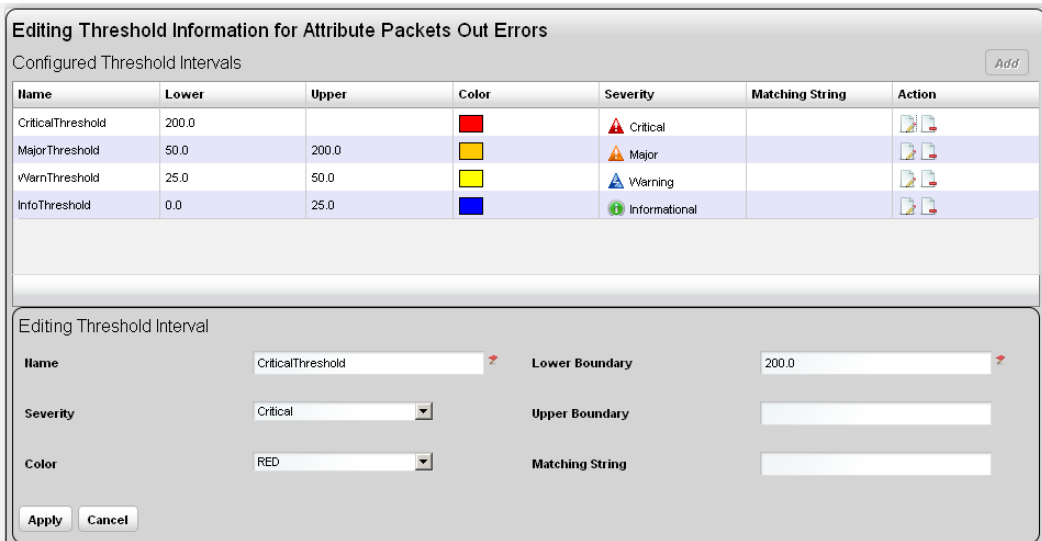
For example; a Key Metric monitor for CPU utilization on a device with two CPUs actually monitors both CPUs. When unchecked, the threshold applies to the average of both CPUs, when checked, the threshold applies to each individual CPU.

 **Tip**

When you check this, you can also apply thresholds to regular expressions. This is useful to monitor components within components, for example cores within a CPU.













Click *Apply* to preserve your edits, or *Cancel* to abandon them.

The threshold interval editor pops up when you select the *Add* button or the *Edit* icon to the right of a threshold’s row in the threshold attribute editor.





**Editing Threshold Information for Attribute Packets Out Errors**

Configured Threshold Intervals Add

Name	Lower	Upper	Color	Severity	Matching String	Action
CriticalThreshold	200.0		<span style="color: red;">■</span>	 Critical		 
MajorThreshold	50.0	200.0	<span style="color: yellow;">■</span>	 Major		 
WarnThreshold	25.0	50.0	<span style="color: yellow;">■</span>	 Warning		 
InfoThreshold	0.0	25.0	<span style="color: blue;">■</span>	 Informational		 

Editing Threshold Interval

**Name**   **Lower Boundary**  

**Severity**  **Upper Boundary**

**Color**  **Matching String**

This screen contains the following fields:

**Name**—The identifier for the threshold interval.

**Severity**—The event severity for crossing this threshold interval (*informational/indeterminate/warning/minor/major/critical*)

**Color**—The color to display threshold interval on graphs.

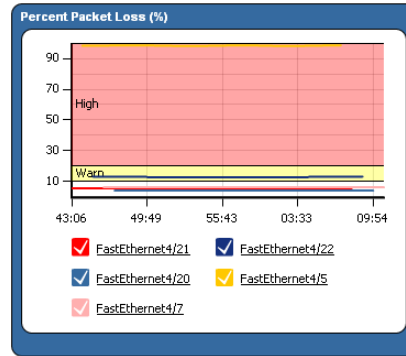
**Lower Boundary**—The interval’s lower boundary.

**Upper Boundary**—The interval’s upper boundary. May be blank.

**Matching String**—A Regex matching string.

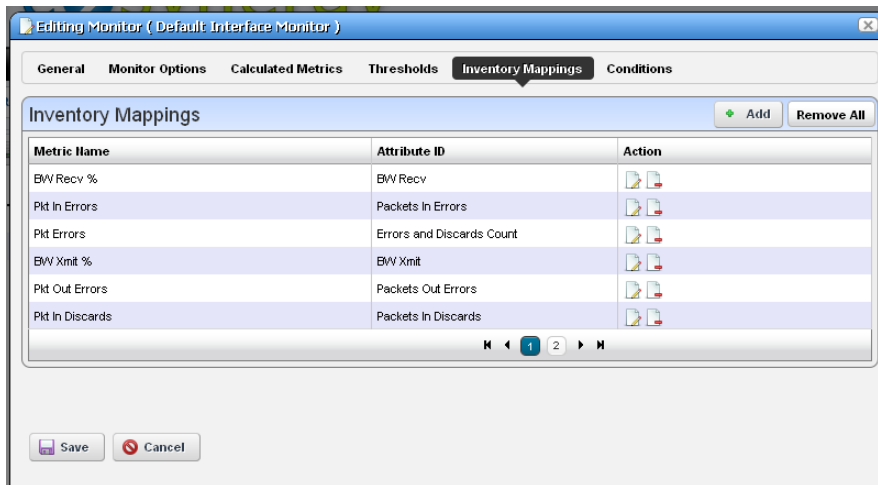
## Threshold Graph Background

If you configure a set of thresholds, the dashboard graph displaying the data monitored displays the threshold colors in the background. When an upper or lower threshold has no upper or lower bound, then those background colors may appear as white.

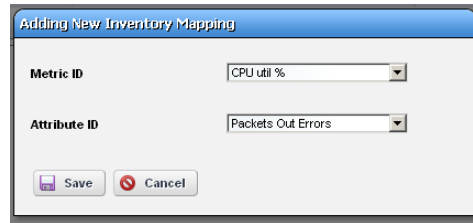


## Inventory Mappings

The inventory mappings panel allows the user to associate any of several predefined inventory metrics with a monitor attribute. The available metrics are *CPU Utilization %*, *Memory Utilization %*, *ICMP Round Trip Time*, *ICMP packet errors*, and *Bandwidth utilization %*.



You can *Add* a new mapping with that button, or *Remove All* listed mappings with that button. You can also edit or delete listed mappings with the *Action* icons to the right of each row. Adding or editing opens the Inventory Mapping Editor.



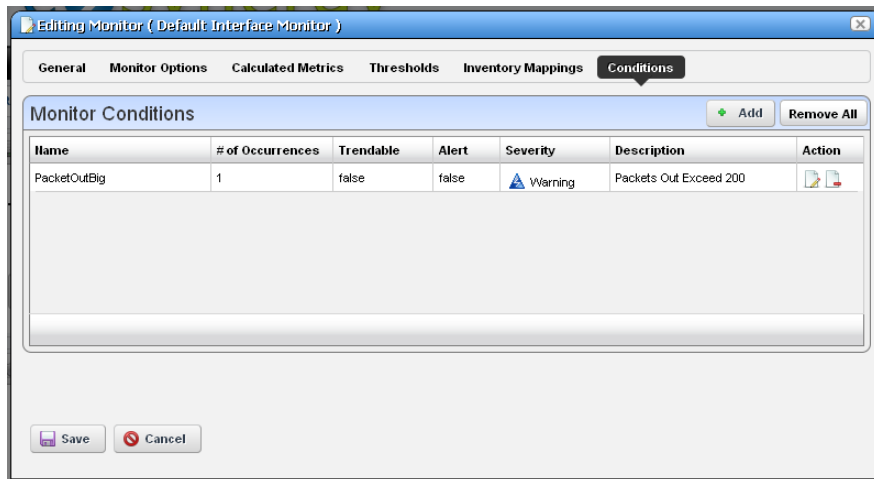
This lets you configure the following:

**Metric ID**—Inventory metric name

**Attribute ID**— Attribute to associate with the inventory metric

## Conditions

This panel lets you add multiple conditions to the monitor you are editing.



Click the *Add* button to enter a new set of conditions, or click the *Edit this entry* button to the right of a listed Monitor Condition to open the editor. Click the *Delete* button to remove a listed set of conditions. Click the *Copy* icon to duplicate the listed condition.

The editor has the following fields and settings to configure:

The screenshot shows a window titled "Adding New Condition". It contains the following sections:

- Condition Properties:**
  - Name: PacketOutBig
  - Alert:
  - Trendable:
  - # of Occurrences: 1
  - Severity: Warning
  - Description: Packets Out Exceed 200
- Condition Filter:**
  - Filter Criteria: AND (Match All of the following)
- Criteria Group:**
  - Match All (selected) / Match Any
  - Clear Conditions
  - Criteria list:
    - Packets Out Errors > greater than > 200
    - ifSpeed > greater than > 10000
  - Apply button

Buttons at the bottom: Save, Cancel.

### Condition Properties

**Name**— Enter a text identifier for the conditions.

**Alert**— Check this if you want Dell OpenManage Network Manager to emit an alert when the monitor satisfies the conditions.

**Trendable**— Check if the conditions specified are trendable.

**Severity**— Specify the severity of the emitted alert, if any.

**# of Occurrences**— Enter the number of occurrences of what is specified in the Condition Filter to satisfy the Conditions.

**Description**— A text description for the conditions.

### Condition Filter

Minimally, use this panel to select a condition, an operator and a value. If you want to use the logical AND or OR operators with a second condition, click the green plus (+), and select a second condition, operator and value. For example, *Packet Out Errors greater than 200 AND ifSpeed greater than 10000* can be a set of conditions that only has to occur once to satisfy this monitor's condition.

Click *Save* to accept your edits, or *Cancel* to abandon them.



## How To:

### Create an SNMP Interface Monitor

To set up a typical performance monitor, follow these steps:

- 1 In the *Resource Monitors* portlet, and create a new monitor by right-clicking and selecting *New*.
- 2 Select the type of monitor from the submenu—for this example, an *SNMP Interfaces* monitor.

#### NOTE:

Some devices have ports rather than interfaces. This monitor works for them too, even though it is an “interface” monitor.

- 3 In the *General* screen, enter a polling interval (5 minutes is the default). For this example, check *Retain polled data* and accept the remaining defaults for checkboxes and the retention policy.
- 4 Select an entity to monitor by clicking the *Add* button in the top portion of the *Monitor Options* screen. For an interface monitor, select *Interface* as the *Type* at the top of the screen. You can also filter the list of interfaces that appear further by selecting *Interface Type* as *ge* (gigabit ethernet), for example.

#### Tip

Notice that you can add refinements like filtering on *Administrative State* and *IP Address* to the filter.

- 5 Select interfaces (Ctrl+click to add more than one), then click *Add Selection* then *Done* to confirm your entity.


#### Tip

Hover your cursor over a line describing an interface to have a more complete description appear as a popup.

- 6 Click *Browse* to display the MIB Browser. For the sake of this example, we elect to monitor *ifInErrors* (in RFC Standard MIBs, RFC1213-MIB > Nodes > mib-2 > interfaces > ifTable > ifEntry > ifInErrors).
- 7 In the *Thresholds* screen, configure thresholds by first clicking *Add*.
- 8 Click *Add* above the threshold levels list for each threshold you want to add.
- 9 In the threshold editor, enter a name (Examples: *Low*, *Medium*, *Overload*), an upper and lower boundary (0 - 10, 10 - 100, 100+), a severity (*Informational*, *Warning*, *Critical*) and color (BLUE, YELLOW, RED). In this case, no string matching is necessary. When the data crosses thresholds, the monitor reacts.

Attributes available depend on the type of monitor you are creating. Notice that you can also check to make crossing this threshold emit a notification (an alarm that would appear on the Alarm panel). You can also configure the type of calculation, and so on. You can even alter existing thresholds by selecting one then clicking *Edit* to the right of the selected threshold.

- 10 Click *Apply* for each threshold interval you configure, then *Apply* for the entire threshold configuration.

 **NOTE:**

If a threshold's counter is an SNMP Counter32 (a 32-bit counter) monitoring can exceed its capacity with a fully utilized gigabit interface in a relatively short period of time. The defaults configured in this monitor account for this, but if you know that this is an issue, you can probably configure the monitor to account for it too.

After taking a look at Thresholds no more configuration is required. Notice, however, that you can also configure *Calculated Metrics*, *Inventory Mappings* and *Conditions* on other screens in this editor to calculate additional values based on the monitored attributes, to map them, and to make conditional properties based on monitored behavior.

 **Tip**

*Calculated Metrics* is particularly valuable if you want to monitor a composite like `ifInErrors + ifOutErrors` or want to calculate a parameter like errors per minute when you have a 5-minute monitoring interval.

- 11 Click *Save* and the monitor is now active.

Notice that the *Availability* icon appears at the top of a *Monitor Status Summary* snap panel in the Expanded Resource Monitor next to a time/date stamp of its last polling. Right-click the monitor and select *Refresh Monitor* to manually initiate polling.

Values displayed in the Overall Availability column of the Monitor Manager do not automatically refresh and may be out of date. The *Reference Tree* snap panel maps the monitor's relationship to its target(s) attribute(s) and other elements. The *Details* snap panel summarizes the monitor's configuration.

- 12 For information about having the monitor's results appear in the a *Dashboard* portlet, see *Dashboard Views* on page 277.



## How To:

### Create an ICMP Monitor

The following steps create an ICMP (ping) monitor.

- 1 In the *Resource Monitors* portlet, and create a new monitor by right-clicking and selecting *New*.
- 2 Select the type of monitor from the submenu—for this example, an *ICMP* monitor.

- 3 In the *General* screen, enter a name (Test ICMP Monitor), and a polling interval (5 minutes is the default). For this example, check *Retain polled data* and accept the remaining defaults for checkboxes and the retention policy.
- 4 Select an entity to monitor by clicking the *Add* button in the top portion of the *Monitor Options* screen.
- 5 Select devices you want to ping, (Ctrl+click to add more than one), then click *Add Selection* then *Done* to confirm your entity.
- 6 Define packets in the ICMP Monitor Options panel, including Packet Size, Packet Count and timeout. You can accept the defaults here, too.
- 7 In the Thresholds tab, select an attribute (MaxRTT, or maximum round trip time) and add the following thresholds by clicking *Add*:  
 Name *High* color red, Lower Boundary 15 and Upper Boundary [blank] Severity *Critical*  
 Name *Fine* color green, Lower Boundary 0 and Upper Boundary 15 Severity *Cleared*.  
 Notice that this example does not emit a notification. If you checked that checkbox, an alarm of the configured severity would accompany crossing the threshold.
- 8 Accept the other defaults and click *Apply*
- 9 Click *Save*.
- 10 Test ICMP Monitor now appears in the portlet.



## How To:

### Create a Key Metrics Monitor

Follow these steps to create a Key Metrics Monitor (also, see *Key Metric Editor* on page 289).

- 1 In the *Resource Monitors* portlet, and create a new monitor by right-clicking and selecting *New*.
- 2 Select the type of monitor from the submenu—for this example, an *Key Metrics* monitor.
- 3 In the *General* screen, enter a name (Test Key Metrics Monitor), and a polling interval (5 minutes is the default). For this example, check *Retain polled data* and accept the remaining defaults for checkboxes and the retention policy.
- 4 Select an entity to monitor by clicking the *Add* button in the top portion of the *Monitor Options* screen.
- 5 Select devices on which you want to monitor Key Metrics.
- 6 Select from the available metrics that appear at the bottom of the screen in *Key Metric Properties* by selecting a category with the pick list at the top of the screen, then click on an *Available* metric, and click the right arrow to make it a *Selected* metric.
- 7 Click *Save* to retain your new Monitor.



- 8 Test Key Metrics Monitor appears in the Resource Monitors portlet.



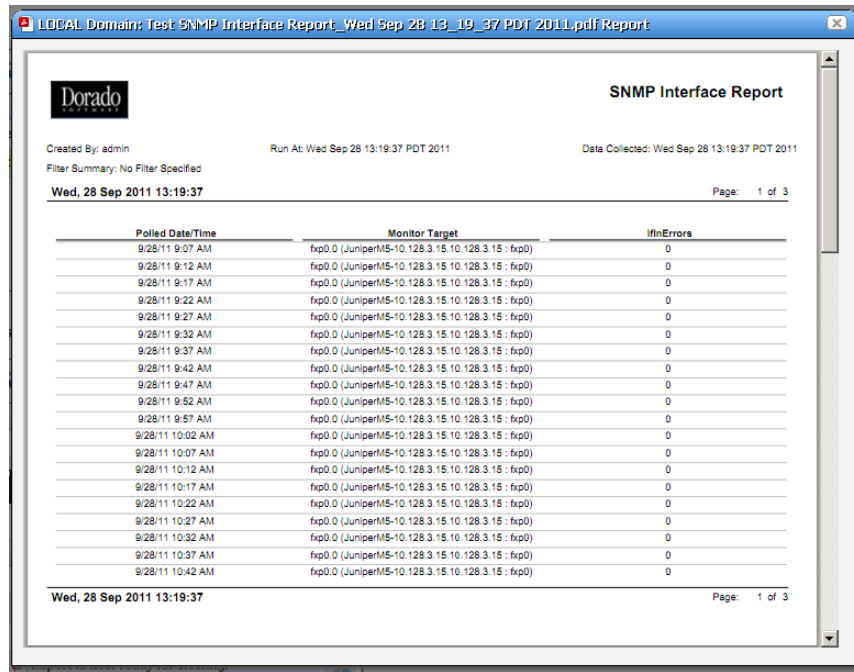
## How To:

### Create a Monitor Report

You can create reports based on your monitors. The following example creates a report based on How to: Create an SNMP Interface Monitor above.

- 1 Create a new Report Template by right-clicking the Report Templates portlet, selecting *New > Table Template*.
- 2 Name the report (here: Test SNMP Interface Report).
- 3 Select a source in the *Source* tab. Here: *Active Monitoring > SNMP Interfaces*.
- 4 Notice that the *Select your inventory columns* panel displays the attributes available based on your monitor selection.
- 5 Select *Available* columns and click the right arrow to move them to *Selected*. In this case we select SNMP Interfaces: Monitor Target, Polled Date / Time, ifInErrors.
- 6 Arrange the columns and fonts as you like in the *Layout* tab.
- 7 *Save* the template.
- 8 Right-click, and select *New* in the Reports portlet.
- 9 Enter a *Name* and *Title* for the report.
- 10 Notice that since this is the first report created since you made the Test SNMP Interface Report template, that it is the *Report Template* already selected.
- 11 Since the monitor already filters devices, we add no filter in the Report, although you could add one to further filter the monitored devices.
- 12 Test SNMP Interface Report should appear in the Reports portlet.
- 13 Right-click and select *Execute* (noticing that you can also schedule such reports, even repeatedly).

- 14 Click the magnifying glass to the right of the Report Completed message in My Alerts to see the report.



- 15 Hover your cursor over the lower right corner of the report to see a set of icons that let you expand, zoom out and in, save, or print the report.



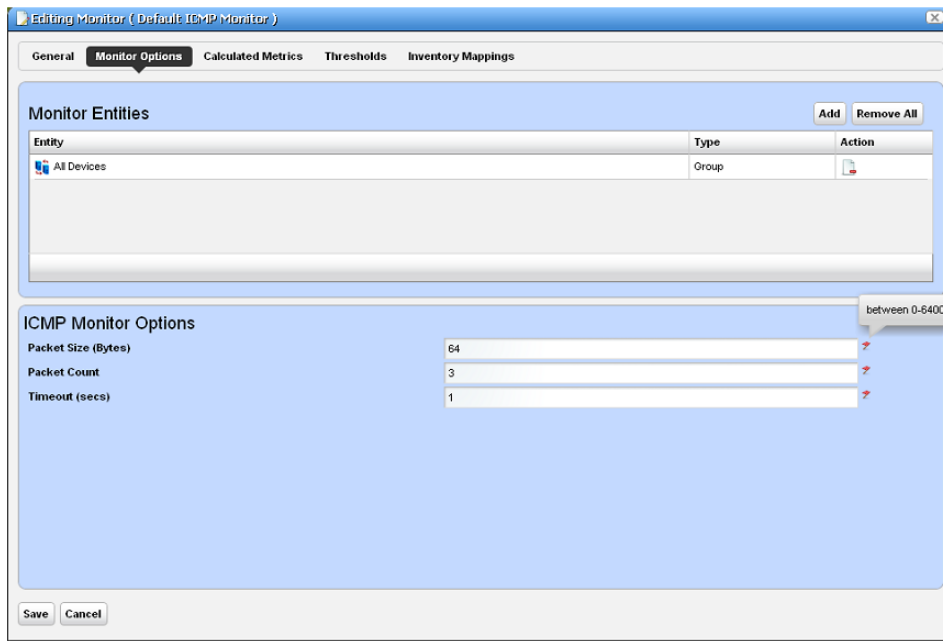
## Monitor Options Type-Specific Panels

The following describes the panels associated with the following Monitor Options types.

- ICMP
- Key Metrics
- Proscan
- SNMP
- SNMP Interfaces
- SNMP Table Monitor

## ICMP

The ICMP Monitor Options panel contains the following properties:



**Packet Size**—Size of packet for ICMP transmission

**Packet Count**—Number of packets to send.

**Timeout**—Number of seconds without a response before a timeout is issued

The ICMP Entity Panel lets you select resource groups and Resource manager objects. Clicking *Add* button displays a selector panel for these.



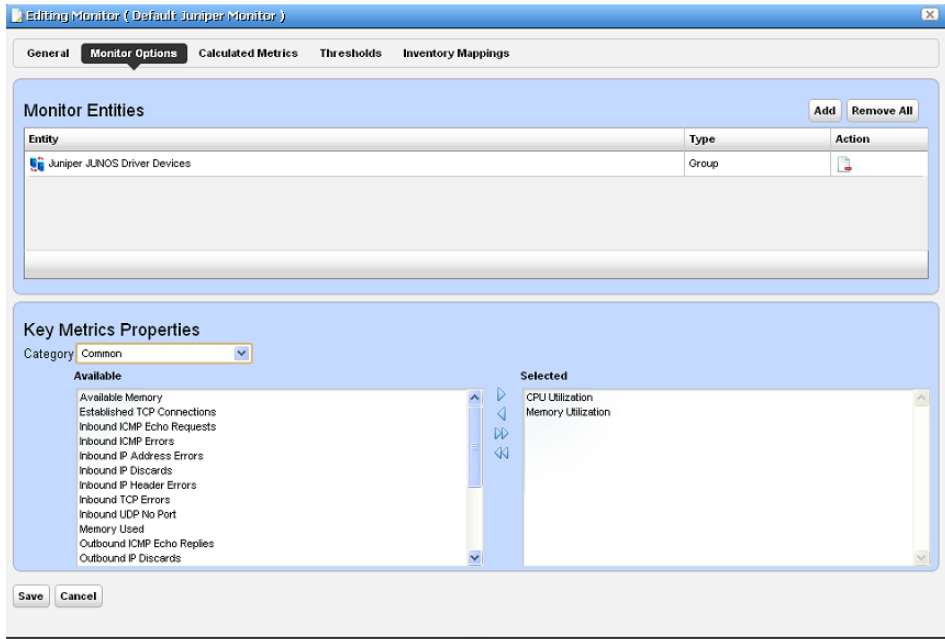
Select the type of entity you want to add, then select any desired filter attributes, then click *Apply Filter*. Select from the entities that appear and add them to the monitor.

 **NOTE:**

Migrating from previous versions updates the Network Status check box to true and redeploys the monitor.

## Key Metrics

The Key Metrics Properties panel contains a list of key metrics you can add to the monitor. They are grouped by category.

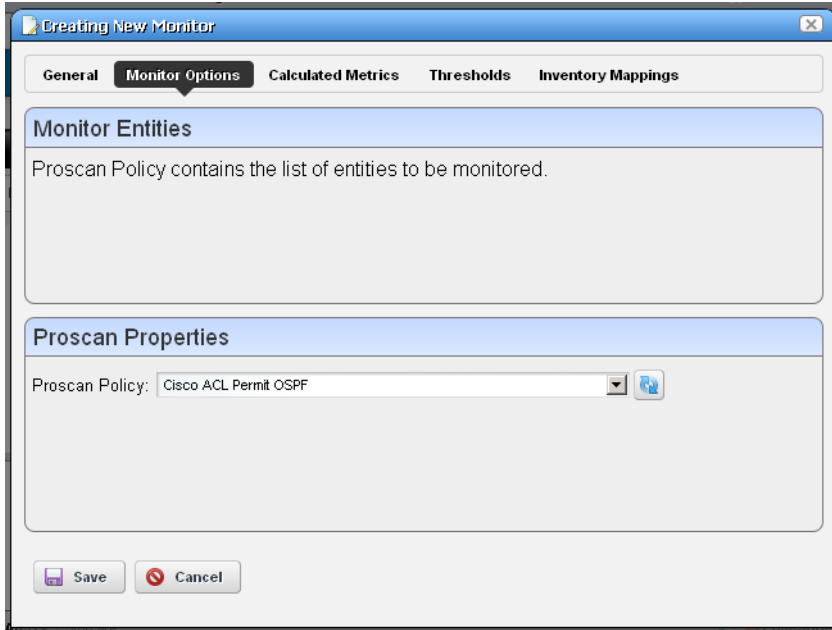


The Monitor Entities Panel lets you select equipment group and equipment manager objects (as described in *ICMP* on page 267, above).

The Key Metrics Properties panel at the bottom of this screen uses a pre-defined list of key metrics. It does not check if the key metrics selected are supported by the devices and groups selected in the monitor.

## Proscan

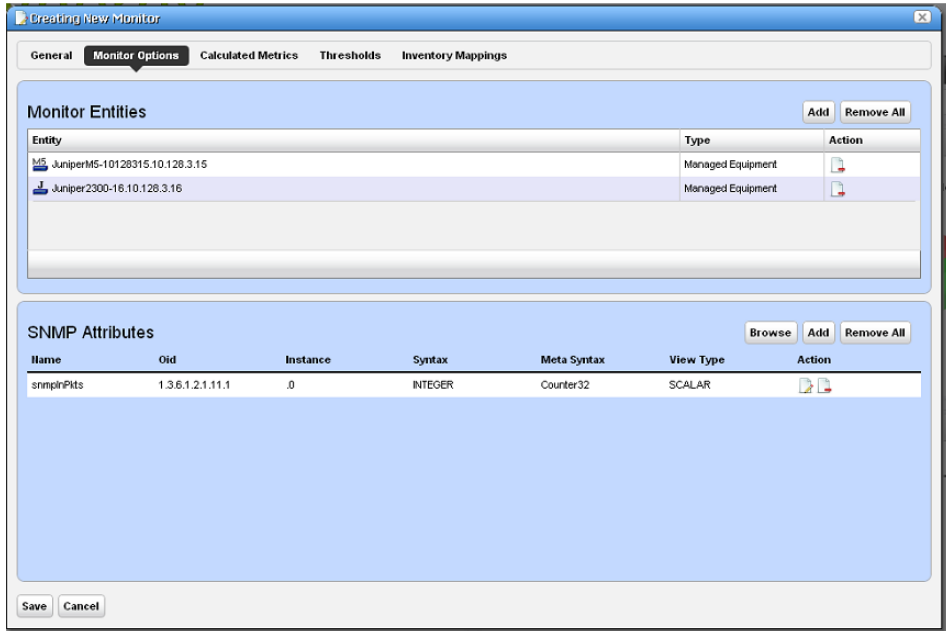
In this screen, you simply select the Proscan policy to monitor. In the Thresholds tab, you can set thresholds for both in and out of compliance numbers.



The Proscan policy contains the target network assets.

## SNMP

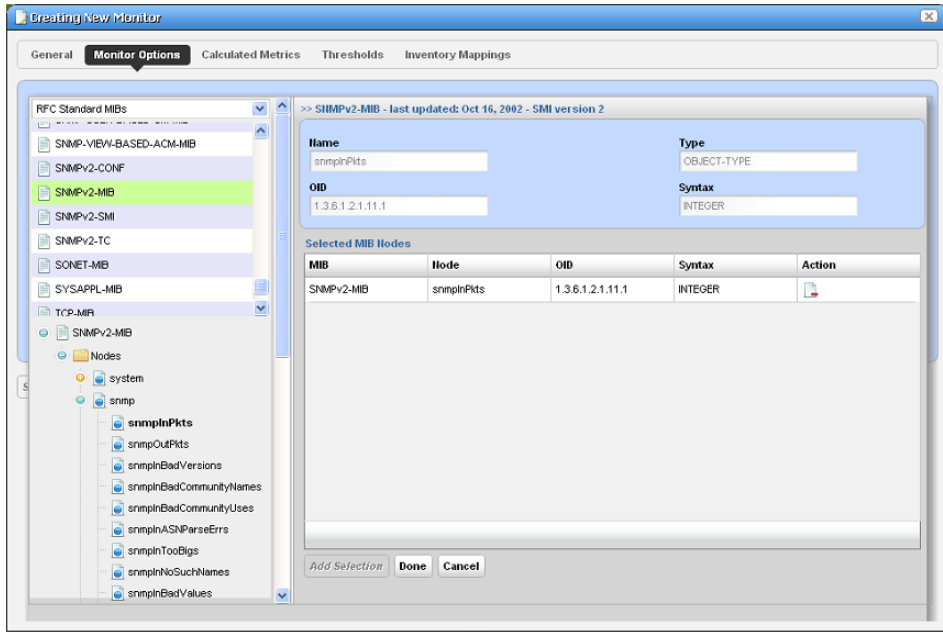
The SNMP attributes panel lets you specify which SNMP attributes are to be monitored.



Specify SNMP attributes as follows:

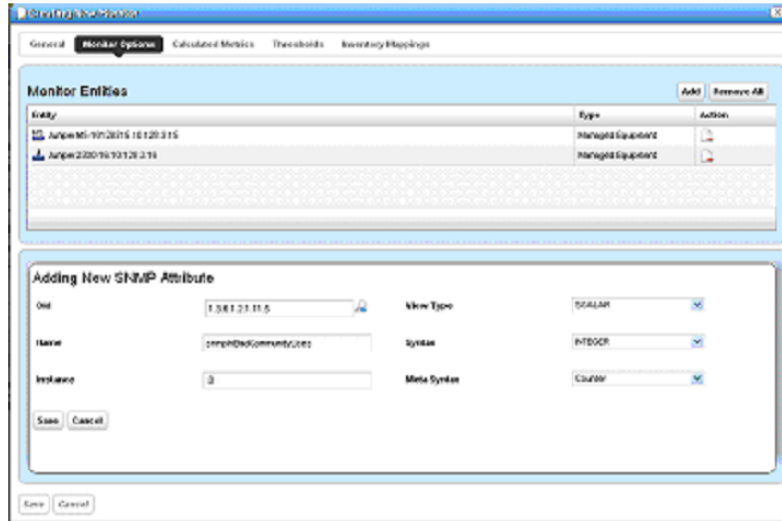
- With the SNMP browser, or
- Entering SNMP attribute properties explicitly.

The *Browse* button launches the SNMP browser.



Click on the desired SNMP nodes and then click on the *Add Selection* button to add an SNMP attribute. When done selecting, click the *Done* button to add selected attributes to the monitor or *Cancel* to abandon the operation and close the browser.

The Add and Edit buttons in the SNMP attribute panel launch the SNMP Attribute editor.



This panel contains the following properties:

**Oid**—The object identifier for this attribute

**Name**—This attribute’s name

**Instance**—SNMP instance. 0 for scalar or the ifIndex value for an SNMP column.

**View Type**—*Scalar* or *Column*.

**Syntax**—*Integer*, *Boolean*, *DisplayString*, and so on.

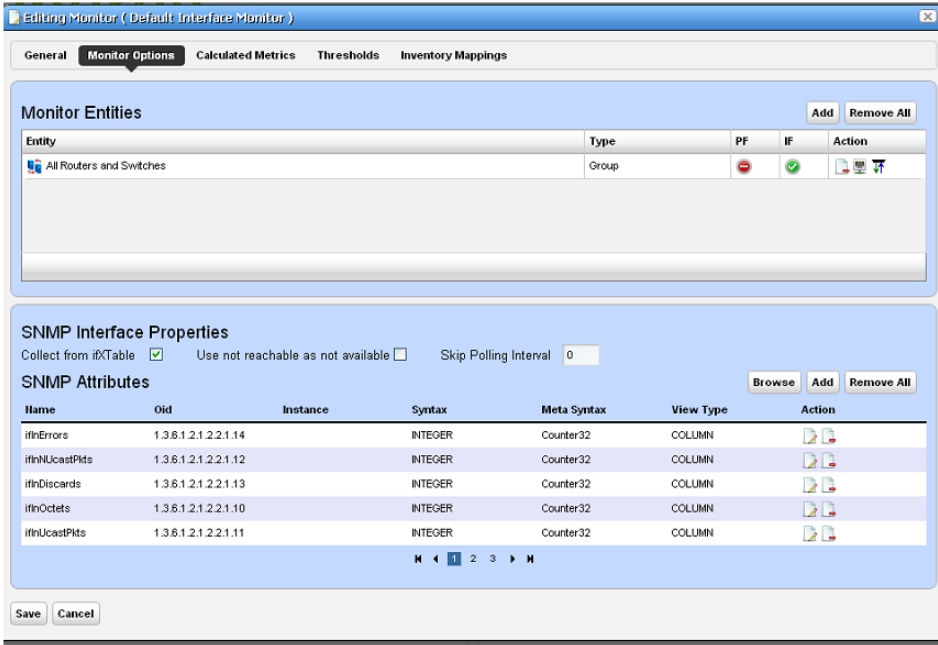
**Meta Syntax**—*Counter*, *Gauge*, and so on.

If you type in an OID and click the search button next to the OID field, the browser searches the MIB for the OID and fills in the other values if it finds the OID.

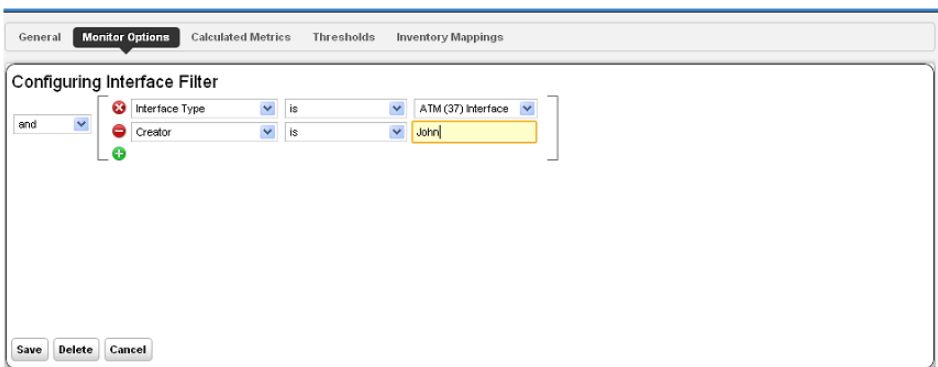


## SNMP Interfaces

The SNMP Interface Monitor Entity editor supports the following entity types: group, equipment manager, port and interface. It also supports port and interface filters on groups and equipment manager objects.



The PF and IF table columns indicate if a port filter or interface filter is configured for the entity. Click the icons on the right side of the list of Monitor Entities to configure filters. Clicking these buttons displays an interface configuration panel.

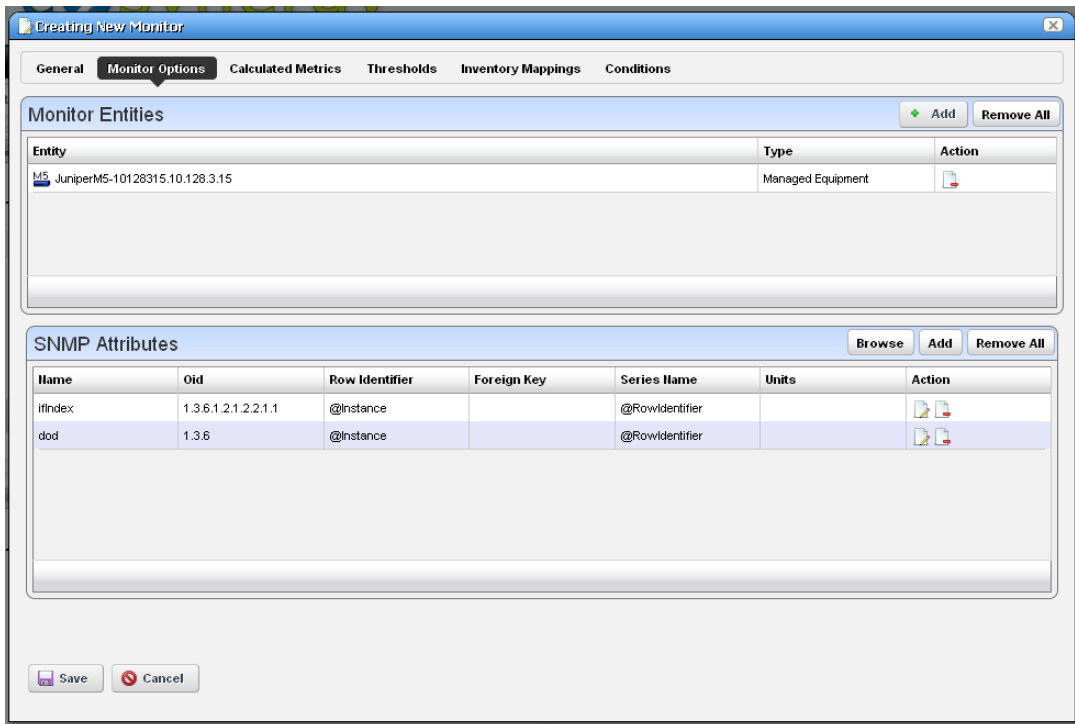


This panel lets you specify filter attributes for the port or interface filters you want to monitor. For example, if you select a device but only want to monitor active interfaces created by a particular user, then these filters do the job.

The SNMP Attributes panel is the same as described in *SNMP* on page 270.

## SNMP Table Monitor

This panel appears if you are creating an SNMP Table monitor. The application stores not absolute numbers from counters but the counter's change since its last measurement.



Columns include the SNMP Attribute Name, OID, Row Identifier, Foreign Key, Series Name, Meta Syntax, Units, and Action.

If you check the Collect from ifXTable checkbox, then OpenManage Network Manager attempts to fetch attributes from the ifXTable. These attributes are ifHighSpeed, ifHCInOctets, ifHCInUcastPkts, ifHCOutOctets and ifHCOutUcastPkts. If any of these attributes are not available, then it fetches from ifTable.

Clicking the *Add* or the *Edit* button to the right opens either a MIB Browser where you can retrieve these attributes, or an Add / Edit SNMP Attributes editor at the bottom of the screen. See the following sections for details.

## MIB Browser

This lets you select attributes to monitor as described in *MIB Browser* on page 188. The SNMP table monitor lets you pick a table column, not the entire table.

## Add / Edit SNMP Attributes

This screen lets you specify individual attributes.

The screenshot shows a window titled "Creating New Monitor" with several tabs: "General", "Monitor Options" (selected), "Calculated Metrics", "Thresholds", "Inventory Mappings", and "Conditions".

Under the "Monitor Options" tab, there is a section titled "Monitor Entities" with "Add" and "Remove All" buttons. It contains a table with the following data:

Entity	Type	Action
M5 JuniperM5-10128315.10.128.3.15	Managed Equipment	[Icon]

Below the table is a section titled "Adding New SNMP Table Attribute" with the following fields:

- Oid**: [Text input field with a magnifying glass icon]
- Name**: [Text input field]
- Series Name**: [Text input field with value "@RowIdentifier"]
- Meta Syntax**: [Dropdown menu with value "Counter"]
- Row Identifier**: [Text input field with value "@Instance" and a red arrow icon]
- Foreign Key**: [Text input field]
- Units**: [Text input field]

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

It has the following fields:

**Oid**— A field where you can enter the object identifier. This also has an integrated search function. Click the magnifying glass icon on the right to activate it. A successful search populates the rest of the fields for the object identifier.

**Row Identifier**—This mandatory field defaults to @instance (The OID instance).

**Name**—The text identifier for the OID

**Foreign Key**—Enter the foreign key, if any.

**Series Name**—This defaults to @RowIdentifier.

**Units**—Enter the units of measurement.

**Meta Syntax**—Further refine the variable type with the pick list. For example, you can select *Counter32* (a 32-bit counter). For Counter types, the monitor computes change from previous readings, and for Gauges it does not.

 **NOTE:**

If a message appears saying: “Device fault: Return packet too big” in the Monitor Status Summary, then you have selected too many SNMP attributes to poll in a single request. Please modify your monitor to request smaller numbers of attributes

## Scheduling Refresh Monitor Targets

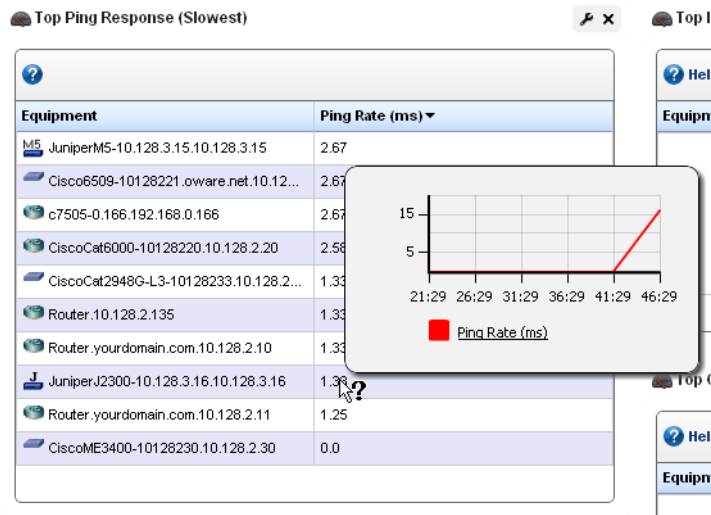
Because monitors can address targets that are members of dynamic groups, refreshing these ensures that group memberships are up-to-date. To do this, you can create or alter the schedule for Monitor Target Refresh. When executed, this updates monitors with groups as targets based on current memberships. This removes targets no longer members of a monitored group and adds new group members. A seeded schedule refreshes these every six hours, by default.

 **Tip**

You can also *Refresh Monitor* manually by right-clicking in the Resource Monitors table.

## Top [Asset] Monitors

Dell OpenManage Network Manager uses seeded, default Active Performance Monitors (APM) to display performance data in several categories. These portlets display the summary results of device monitoring, for example, the devices slowest to respond to ping.



Devices appear, ranked by the monitored parameter. Hover the cursor over a row's summary graph of *Ping Rate* and a popup graph of recent activity over time appears.

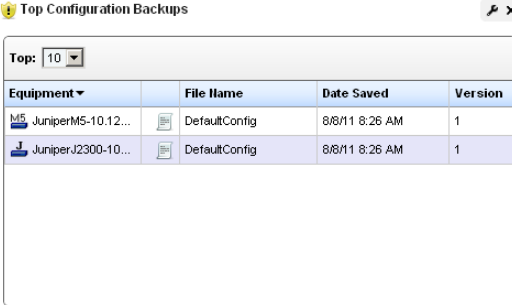
If you right-click a monitored item, you can select from menu items like those that appear in the portlet described in *Managed Resources* on page 166.

For some portlets (for example Top CPU Utilization, Top Interface Errors and Top Memory Utilization), the right-click Performance menu items include Key Metrics. The menu can include *Performance* which displays Dashboard Views related to the selected monitor.

## Top Configuration Backups

This panel lists the most recent configurations backed up from devices. The pick list in the upper right corner lets you select not just the top 10 such backups, but the top 5, 10, 15, 20, and 25.

Right-clicking a backup offers the same options as the portlet described in *Configuration Files* on page 229.




Equipment	File Name	Date Saved	Version
MS JuniperMS-10.12...	DefaultConfig	8/8/11 8:26 AM	1
J JuniperJ2300-10...	DefaultConfig	8/8/11 8:26 AM	1

## Dashboard Views

The Dashboard Views portlet lets you assemble several monitors into a single display, or dashboard. You can create and display dashboards by right-clicking items in Managed Resources, selecting *Show Performance*, or by selecting *New* in the *Dashboard Views* portlet.

Right-click the listed dashboards, and a menu appears that lets you *Copy* and rename, *Delete*, *Edit*, create a *New* simple or custom dashboard, or *Launch* a Dashboard View (either *Maximize*—a larger view—or as a *Popup*). See *Dashboard Editor* on page 281 for information about creating or modifying dashboards. For an explanation of *Convert*, see *Convert Simple Dashboards to Custom Dashboards* on page 286.

The *Performance Dashboard* on page 279 and *Dashboard Editor* on page 281 describe configuring simple dashboards. See the How to: *Create a Custom Dashboard View* on page 282 section for a description of custom dashboard view creation.



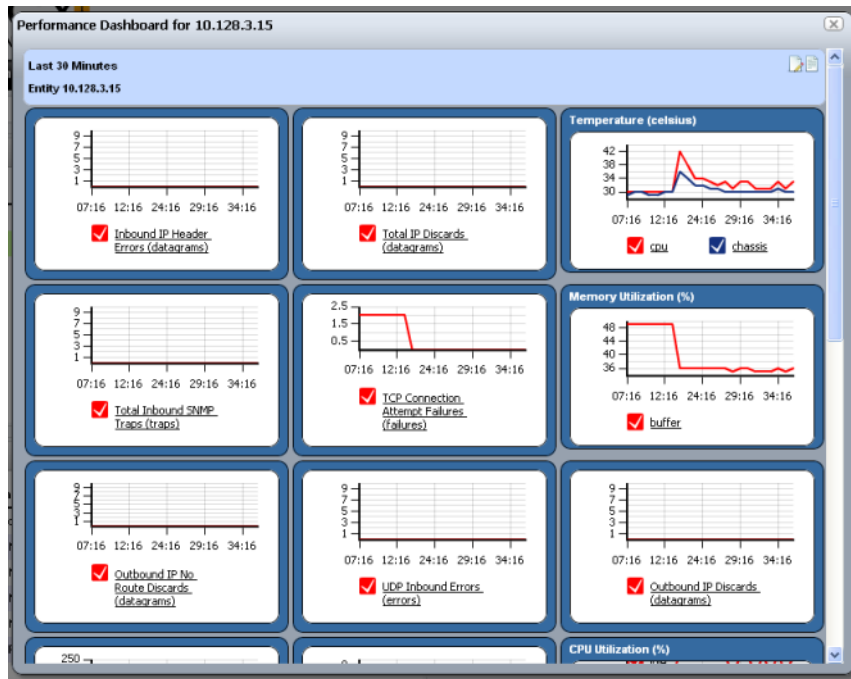
Name	Created By	Created Date	Dashboard Type
TestView	System	8/8/11 10:52 AM	Simple

You can also Convert Simple Dashboards to Custom Dashboards, as described below. When you *Edit* a view, Dashboard Editor appears. It lets you select which monitors appear in the dashboard, the monitored entities, and attributes.

The expanded portlet offers similar capabilities. To make a monitor appear on a page, use the portlet described in *Performance Dashboard* on page 279.

### Launch a Dashboard View

Launching a view lets you view the monitors active for a Dashboard view.



Some packages display a *Network Dashboard* by default. Click the *select new* text in the upper right corner of the dashboard to select an alternative, already configured view from those in Dashboard Views portlet. Click the *edit* button in that same corner to alter the configuration of the existing dashboard. See *Dashboard Editor* on page 281 for more about altering views.

You can configure Dashboards appear by configuring them in the Dashboard Views portlet, or by selecting a device or devices in Managed Resources portlet, right-clicking and choosing *Show Performance*. To select more than one device, use the expanded Managed Resources portlet.

The first time you create a default dashboard for a single device, Dell OpenManage Network Manager saves it in the Dashboard Views manager. Invoking *Show Performance* for that device subsequently displays its default view.

The icons in the dashboard's upper right corner let you edit *Dashboard Properties* with the Dashboard Editor, or *Save* the dashboard with the other icon.

### **Tip**

Hovering the cursor over the individual charts displays the charted attribute value(s) as popup tooltips. If a graph has multiple lines, the data points for different lines are charted at different times (Dell OpenManage Network Manager distributes polling to balance the load on its mediation service). Hover the cursor over the time when a line's data point appears, and that line's value appears as a tooltip. It may seem a device reporting the same value as others is not graphed properly, but mousing over the graph displays the value.

### **How To:**

#### Create a Simple Dashboard View

Follow these steps to create a simple dashboard view. See *How to: Create a Custom Dashboard View* on page 282 for more complex monitor creation.

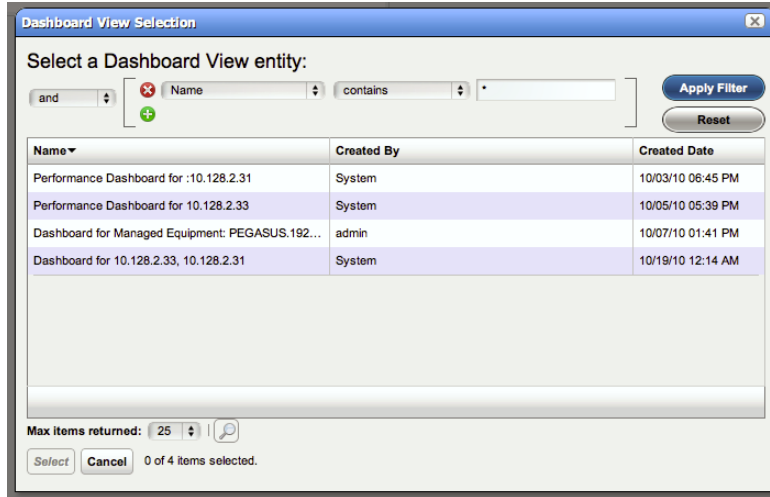
- 1 In the Dashboard Views portlet, right click to select *New > Simple Dashboard*.
- 2 Select a name (for example *SNMP Interface*, to display the monitor configured in *How to: Create an SNMP Interface Monitor* on page 262).
- 3 Click *Add Entity* in the Entities panel.
- 4 In the filter that appears, select the type: *Interface*.
- 5 Filter for the IP address of the entity monitored in the previous SNMP interface monitor creation, select it and click *Add Selection* and *Done*.
- 6 Select the *ifInErrors* attribute, and click the right arrow in the Dashboard View Attributes panel.
- 7 Click *Save*. The dashboard view you have configured should appear in the portlet.
- 8 To launch it, right-click and either *Launch (Popup)* or *Launch (Maximize)*
- 9 If you want to convert this simple dashboard to a custom dashboard so you can alter it further, right-click and click *Convert*.

## Performance Dashboard

This portlet lets you install and configure Dashboard Views as permanent displays rather than portlets. When you initially install this portlet, it appears empty. The message "No Dashboard View has been set:" appears with a *Select* button. Click that button to open the Dashboard View Selection screen.

## Dashboard View Selection

This screen displays any existing dashboards so you can select one for the Performance Dashboard you want to appear on a page in Dell OpenManage Network Manager.



Use the filter at the top of this selector to limit the listed dashboards from which you can select. See *Dashboard Views* on page 277 for more about creating and configuring the views from which you select.

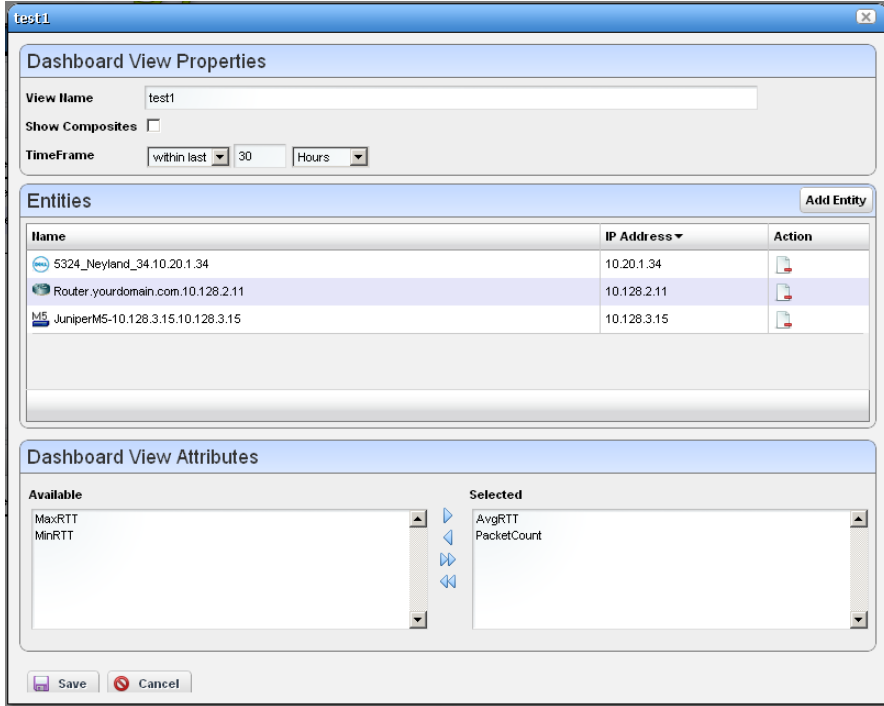
### Tip

If you delete the Network Status Dashboard can put it back by adding the Performance Dashboard portlet to the desired page, then select the desired Dashboard View you would like to display as your Network Dashboard.



# Dashboard Editor

When you *Edit* dashboard by right-clicking a resource in Managed Resources and selecting *Show Performance*, or create (select *New*) a dashboard from the Dashboard Views portlet, an editor appears that lets you select and rearrange the monitor components of the dashboard.



This screen has the following fields:

**View Name**—The identifier for the dashboard. The default is “Performance dashboard for [IP address],” but you can edit this. This is what appears in the Dashboard Views list.

**Show Composites**—Show attributes that are constructed from other attributes.

**TimeFrame**—Use the selectors to configure the time frame for the performance measurement displayed.

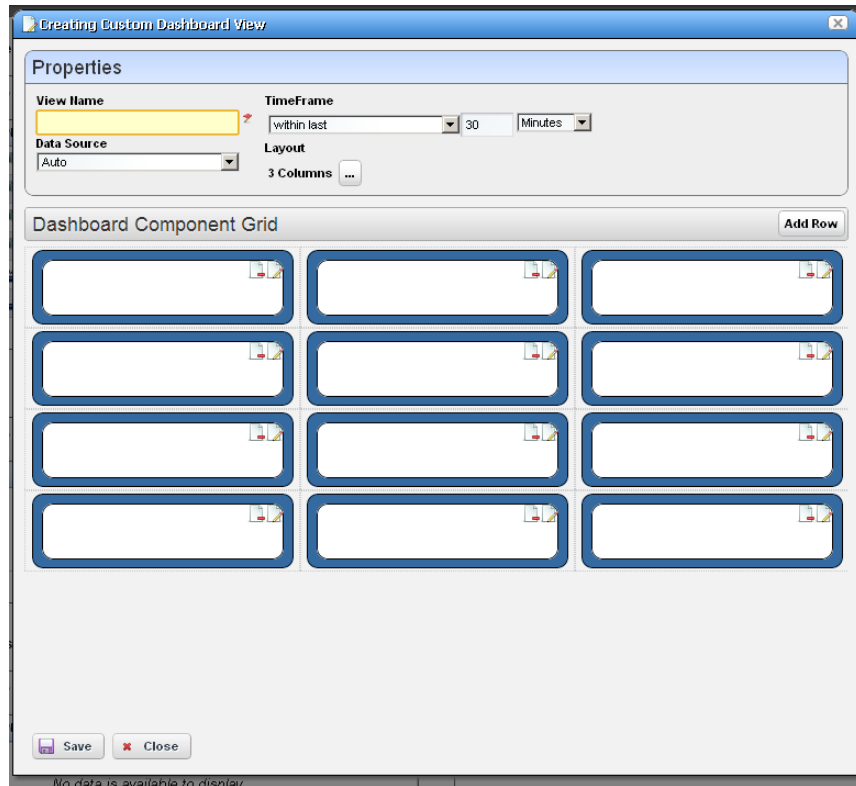
**Entities**—Select the equipment you want to monitor. When you right-click to *Show Performance* with resource(s) selected, those resources appear in this list.

**Dashboard View Attributes**—Click the arrows between *Available* and *Selected* panels to select monitors for the dashboard. The Available Attributes list shows all the available attributes for that device based on its monitor affiliations. If you select none, a chart appears for each attribute that has data. This is the default. If the user moves some attributes to the *Selected* list then only charts for those attributes appear.

## **How To:** Create a Custom Dashboard View

The following steps create a custom dashboard view:

- 1 In the Dashboard Views portlet, select the *New Custom Dashboard* command. An empty default view with twelve components appears.



The Properties panel contains the following controls:

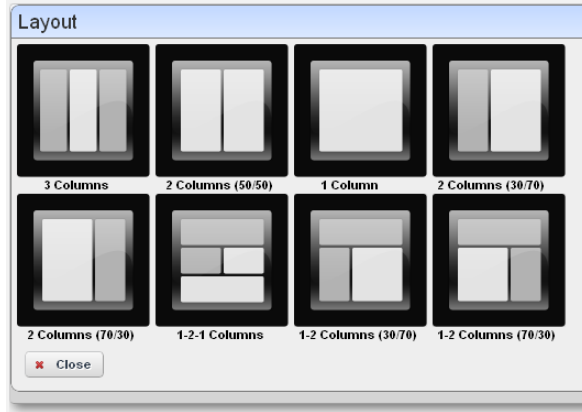
**View Name**—The name of the dashboard view (Required)

**Time Frame**—The period over which to display the data. May be either relative (like *last 30 minutes*) or absolute (between specific dates and times). The specified frame applies to all charts in the dashboard.

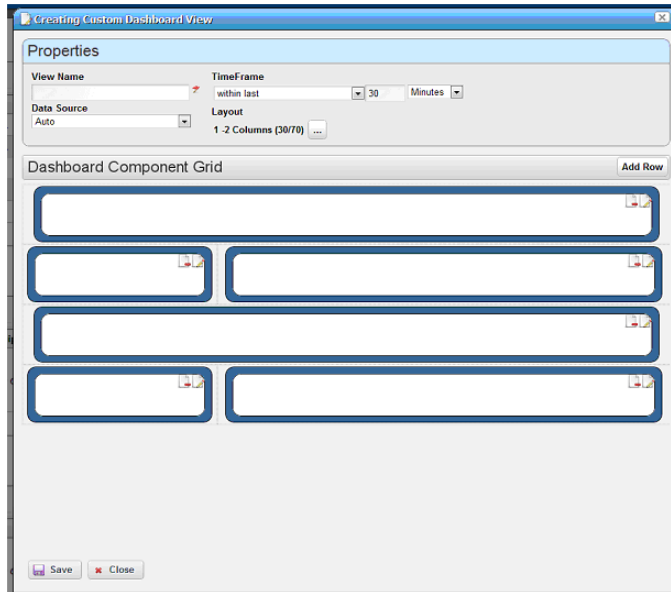
**Data Source**—Source for the data. *Current* displays current (raw) data. *Hourly* displays rolled up hourly data. *Daily* displays rolled up daily data. *Auto* (default) determines which data source to use based on the selected time frame.

**Layout**—Select the desired layout style used to display the dashboard components.

- 2 To select a layout style, click on the ... button next to the current layout. The layout chooser appears.



- 3 Click on the desired layout or click *Close* to keep the current layout. The components displayed to reflect the selected new layout.



If no dashboard components have been configured yet a default configuration appears with three or four rows depending on the dashboard style. If the dashboard components have been configured it will create at least enough rows to display all the configured dashboard

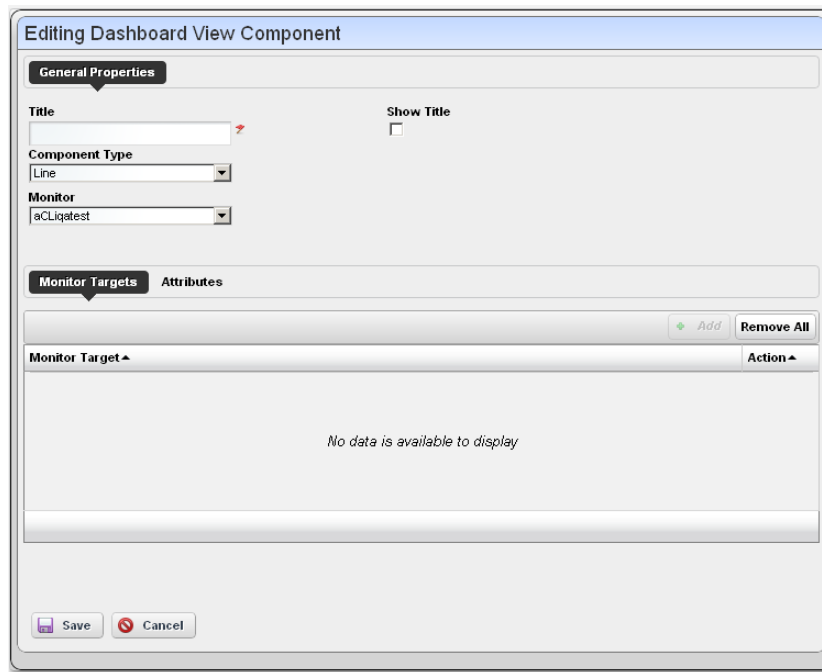
components. Add more rows by clicking on the *Add Row* button. An individual dashboard component can be deleted by clicking on the delete button on the component.

### Moving Dashboard Components

- 4 To move a dashboard component to another location, click and drag it over another component. When you release the mouse, the components exchange places.

### Configuring Dashboard Components

- 5 To configure a dashboard component, click the *Edit* button in the upper right corner of the component. The component editor appears.



The following properties appear in the General Properties section:

**Title**—Title of this component (required)

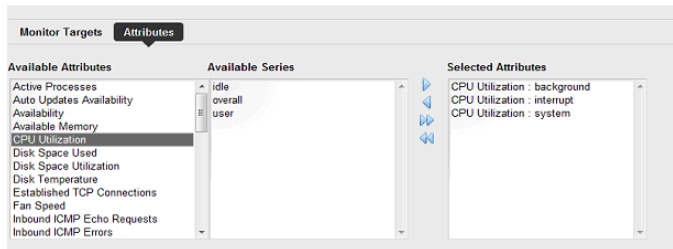
**Show Title**—Check to display this title above the chart for this component. This overrides the default title that is shown for some charts.

**Component Type**—Combo Box which specifies what type of component to create. These include the following chart types, *Line*, *Dial*, *Bar*, *Top Talkers* (a line chart showing the top [or bottom] n components for a specific attribute on a specific monitor) *Top Sub-components* (a line chart showing the top [or bottom] n subcomponents belonging to a specific device for a specific attribute. See

Other controls appear depending on the component type selected. These components also have a *Monitor* control, a pick list where you can select from which monitor the charted data originates. See Dial Chart Properties, Top Talkers Properties and Top Sub-components Properties below for specifics about those.

The line and bar components have two tabs under the general properties section: *Monitor Targets* and *Attributes*. The Monitor Targets section lets you select the devices that are sources of data. Click the *Add* button displays the monitor target selector.

- 6 The Attributes tab selects the attribute(s) that appear in the chart. If an attribute is a composite, then its series appears in the Available Series listbox.



Select the desired series and click the right arrow to move them to the Selected Attributes listbox.

If the attribute is not a composite, then nothing appears in the Available Series listbox. Here, click the right arrow to move the attribute to the *Selected Attributes* listbox.

### Dial Chart Properties

Dial charts have the following additional properties

**Monitor**—Select which monitor the charted data comes from in the pick list.

**Attribute**—The attribute to get data for.

**Min / Max Value**—The minimum / maximum value on the dial.

**Entity**—The monitor target to get the data for. Clicking on the + button brings up the entity selector.

### Top Talkers Properties

Top Talkers components have the following properties.

**Monitor**—Select which monitor the charted data comes from in the pick list.

**Attribute**—The attribute to get data for.

**Max # of Entities**—The number of entities to display

**Order**—Select either *Ascending* (Bottom n), or *Descending* (Top n).

### Top Subcomponents Properties

Top Subcomponents components have the following properties.

**Entity**—The parent entity for the found subcomponents. Clicking on the + button brings up the entity selector.

**Attribute**—The attribute to get data for.

**Max # of Entities**—The number of entities to display

**Order**—Select either *Ascending* (Bottom n), or *Descending* (Top n).

### Convert Simple Dashboards to Custom Dashboards

To convert a simple dashboard to a custom dashboard use the *Convert* command on the *Dashboard Views* menu. You cannot convert custom dashboards to simple dashboards.

## Show Performance Templates

By default, the Show Performance command displays data for the first twelve attributes it finds. You can control which attributes appear when you select Show Performance by creating a performance template. A performance template lets you set dashboard parameters and associate them to one or more device models. Then, when you execute Show Performance on a device of that type, those dashboard parameters display the dashboard for that device.



### How To:

#### Create A Performance Template

To create a performance template, follow these steps:

- 1 Right click in the Dashboard Views portlet and click on the *Performance Templates* menu item.
- 2 The Performance Templates manager appears.

- To create a new performance template, click on the Add button. The Performance Template Editor appears.

**Adding New Performance Template**

**General Template Parameters**

Template Name  
JuniperRouterMaxRTT

Show Composites

Time Frame  
within last 30 Minutes

**Device Models**

Specify which device model(s) will use this template

MS Core/Edge Router  
M20 Core/Edge Router

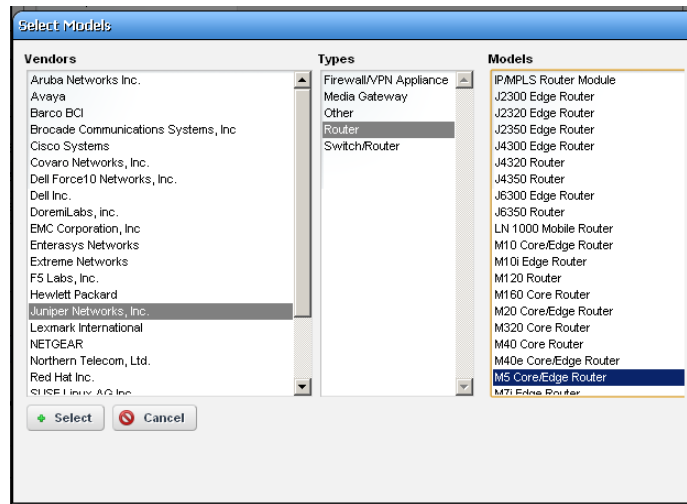
**Attributes**

Monitors	Available Attributes	Selected Attributes
Default Cisco Monitor	AvgRTT	Default ICMP Monitor : MaxRTT
Default ICMP Monitor	MinRTT	
Default Interface Monitor	PacketCount	
Default Juniper Monitor		
Default VMI Monitor		

Save Cancel

- Name your template. The Show Composites and Time Frame fields are the same as in the dashboard (see *Dashboard Editor* on page 281).

- 5 To specify which device model(s) this template will apply to, click on the + button in the Device Models panel. The model selector appears.

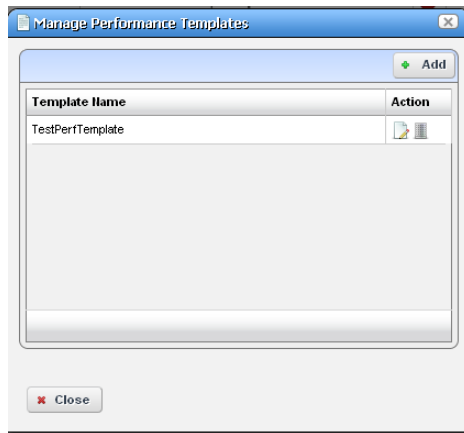


Select multiple devices by clicking + repeatedly, selecting a single device each time. You can also make several templates for each device. See *Multiple Performance Templates* on page 289 for the way that works.

- 6 Click on a vendor to see the device types for that vendor. Then click on a device type to see the models available for that vendor and device type. Select the model you want and click on the select button.
- 7 To select the attributes that you want to appear by default in a performance dashboard for the selected device, click on a monitor to see the attributes available for that monitor. Click on the right arrow button to move the selected attributes from *Available* to *Selected*. Those are the attributes that will appear by default in dashboards for the selected device.



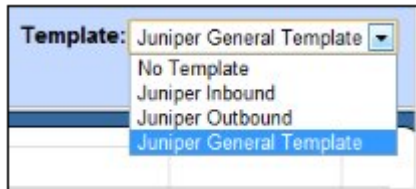
- When you have selected all the parameters you want, click *Save*. It then appears in the template list.



To edit or delete your template, use the buttons in the action column of the table.

Now when you click on show performance, Dell OpenManage Network Manager checks whether a template for that device type exists. If one exists, then that template guides what appears in the performance view for the device.

### Multiple Performance Templates



The template name appears in the upper right corner of dashboards that appear when you select Show Performance.

If other templates for that device type exist they also appear in a template pick list in the upper right corner. You can pick another template to display its attribute selection. The *No Template* selection displays the default dozen attributes that would appear if you

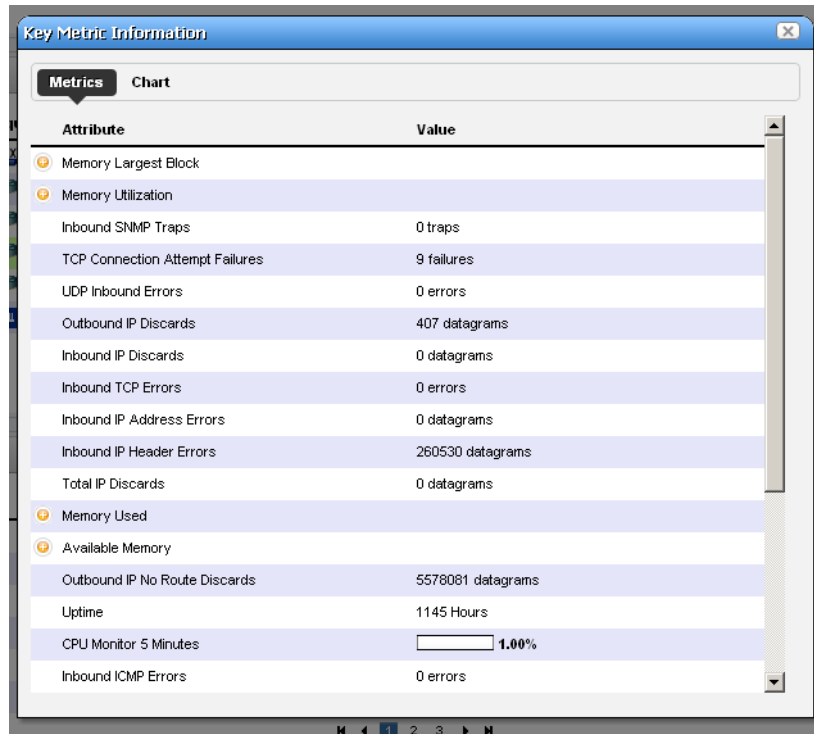
selected Show Performance without a template defined for the device.

## Key Metric Editor

When you select *Performance > Show Key Metrics*, this editor appears for devices that have such metrics. It displays the available Metrics, and a Chart panel where you can configure their display.

## Metrics

This panel's display depends on the selected device.

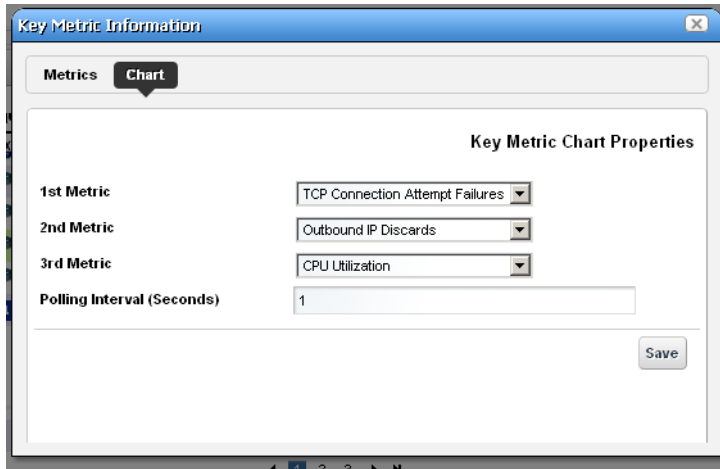


The screenshot shows a window titled "Key Metric Information" with a "Metrics" tab selected. The window displays a table of system metrics. The table has two columns: "Attribute" and "Value". The metrics listed include memory usage, network errors, and system uptime. The "CPU Monitor 5 Minutes" metric is highlighted with a value of 1.00%.

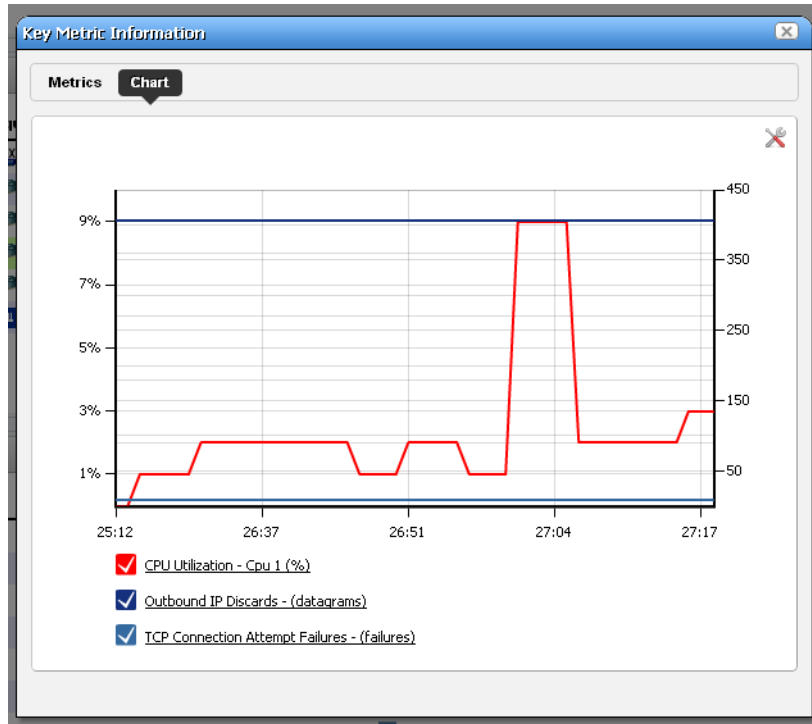
Attribute	Value
Memory Largest Block	
Memory Utilization	
Inbound SNMP Traps	0 traps
TCP Connection Attempt Failures	9 failures
UDP Inbound Errors	0 errors
Outbound IP Discards	407 datagrams
Inbound IP Discards	0 datagrams
Inbound TCP Errors	0 errors
Inbound IP Address Errors	0 datagrams
Inbound IP Header Errors	260530 datagrams
Total IP Discards	0 datagrams
Memory Used	
Available Memory	
Outbound IP No Route Discards	5578081 datagrams
Uptime	1145 Hours
CPU Monitor 5 Minutes	<input type="text" value="1.00%"/>
Inbound ICMP Errors	0 errors

## Chart

Click *Chart* to first select up to three metrics you want to graph, and the polling interval for the graph.



Then click *Save*, and the graph appears.



Click the screwdriver / wrench icon in the upper right corner to return to the chart configuration screen.

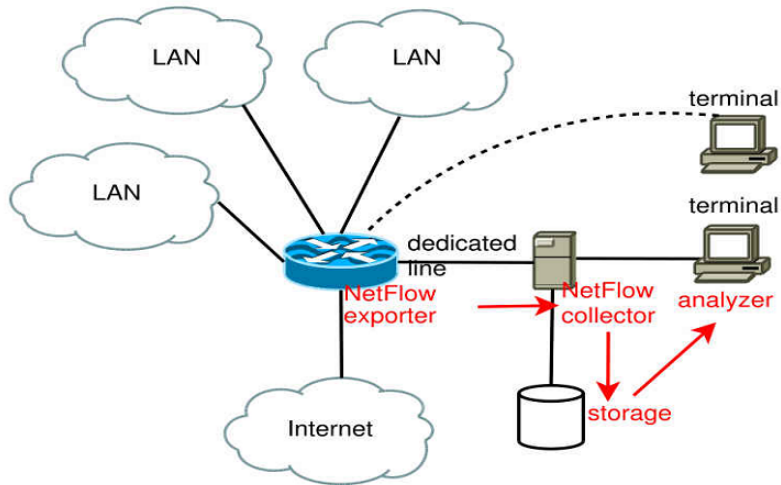
# Traffic Flow Analyzer

OpenManage Network Manager's Traffic Flow Analyzer listens on UDP ports for NetFlow, or JFlow datagrams. A flow is a unidirectional stream of packets between two network nodes. The following key parameters appear in flows:

- Source IP address
- Destination IP address
- Source port number
- Destination port number
- Layer 3 protocol type
- ToS byte (Type of Service)
- Input logical interface

Using that data, Traffic Flow Analyzer can help you visualize network traffic, troubleshoot and anticipate bottlenecks.

# How does it work?



- The NetFlow exporting router monitors traffic traversing it
- The router becomes an Exporter of NetFlow data.
- It forwards information to the NetFlow Collector
- Collector stores, correlates and presents the information about
- Traffic bottlenecks in networks?
- Applications responsible for bandwidth utilization?

## Definitions

**NetFlow**—NetFlow is a traffic profile monitoring technology

**J-Flow**—Juniper's implementation of NetFlow.

**sFlow**—For Dell devices.

**Collector**—Application listening on a UDP port for NetFlow datagram.

**Exporter**—Network element that sends the NetFlow datagram.

**Conversations**—IP communications between two network nodes.

**Flow**—A flow is a unidirectional stream of packets between two network nodes.

## Setup

If they are not already set up to emit flow information, set up devices themselves to emit flow data. Consult the manuals for your devices for instructions about how to do this.

Set up Dell OpenManage Network Manager with the following:

**Exporter Registration**—To register a device, right-click in Resources portlet, after you select the router and choose *Traffic Analyzer > Register*. The system should then be ready to accept flow data from the device.

**Router Configuration**—You must configure the router to send flow reports to the Dell OpenManage Network Manager server on port 9996 by default.

**Resolving Autonomous System (AS) Numbers**—Dell OpenManage Network Manager provides local resolution of autonomous system numbers (ASN) based on static mapping of AS number registrations. It also supports user overrides to the default mappings. To do this, configure properties you can find in the `\owareapps\trafficanalyzer\lib\ta.properties` file. Remember, best practice is to override properties as described in *Overriding Properties* on page 23.



## How To:

### Use Traffic Flow Analyzer

- 1 Register the device(s) you want to analyze. (As in *Exporter Registration*). A message confirms registration's success.
- 2 Look in the Traffic Flow Portlet for the flows captured.
- 3 Remember, you can Drill Down to specific data, and Search for specific devices monitored.

For more about Traffic Flow in context of network management, see *Traffic Flow Analyzer - Example* on page 301.

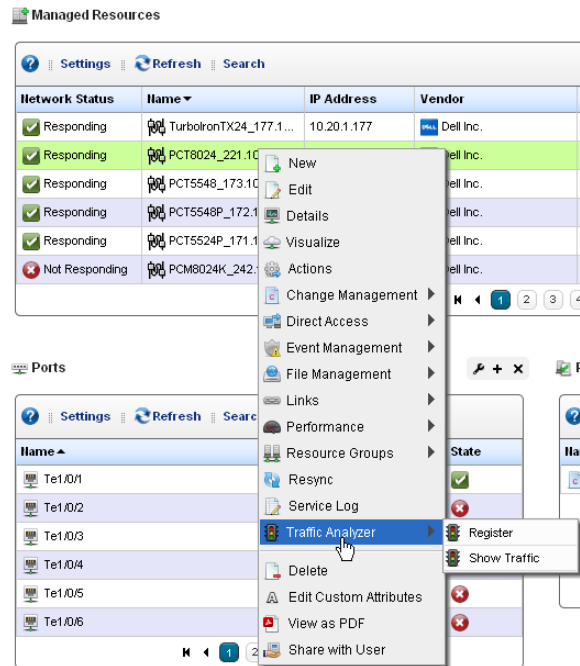
## Exporter Registration

Before you can collect traffic data from a device, you must *Register* it as a traffic flow exporter. If a device is not registered, the *Register* command appears in the menu. If it is registered the *Unregister* command appears. When you successfully register an eligible device, a success message appears; otherwise, a failure message appears, and no registration occurs.

The *Show Traffic* menu option opens a drop-in (full screen) Traffic Flow Portlet with a pick list of available information types.

This displays the *Exporters Detail*, *Top 5 Applications*, *Top 5 Autonomous Systems*, *Top 5 Conversations*, *Top 5 Endpoints*, *Top 5 Protocols*, *Top 5 Receivers*, and *Top 5 Senders* related to the device selected before right-clicking. Select a type and click the *Refresh* double arrow to the right of the selector.

The screen that then appears has the features of the Expanded Traffic Flow Portlet described below. See also *How to: Use Traffic Flow Analyzer* on page 295.

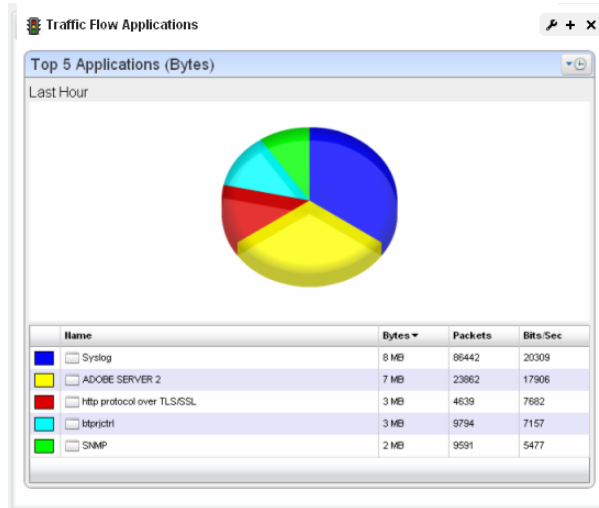


## Traffic Flow Portlet

Traffic Flow Analyzer uses several types of portlets, one for each of the types of objects on which it reports. These are Applications, Autonomous Systems, Conversations, Endpoints, Exporters, Protocols, Receivers and Senders.



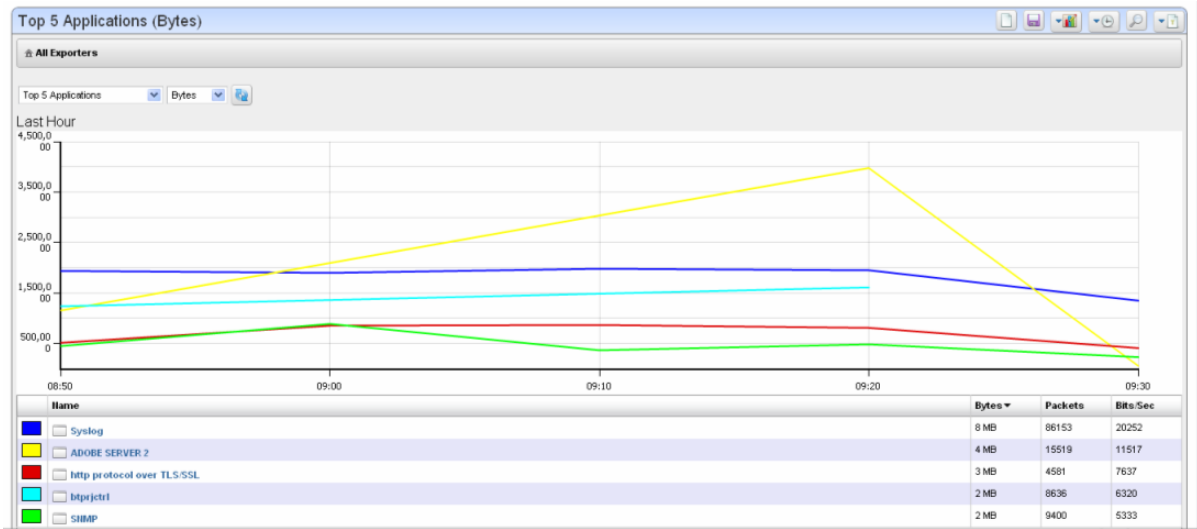
When you add one of the traffic analyzer portlets to a page, its summary, or minimized form appears. This displays a simple view containing a pie chart and a table showing the summarized collected data over the configured time period. The only thing that can be changed in this view is the period. Change this by clicking the clock dropdown button in the upper right corner of the portlet.



The Expanded Traffic Flow Portlet displays an interactive graph. You can also Drill Down to details about components within this portlet by clicking on one of the links in the table below the graph.

## Expanded Traffic Flow Portlet

When you expand the portlet, a more complex interactive view appears. Initially, it displays a line graph for the selected period.



### NOTE:

It may seem a device reporting the same value as others is not graphed properly, but mousing over the graph displays the value.

The following controls appear in its title bar:

**Select Chart Type**—Lets you change the chart type. Available chart types include *Pie*, *Line*, *Bar*, *Stacked Bar* and *Column*.

**Select Timeframe**—Lets you change the period between *Last 15 Minutes*, *Last Hour*, *Last 24 Hours*, *Last 5 Days* and *Last 30 Days*.

**Search**—Displays a search dialogue to find specific traffic data.

**Report Type**—Lets you change the report type between Top 5, 10 or 25 and Bottom 5, 10 or 25.

**Load View**—Loads a saved traffic flow view, created with the *Save* button.

**Save**—Saves the current view to a named view.

Below the title bar a navigation bar displays the context path. See Drill Down, below, for more about this.

Below that navigation bar a row containing the following controls appear:

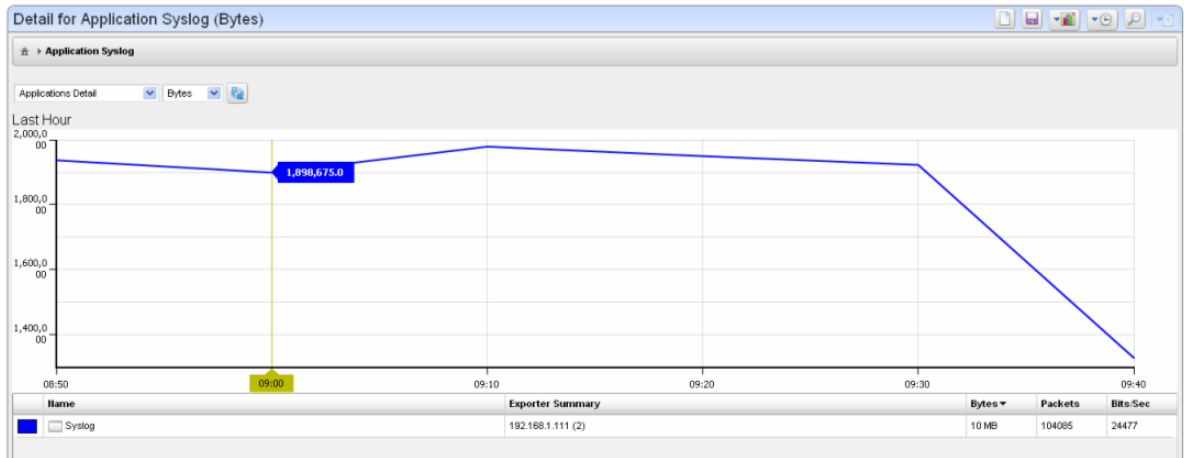
**Entity Type**—Selects the type of entity to report on (Conversations, End points, and so on).

**Attribute**—Selects which attribute to graph (Bytes, Packets, Bits/Sec).

**Refresh**—Refreshes the screen (runs the report) applying any new settings.

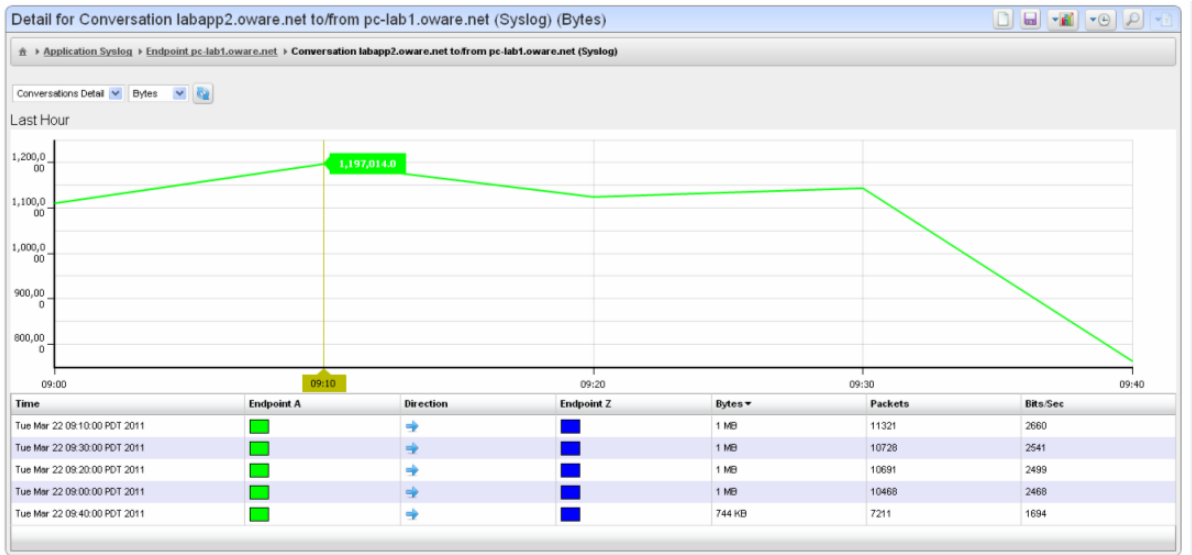
## Drill Down

you can “drill down” into a report by clicking on one of the links in the table. This displays a detail view of the selected entity and the name of the entity appears in the navigation bar.



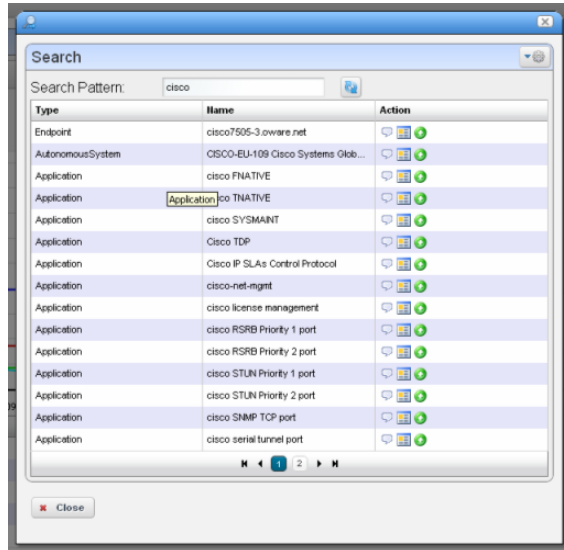
When a detail view appears, the entity type appears as in the title bar. You can change to a “Top / Bottom n” report of a different type, then click refresh to display a report of the top entities that apply to the current detailed entity. This process can continue until the conversation detail view is reached. This is the end of the line.

To go back up through the drill-down path the user can click anywhere on the navigation bar.



## Search

Search by clicking on the Search (magnifying glass) icon in the title bar. Type any string in the next screen to search through the traffic data. A list of all entities found matching the string appears below it.



Entity found in the search support the following actions:

**View Top Conversations**—Displays the top n conversations for the selected entity.

**Show Detail View**—Displays a top level detail view of the selected entity.

**Add to Current View**—Adds the entity to the current view and drills down to it.

### Tip

The *Settings* button (the gear in the upper right corner) lets you confine the search by types (*All*, *Applications*, *Protocols*, and so on).

## Traffic Flow Analyzer - Example

The following describes typical situations where flow is useful. When ports are over-utilized because of intermittent performance problems diagnosis of the problem sometimes difficult. Turn on flow traffic data collection to evaluate who, what applications, and so on, are responsible for the traffic on the affected ports. This avoids getting overwhelmed with collection of traffic going in all directions. Follow these steps to do this:

- 1 From the Resources monitor, select a desired router that has support for NetFlow

- 2 Enable NetFlow on most impacted routers that support NetFlow. Also, register a number of exporters to enable an efficient and scalable data collection environment.

 **NOTE:**

You can disable NetFlow and unregister exporters.

- 3 After NetFlow has been running for a while, verify that bandwidth utilization is within expectation. This will help insure optimum performance of critical business applications.
- 4 Select the Top 5 Applications portlet (or add it to the page).
- 5 From the list of the Top 5 Applications, you'll typically see most bandwidth is being consumed by the key applications in our organization.

### **Alternative 1**

- 6 To ensure bandwidth is not being hijacked by unauthorized or unwanted video or music streaming applications, select the Top 5 Conversations.
- 7 Often the top conversation is video streaming software.
- 8 To answer "Where and who is running this rogue application?," drill down into the conversation to see End points involved in the conversation. This identifies the user running the streaming application. You could now go and stop (or block) this rogue application.

### **Alternative 2**

An alarm indicates port X is surpassing its threshold. If the port has become a bottleneck in the overall network bandwidth, we want to identify what applications are at cause, and who is responsible for running them.

- 1 Look in the Top 5 Traffic Flow Endpoints portlet.
- 2 From the list of the Top 5 Endpoints, you will typically see that port X is high on the list.
- 3 Expand the portlet and drill down into the port X endpoint to see what are the top conversations going through port X.
- 4 Drill down into conversations to identify any unauthorized applications.
- 5 Drill down further to identify users of any unauthorized applications
- 6 Now, go stop them!

## Change Management – ProScan

Dell OpenManage Network Manager's change management utility is ProScan, which lets you scan stored configurations to verify managed devices compliance with company, department or industry standards. This application automatically tracks all changes occurring to managed devices. You can report on user-specified values found in persisted backup configuration files for a group of devices. This lets network managers, security officers and external auditors generate detailed audit trail documents to validate compliance with both internal standards (ISO 17799, NSA Guidelines) as well as industry regulations (Sarbanes-Oxley, GLBA, HIPAA).

Compliance reporting lets you specify a text string, regular expression, or optionally the generated configlet from File Management (NetConfig) for matching. Group results must be separated by device like Adaptive CLI Manager. When ProScan policies run, the application emits notifications whose contents depend on whether compliance was or was not maintained.



### Tip

Your system may have several ProScan examples. You can use these as provided, or alter them to suit your network.



### How To:

#### Use ProScan / Change Management

The following outlines common use cases for this software, and the steps to achieve the goals of each case:

#### **Goal: Verify configurations are compliant on a scheduled / recurring basis.**

- 1 Create ProScan policy(ies) based on what indicates compliance. Right-click *New* > *Policy* in the ProScan portlet.
- 2 Specify the Name and Input source (based on Device Backup, Current Config, Configuration Label, By Date and Adaptive CLI Results)

- 3 Add Targets > Filter Option available for selecting Equipment/Group



### Tip

The advantage of selecting dynamic device groups is that newly discovered devices of the selected type are automatically members of the group, so they are scanned too. A benign warning (“No proscan policies have target group(s)”) lets you know you have not selected either dynamic or static groups when you execute a ProScan policy without them.

- 4 Specify Proscan Compliance Criteria. Add Criteria.
- 5 Save.
- 6 Execute or schedule your created ProScan policies.
- 7 Any out-of-compliance devices throw an alarm, which you can email, or configure to trigger other actions (see the next use case).

### **Goal:...And if not compliant restore compliant configuration**

In addition to the steps in the previous section:

- 8 Create an action to restore the labelled compliant configuration.
- 9 Create event processing rule that says when ProScan fails execute the restore action in 7.

If you have multiple device types you do not need to assign actions for each device, or even each device type. OpenManage Network Manager supports the *assigned policies*, so it knows which actions to do to that device based on which device sent the trap.



## How To:

### Configure ProScan Groups

If you have different ProScans for different device type, then you can run a ProScan Group and automatically scan even different types of devices.in one action. For more about this, see [Creating or Modifying ProScan Policy Groups](#) on page 325.

- 1 Right-click and select *New > Group*.
- 2 Specify the Proscan Policy Group Parameters.
- 3 Add ProScan Policies.



### Tip

These policies can be in multiple groups.

- 4 Add Targets. Notice that group targets appear in the “child” policies, grayed out. Child policies can add more targets.
- 5 Save.
- 6 Execute or schedule the group policies to run against the selected targets.





## How To:

### Do Change Management (Example)

The following describes an example use of Change Manager. This backs up a configuration file, modifies it, then scans the file for the modified text, and acts according to the result. The following steps describe how to do this:

- 1 Back up a device configuration. Select a device and click the *File Management > Backup* right-click menu in Managed Resources portlet.
- 2 Right click, and Export this backup to a file in the Configuration Files portlet.
- 3 Edit this config file, adding the word “MyTestContact” somewhere in its text that has no impact. For example, the snmp-server contact, or in comments.



#### Tip

Some devices let you create descriptions within their configurations so you can enter a word without impact there.

- 4 Now import this edited file from the Managed Resources portlet after you have right-clicked on the same device from which you exported it. Renaming it something distinctive is helpful.
- 5 Right-click this file and *Restore* to the device. Since the name is a comment or description, it should not interfere with the device’s operations.
- 6 Right-click the device and select *File Management > Backup*. This makes the MyTestContact file label Current.



#### Tip

To confirm MyTestContact is labeled Current, you can use an Advanced filter in the expanded Configuration Files portlet to view only Current labels.

- 7 Now, create a ProScan policy by right-clicking in the ProScan portlet, selecting *New > Policy*.
- 8 In the General tab, name this policy MyTestContactScan, and as an input, select the *Configuration Label > Current* label as the Input Source.
- 9 In the Targets tab, select the equipment from which you exported the config file.
- 10 In the Criteria tab, click *Add Criteria* enter *contains MyTestContact* as the *Match All of the following criteria*.
- 11 Click *Save*.
- 12 Right-click the new policy and select *Execute Compliance*.
- 13 The audit screen that appears should indicate *Success*.
- 14 Right-click and *Open* the MyTestContactScan policy, and change the Criteria to “does not contain” MyTestContact.
- 15 *Save*

- 16 Re-execute the policy.
- 17 The audit screen that appears should indicate *Failure*.

### Alarms / Events

Once you have a ProScan policy that has failed, the redcellProScanFailureNotification alarm appears in the Alarms portlet. Success produces an event, not an alarm (visible in the Event History portlet) called redcellProScanClearNotification.

To create a response, create processing rules for the event / alarm (see Event Processing Rules on page 108). For example, you could restore the Compliant-labeled configuration file if redcellProScanFailureNotification occurs, or send an e-mail to a technician, among many other responses.

### Some Limitations in this Example

Note that this example does not change authentication, either for telnet or SNMP. If it did alter the SNMP authentication, you would have to create an SNMP authentication alternative before scanning could occur.

## ProScan Portlet

This portlet lets you configure compliance requirements. You can use filtering in the Expanded ProScan Portlet to limit the visible policies.

The *Icon* and *ProScan Type* columns indicate whether the policy is a single policy or a group. Columns also display the *Overall Compliance* of a policy, and the *Target(s)* (number of devices to scan), and whether the policy is

*Monitored* (red means no, green means yes. See Proscan on page 269 in Chapter 7, Monitoring for details). Finally, you can see whether a policy’s execution is scheduled. To execute a policy manually, go to the Managed Resources portlet, and right-click the targeted device to find the *Change Management* menu item. You can *Execute ProScan* policies that target the device with that menu item. If you want to execute a ProScan policy not already associated with the device or group, then select *Execute Proscan Policy*. A selection screen appears where you can select a policy and either execute or schedule it.

Name	Target(s)	Overall Compliance	Monitored	Scheduled
Cisco tacacs+ enabled			No	No
Cisco SNMP Community String NOT public			No	No
Cisco SNMP Community String NOT priv...			No	No
Cisco RADIUS Enabled			No	No
Cisco monitor logging Enabled			No	No
Cisco IP Finger Disabled			No	No

## Overall Compliance

Overall Compliance can have the following values and flag icon colors:

**All Compliant**—Icon: Green. All selected equipment is in compliance with the policy.

**None Compliant**—Icon: Red. None of the selected equipment is in compliance with the policy.

**None Determined**—Icon: blank. None of the equipment has been tested for compliance.

**Partial Compliance**—Icon: Yellow. Not all equipment complies with the policy but all equipment has been tested.

**Compliance Varies**—Icon: Yellow. Not all equipment has been tested for compliance. The tested equipment might be compliant or not compliant.

## Portlet Menu

This screen also has the following right-click menu items:

**New**— Select either a new policy or group. Creating a new policy opens the ProScan Policy Editor, through which you can define one. See *Creating or Modifying a ProScan Policy* on page 310 for more information about the Editor. See *Creating or Modifying ProScan Policy Groups* on page 325 for the group editor.

**Edit**—Opens the selected policy or group for modification. See *Creating or Modifying a ProScan Policy* on page 310 for more information. See *Creating or Modifying ProScan Policy Groups* on page 325 for the group editor.

**Refresh Targets**—Queries to check targets, particularly those in dynamic groups, are up-to-date.



Best practice is to **Refresh ProScan Targets** before running a scan particularly if your network has changed since the last scan. You can also schedule this. See *Schedules* on page 95.

**Modify Targets**—Lets you modify and/or select target equipment for the policy.

**Schedule**—Configure a policy to run on a schedule.

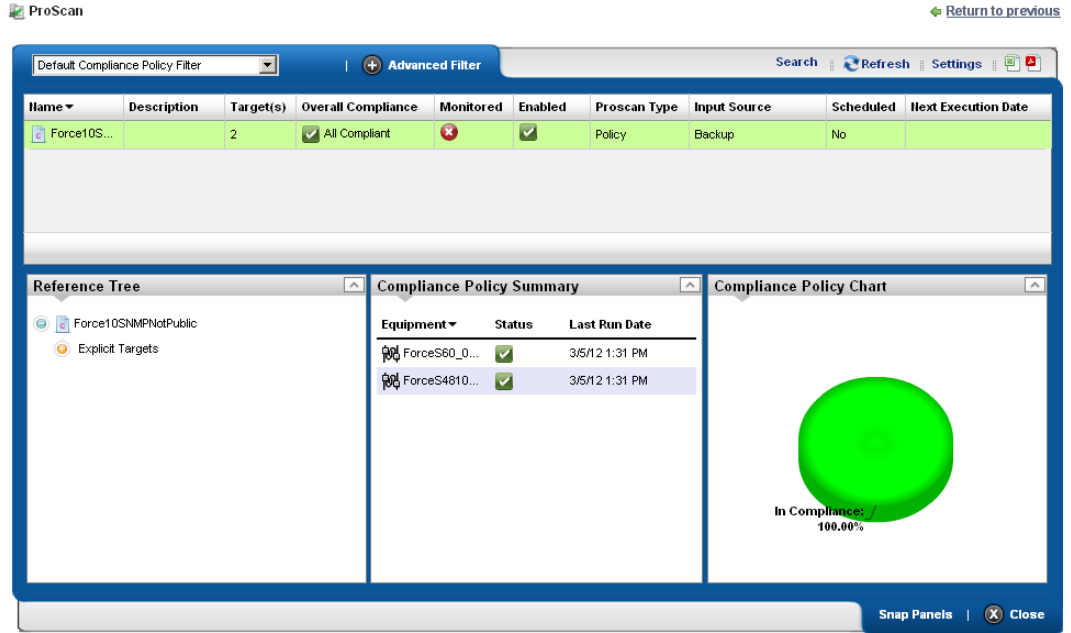
**Audit**—Opens an Audit Viewer with the results of a selected policy's runs. This is one way to see the historical results of proscan policy runs. Another is to consult the Compliance Policy Summary snap-in in the Expanded ProScan Portlet.

**Delete**—Deletes the selected policy. Select the item to remove and click *Delete*. The application prompts you for confirmation.

**Import / Export**—Lets you import policies or export the selected policy.

## Expanded ProScan Portlet

The expanded ProScan portlet lets you see the Compliance Policy Summary, a reference tree of the connections between a policy and its targets, and a Compliance Policy Chart snap panel.



The screenshot shows the ProScan interface with a table of policies and three snap panels below. The table has columns for Name, Description, Target(s), Overall Compliance, Monitored, Enabled, Proscan Type, Input Source, Scheduled, and Next Execution Date. The snap panels are: Reference Tree (showing Force10SNMPNotPublic and Explicit Targets), Compliance Policy Summary (showing a table of equipment with status and last run date), and Compliance Policy Chart (showing a green circle representing 100% compliance).

Name	Description	Target(s)	Overall Compliance	Monitored	Enabled	Proscan Type	Input Source	Scheduled	Next Execution Date
Force10S...		2	All Compliant	✘	✔	Policy	Backup	No	

Equipment	Status	Last Run Date
ForceS60_0...	✔	3/5/12 1:31 PM
ForceS4810...	✔	3/5/12 1:31 PM

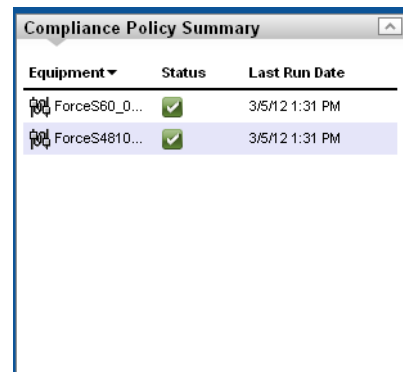
  

In Compliance: 100.00%

See Compliance Policy Summary on page 308 for a description of the snap panel that appears below the listed policies in this manager.

## Compliance Policy Summary

This snap panel appears at the bottom of the expanded portlet described in ProScan Portlet on page 306. It catalogs the compliance policy's history and lists the *Equipment* scanned, a status icon indicating whether the run discovered equipment *in* (green) or *out* (red) of compliance. If you added equipment to a policy before it



The screenshot shows the Compliance Policy Summary snap panel with a table of equipment. The table has columns for Equipment, Status, and Last Run Date. The equipment listed are ForceS60\_0... and ForceS4810..., both with a green checkmark status and a last run date of 3/5/12 1:31 PM.

Equipment	Status	Last Run Date
ForceS60_0...	✔	3/5/12 1:31 PM
ForceS4810...	✔	3/5/12 1:31 PM

has run, you may also see a *Not Executed* (blue) status. Each run date for the policy and equipment combination selected in the list at the top of the detail panel screen appears as a row in this panel.

 **Tip**

You can also see compliance failure messages in OpenManage Network Manager's audit trails.

Compliance scans do not stop the first time they fail. They continue so all failures of compliance in the entire device configuration appear cataloged in the result.

Each time OpenManage Network Manager executes a compliance policy it stores a history record in the database. Similarly, edits to these policies update history records. When you edit a compliance policy to add/remove equipment, OpenManage Network Manager creates or deletes the corresponding history record. Every time OpenManage Network Manager executes the compliance policy, it updates the Last Run Date, Status and Details on the history record.

 **NOTE:**

Executing Proscan policies may trigger a benign warning that "No proscan policies have target group(s)" if that is the case. You can safely ignore this warning message.

### Groups

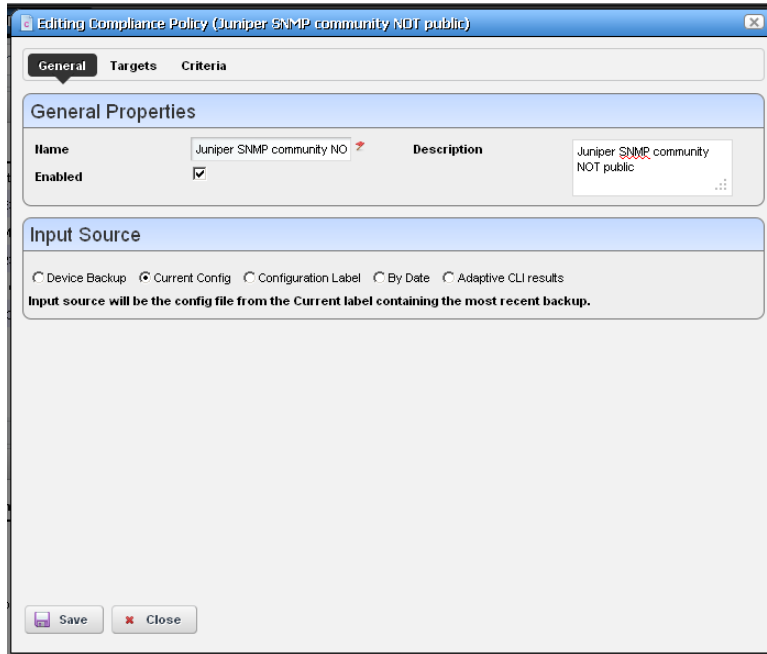
When you run a ProScan group policy, the history for the group appears in this detail panel just as it would for a single policy. History concatenates the results of the component policies, as does reporting. See Compliance and Change Reporting on page 329.

 **Tip**

You can print a *Compliance Policy Violation* report from Report Manager. It produces a document based on the Compliance Policy History.

# Creating or Modifying a ProScan Policy

This series of screens lets you configure ProScan policies.



This screen has the following tabs:

- General
- Targets
- Criteria

The Compliance Policy Job Status screen displays progress of a ProScan policy as it executes.

## Tip

If you have more than one type of device, you must typically have more than one ProScan policy to address each device type. To run more than one ProScan, so you can address multiple types of devices, create a ProScan group. See [Creating or Modifying ProScan Policy Groups](#) on page 325.

## General

This tab has the following fields:

### General Properties

**Name**—A unique identifier for the policy (editable only when you click *New*, not on existing policies).

**Enabled**—Check to enable this policy.

**Description**—A text description of the policy. This also appears when the policy is listed in the manager.

### **Input Source**

Use the radio buttons to select a source. Select from among the following options:

**Device Backup**—Retrieve the configuration from the device and scan it for compliance.

**Current Config**—The scan the current configuration backed up from the device.

**Configuration Label**—Select the configuration to run against based on a label. This software automatically updates the *Current* label so it points to the most recently backed up configuration files.

**By date**—When you click this radio button, you can then select a configuration file backed up that precedes a specified date most closely in a selector that appears below the radio button.

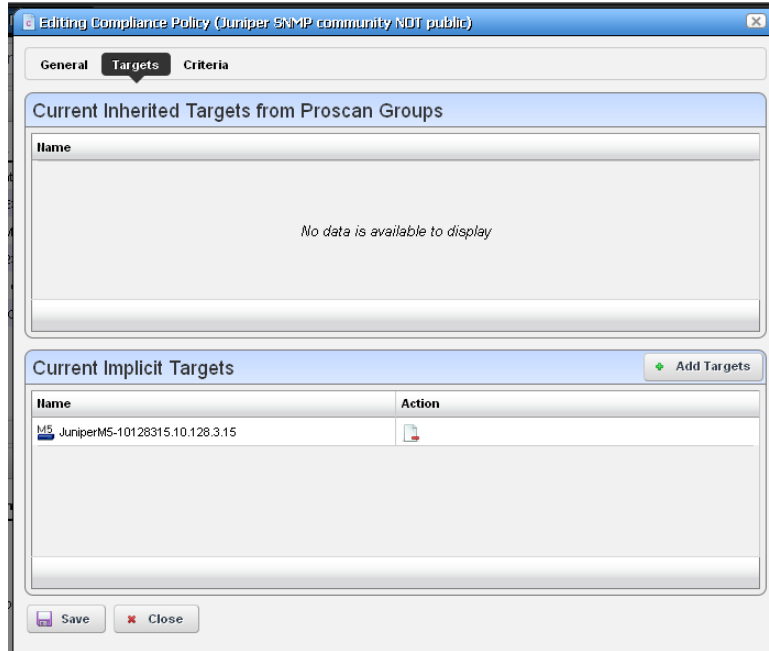
#### **NOTE:**

You can scan even historic configurations for compliance, with the **Based on date** field. There is no validation to ensure this date is the current one.

**Adaptive CLI**—Select a desired *Show* Adaptive CLI to scan the target device below the radio button. The policy configured scans the show results, and that show appears in the Audit screen.

## Targets

The top of this screen (*Current Inherited Targets*) displays any targets inherited from already-configured ProScan Groups. Click *Add Targets* in the *Current Implicit Targets* panel at the bottom to select equipment that are targets to scan with this policy. You can also select listed equipment and click the *Remove* icon to delete it from the list.



### Tip

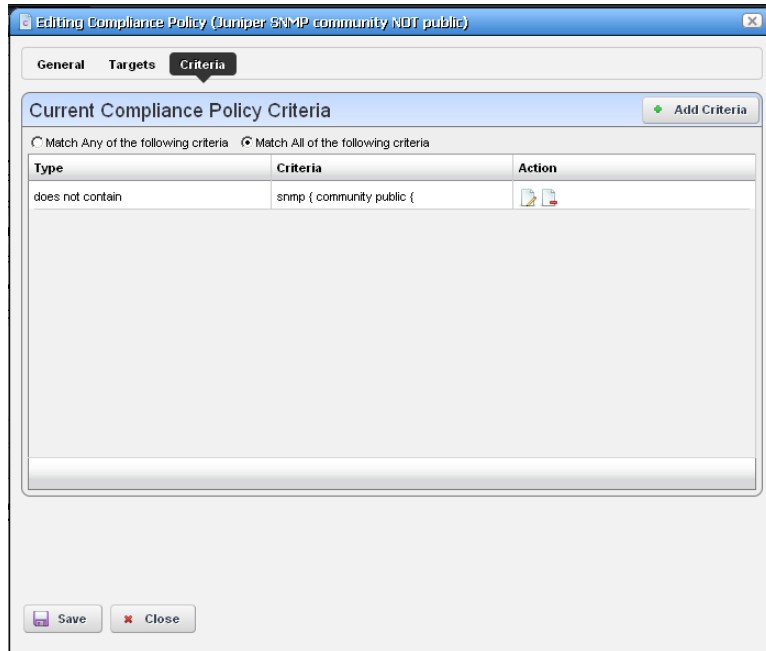
Use filtering in the subsequent selector screen to make individual selection easier, but do not forget this is *not* dynamic selection. You must assign policies whenever your managed environment adds new equipment.

To provide information for individual policies that are part of groups, this screen displays inherited group targets grayed out. See *Creating or Modifying ProScan Policy Groups* on page 325 for more about groups.



## Criteria

This screen lets you filter configuration files based on text, or Regular Expressions. Click *Add* to open an editor line.



This screen ultimately determines whether the configuration file(s) for the selected equipment complies with the applicable policy. To create a policy, first select whether you want to *Match Any* (logical OR), or *All* (logical AND) of the criteria you configure with the radio buttons at the top of this screen.

See these sections for more about criteria:

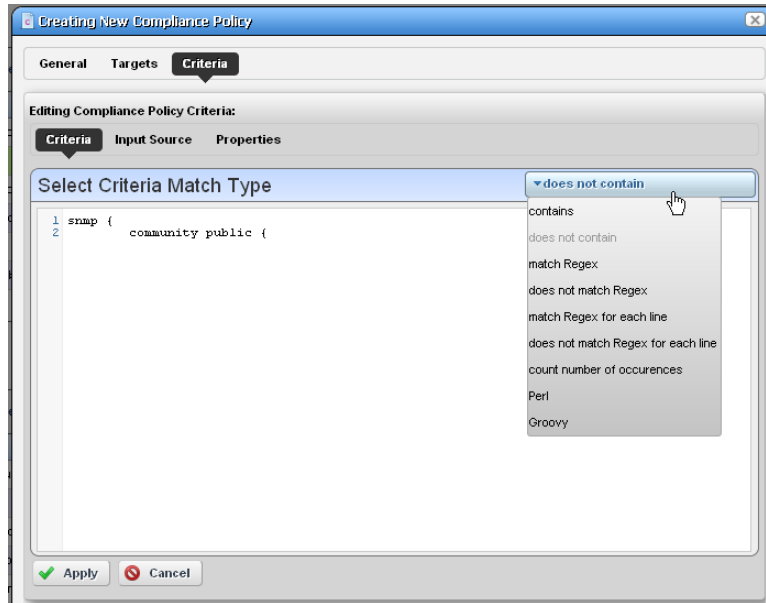
- Editing Compliance Policy Criteria
- Match Regex for each line
- Count number of occurrences
- Input Source Grouping

For additional criteria information consult these sections:

- Create Source Group Criteria
- Regular Expressions
- Perl / Java (Groovy) Language Policies

## Editing Compliance Policy Criteria

After clicking *Add Criteria*, use the pick list on the upper right to select an operation to select a criteria match type (*Contains*, *Doesn't contain*, *[does not] match Regex* (see *Regular Expressions on page 320*), *[does not] Match Regex for each line*, *Count number of occurrences*, *Perl* or *Java* (Groovy)). Specify the match string or regular expression (Regex) in the text editor below the pick list.



### Tip

With the *Add Criteria* button, you can configure multi-criteria policies with several lines. For example, configure one saying a maximum of four lines containing `name-server` can appear (<5), in any order (*Match Regex for each line*), and another that says the configuration must contain `no ip domain lookup [domain]`. Notice the radio buttons *Match Any of the following* and *Match all of the following*. Selecting *Any* means that if either of the lines matched the policy would succeed. Selecting *All* says that both lines must pass before the policy is successful.

For more complex scans, you can also enter Perl or Java (Groovy) language policies. See *Perl / Java (Groovy) Language Policies on page 322* for details about these.

### NOTE:

The *does not* operators are just the negative of the match without *does not*.

Click the *Apply* green check button to accept your term, or the *Cancel* button to abandon your edits.

You can edit already listed compliance tests by clicking the *Edit* button (pencil and paper) in the list row. You can delete them by clicking the *Delete* button next to the criterion.

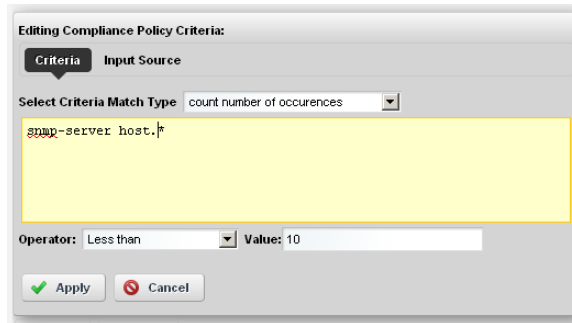
### Match Regex for each line

In using this type of term, OpenManage Network Manager processes each line separately, comparing the input source to the match criteria. This returns a true value only if the criteria find a match in the source. The order of matching is not important since OpenManage Network Manager processes each line separately.

### Count number of occurrences

This operator lets you specify a less than, greater than, or equal mathematical operator (<, >, =) and a number of lines after you provide regex or string criteria with the operator and count value.

This returns true if the criteria (as a whole) match the input source count and operator combination. On the other hand, for example, if you choose a match criterion that includes =9 lines as the operator, and the scanned configuration has ten lines that match, the scan returns *false*.

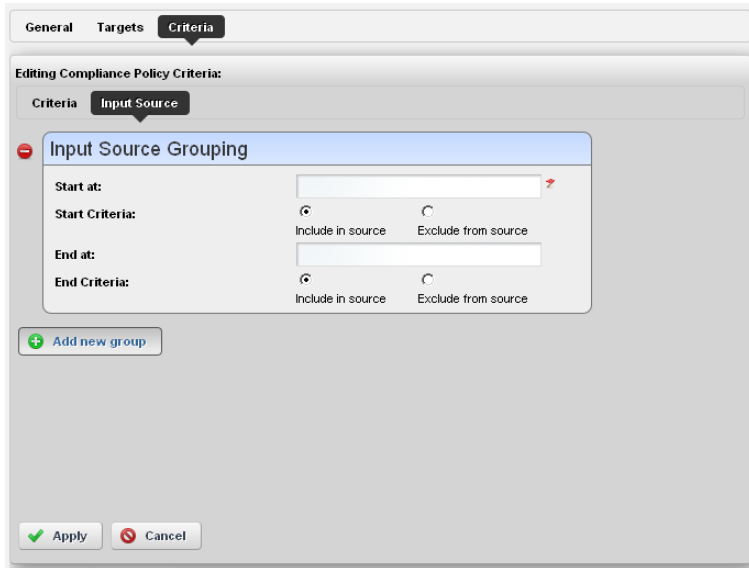


### Input Source Grouping

Configuration files often have repeating sections or groups of parameters. OpenManage Network Manager scan configurations by section using *Start Criteria* and *End Criteria* Regex group criteria patterns. A configuration can contain multiple start and stops. This is especially useful when the criteria provided might occur multiple times in the input source but you want to find only the instances which are preceded by a particular line in the source.

Click *Add new group* in the *Input Source* panel, and the grouping editor appears. (Click the red icon to the source grouping's left to delete it.)

Enter the starting and ending regular expressions (*Start at / End at*), and elect whether the beginning or end of the source group includes or excludes what that expression matches. Click *Apply* to accept your edits, or *Cancel* to abandon them. You can create multiple group criteria.



OpenManage Network Manager applies the group criteria in order, from top to bottom.

When you have defined a *Start* and *Stop*, OpenManage Network Manager finds the information between these. OpenManage Network Manager logically extracts the data from the main config (essentially creating sections) and then does the audit.

For example, if your configuration has one section of *router bgp* and multiple sections for each *bgp neighbor*, you can specify matches within each neighbor. Your policy can audit each router *bgp* section and each neighbor within each router *bgp*.

See *Create Source Group Criteria* below for an example of how to use these capabilities. Also, see *Regular Expressions* below for more about what match criteria are supported.



## How To:

### Create Source Group Criteria

Here is an example of how you can use source group criteria. Suppose you want to scan for the following text:

```
neighbor 2.3.4.5 activate
neighbor 2.3.4.5 route-map allanRM01
```

This is within the following configuration:

```
router ospf 888
  log-adjacency-changes
```

```

redistribute bgp 88 metric 10010 metric-type 1 subnets tag 334 route-map
  allanRM02
network 2.3.4.0 0.0.0.255 area 123
network 2.3.5.0 0.0.0.255 area 124
network 2.3.6.0 0.0.0.255 area 125
!
router isis
!
router rip
  version 2
  network 175.92.0.0
  no auto-summary
!
address-family ipv4 vrf VPN_PE_A
no auto-summary
  no synchronization
  exit-address-family
!
router bgp 88
  bgp log-neighbor-changes
  neighbor 2.3.4.5 remote-as 22
  neighbor description "This is Test"
  neighbor test-parameter xxx
  neighbor 4.5.6.7 remote-as 66
  neighbor description "This is Test"
neighbor test-parameter xxx
!
address-family ipv4
redistribute connected route-map map-12
redistribute static route-map hjlhjhjhjk
redistribute ospf 888 metric 500 match internal external 2 nssa-external 1
  nssa-external 2 route-map allanRM03
neighbor 2.3.4.5 activate
neighbor 2.3.4.5 route-map allanRM01 in
neighbor 4.5.6.7 activate
neighbor 4.5.6.7 route-map allanRM02 in

```

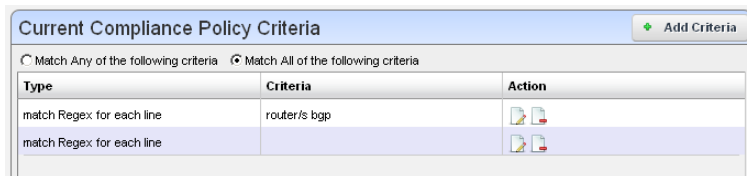
```

default-information originate
no auto-summary
no synchronization
exit-address-family
!
address-family ipv4 vrf VPN_PE_A
redistribute ospf 10 vrf VPN_PE_A match internal external 1 external 2
no auto-summary
no synchronization
exit-address-family
!

```

In addition, within this configuration, you want to check if the target lines are present under each address-family in the *router bgp* section. To scan for this, follow these steps:

- 1 Select the *Match All of the following* radio button and enter both of the above lines as match criteria. Select the *Config Term* as *match Regex for each line*, so the order in which these lines appears does not matter.
- 2 Add a source group criterion to search for a section that begins with “routers bgp”—in regex: `routers\sbgp`. No end match criterion is needed. Click *Apply*.
- 3 Click *Add* to make another criterion. This time, the start is `address-family\s`, and the end is `exit-address-family`. Click *Apply*.
- 4 You should see both criteria listed in the editor



- 5 Applying the first group criterion finds the match (underlined) in the following:

```

router bgp 88
  bgp log-neighbor-changes
  neighbor 2.3.4.5 remote-as 22
  neighbor description "This is Test"
  neighbor test-parameter xxx
  neighbor 4.5.6.7 remote-as 66
  neighbor description "This is Test"
  neighbor test-parameter xxx
!

```

```

address-family ipv4
redistribute connected route-map map-12
redistribute static route-map hjlhjhjhjk
redistribute ospf 888 metric 500 match internal external 2 nssa-external 1
  nssa-external 2 route-map allanRM03
neighbor 2.3.4.5 activate
neighbor 2.3.4.5 route-map allanRM01 in
neighbor 4.5.6.7 activate
neighbor 4.5.6.7 route-map allanRM02 in
default-information originate
no auto-summary
no synchronization
exit-address-family
!
address-family ipv4 vrf VPN_PE_A
redistribute ospf 10 vrf VPN_PE_A match internal external 1 external 2
no auto-summary
no synchronization
exit-address-family
!

```

6 Applying the second group criterion on the above result divides the source:

Source 1:

```

address-family ipv4
redistribute connected route-map map-12
redistribute static route-map hjlhjhjhjk
redistribute ospf 888 metric 500 match internal external 2 nssa-external 1
  nssa-external 2 route-map allanRM03
neighbor 2.3.4.5 activate
neighbor 2.3.4.5 route-map allanRM01 in
neighbor 4.5.6.7 activate
neighbor 4.5.6.7 route-map allanRM02 in
default-information originate
no auto-summary
no synchronization
exit-address-family

```

Source 2:

```
address-family ipv4 vrf VPN_PE_A
 redistribute ospf 10 vrf VPN_PE_A match internal external 1 external 2
 no auto-summary
 no synchronization
 exit-address-family
```

This creates two sources sections.

- 7 Now OpenManage Network Manager applies the regex in the criteria field to each of the sources. It returns *true* only if both sources pass (we selected the *Match All* radio button). In this case “Source 2” does not have those lines, so OpenManage Network Manager returns a false value.
- 8 The error details appear in the audit trail panel.

## Regular Expressions

The following table outlines standard, supported regular expressions.

Label	Pattern
Single digit	\d
Two digits	\d{2}
Three digits	\d{3}
Four digits	\d{4}
Five digits	\d{5}
Number	[0-9]+ One or more [0-9]* Zero or more
Decimal	.[0-9]+
Float	[0-9]+.[0-9]+
IP Address	(\d{1,3}.)\{3\}\d{1,3}
IP Address/Mask	(\d{1,3}.)\{3\}\d{1,3}\^d+
Domestic phone number with extension	1?[\s\-\.\.]*\((?[1-9]\d{2})\)?[\s\-\.\.]*([0-9]{3})[\s\-\.\.]*([09]{4})[\s\-\.\.]*([0-9]{3,4})?
MAC Address	([0-9a-fA-F]{1,2}:){5}[0-9a-fA-F]{1,2}
MAC Address	([0-9a-fA-F]{1,2}.){5}[0-9a-fA-F]{1,2}
MIB2 OID	(1.3.6.1.6.1.2.1.\(d+\.\)+\d)
Enterprise OID	(1.3.6.1.4.1.\(d+\.\)+\d)
Time	[0-1][0-3]:[0-5][0-9]:[0-5][0-9]
All	.*



Label	Pattern
Ending Number	\d+\$
Character	\w
Word	\w+ One or more. \w* Zero or more.
Whitespace	\s+ One or more. \s* Zero or more.
String w/o space	\S+ One or more. \S* Zero or more.
Newline	\n
FormFeed	\f
Tab	\t
Carriage Return	\r
Backspace	\b
Escape	\e
Backslash	\B
URL	(?:^ ")(http ftp mailto):(?:/)?(\w+(?:[.:@]\w+)*)(?:/ @)([^\?"]*)(?:\?([^\?"]*))?(?:\$ ")
HTML Tag	<(\w+)[^>]*?>(.*?)</\1>

Here are some examples of such expressions:

Label	Pattern
Email address (U.S.)	^[A-Za-z0-9._%+-]+@[A-Za-z0-9.-]+\.[A-Za-z]{2,4}\$
MAC Address	([0-9a-fA-F]{1,2}:){5}[0-9a-fA-F]{1,2}
Time hh:mm:ss	(0[0-9] 1[0-2]):[0-5][0-9]:[0-5][0-9]
IP Address	(\d{1,3}.){3}\d{1,3}
Validated IP Address (restricts what matches better than the previous example)	(25[0-5] 2[0-4][0-9] [01]?[0-9][0-9?])\.(25[0-5] 2[0-4][0-9] [01]?[0-9][0-9?])\.(25[0-5] 2[0-4][0-9] [01]?[0-9][0-9?])\.(25[0-5] 2[0-4][0-9] [01]?[0-9][0-9?])
MIB2 OID	(1.2.6.1.6.1.2.1.(\\d+\\.)+\\d

The following are examples of the kinds of matching possible:



**CAUTION:**

Cutting and pasting from notepad into OpenManage Network Manager may cause carriage return or line-feed issues. Best practice is to compose these within OpenManage Network Manager.

## Perl / Java (Groovy) Language Policies

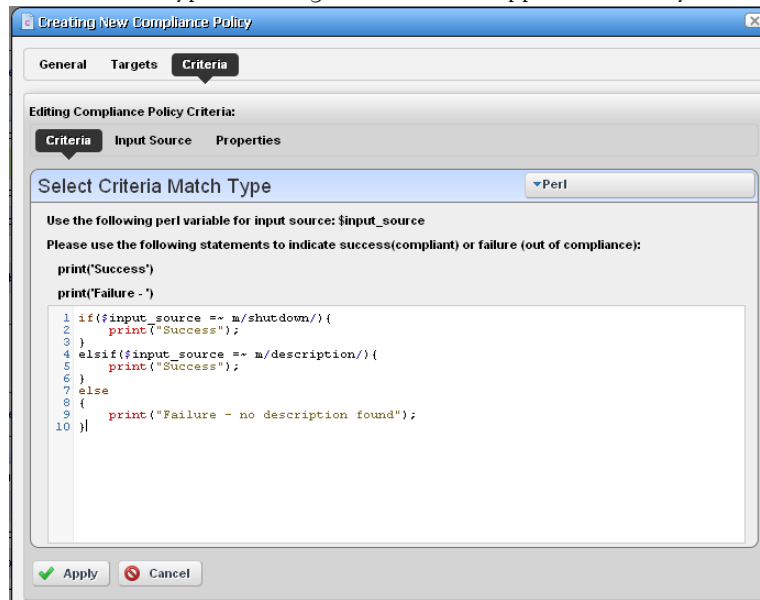
In addition to regular expressions, you can enter Config Terms that use either Perl or Java (Groovy) language capabilities for scans. The following sections describe these.

- Perl
- Java (Groovy)

These scans are compiled at runtime, and the Java scan uses the Groovy libraries, included with OpenManage Network Manager. As always, you must install Perl on Windows application servers if you want to use that type of Config Term (it typically comes with other supported operating systems).

### Perl

When you select Perl as the type of Config term, an editor appears that lets you enter Perl scans.



As the screen says `$input_source` is what the code scans. The following is example of the type of Perl you can enter that scans for contents like `description` in shut down interfaces, and prints output "Success" visible in the Audit viewer when it finds a matching term like `description` in whatever source you select:

```
if($input_source =~ m/shutdown/){
    print("Success");
}
elsif($input_source =~ m/description/){
    print("Success");
}
```

```

}
else
{
    print("Failure - no description found");
}

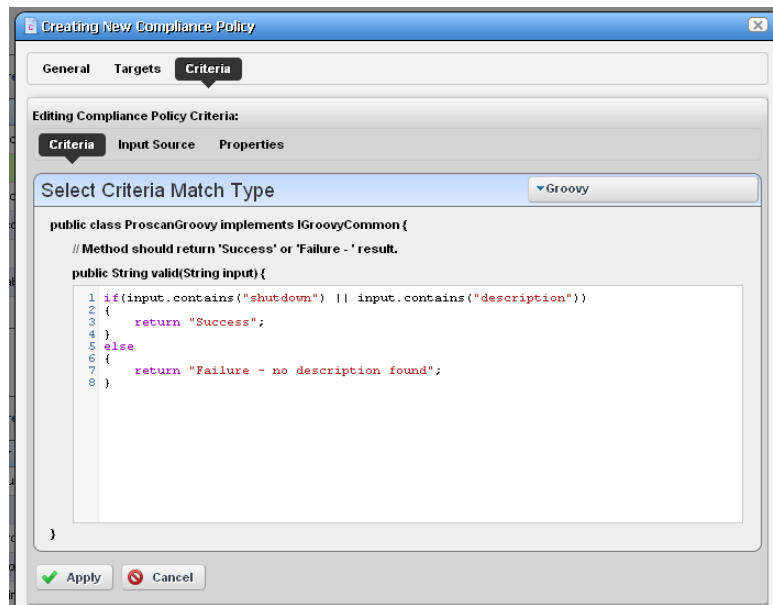
```

**Tip**

Notice that you can also combine these scans with the *Edit Source Group Criteria* regular expressions to streamline them.

### Java (Groovy)

When you select Groovy as the type of Config term, an editor appears that lets you enter that type of scans.



As the screen says this implements ProScanGroovy or Groovy Java classes. The method should return 'Success' or 'Failure -' results, and assumes public String validate (String input) { precedes what you enter in the text editor. The following is example of the type of Java code you can enter that scans for contents like description in shut down interfaces, and prints output "Success" visible in the Audit viewer when it finds a matching term like description in whatever source you select:

```

if(input.contains("shutdown") || input.contains("description"))
{

```

```

    return "Success";
}
else
{
    return "Failure - no description found";
}

```

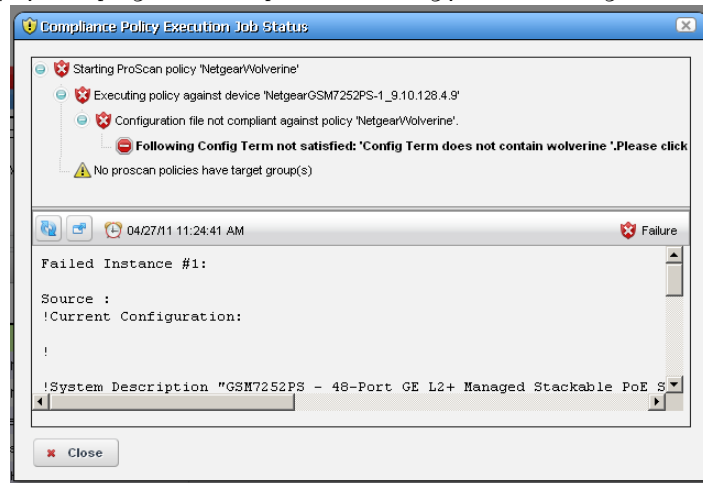
### Tip

Notice that you can also combine these scans with the *Edit Source Group Criteria* regular expressions to streamline them.

Click *Save* to preserve the policy you have configured in these screens, or click *Close* (in the tool bar) to abandon your edits.

## Compliance Policy Job Status

This screen displays the progress of compliance scanning you have configured.



You can the revisit history of this policy’s use in the Audit portlet (see Audit Trail Portlet on page 93). Select an audit trail in this portlet to review details.

When you see the *Success* indicator, then the scanned item is compliant. If you also see a warning message that no policies have target groups, this does not have an impact on compliance.

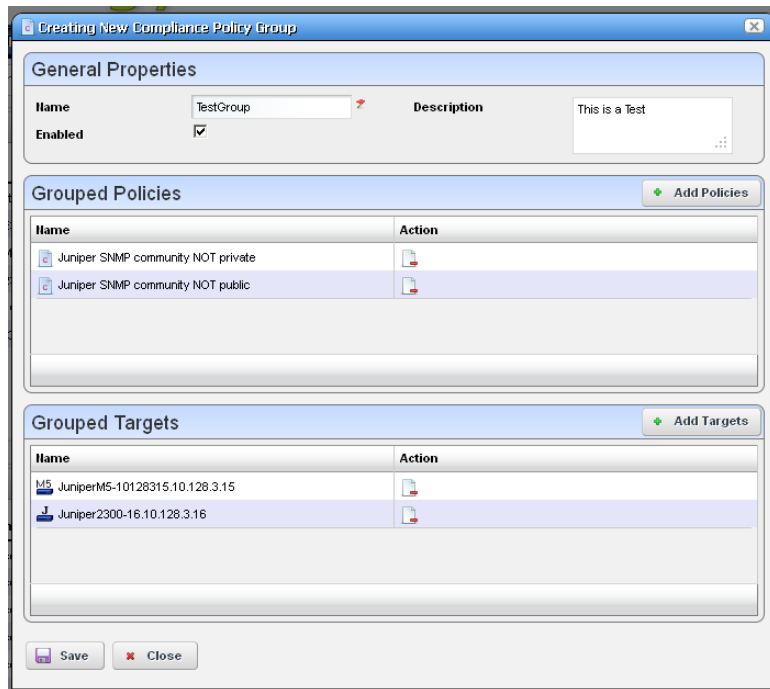


When you see the *Failure* indicator, then the scanned item is *Not* compliant. Select the “Following Config Term not satisfied” message to see the contents of the failed file at the bottom of this screen.



## Creating or Modifying ProScan Policy Groups

When you create or modify a ProScan Policy Group after right-clicking *New > Group* or *Open* when you have selected a group, the ProScan Policy Group editor appears.



This has the following to configure:

**Name**—A text identifier for the group.

**Enabled**—Check to enable this grouping.

**Grouped Policies** —Click *Add Policy* to select ProScan policies in a selector screen. Click the *Remove* icon to delete a selected policy. You can use individual policies in several groups.

**Grouped Targets**—Click *Add Targets* to select targets for the scans.

### NOTE:

*Individual policies that are part of groups display inherited group targets grayed out.*

Executing a group executes all the member policies and update the history records of the group and member policies. Any policy execution also update its parent group history records.

# Change Determination Process

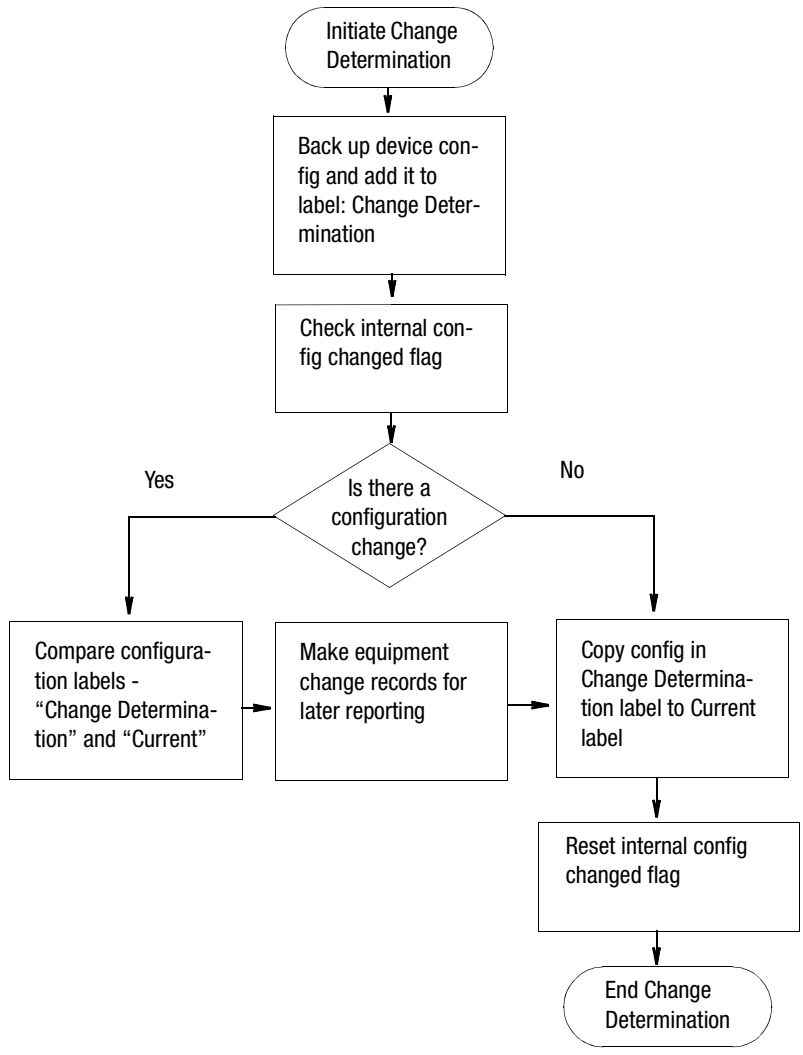
If you run the *Change Determination (CD) Process*, it collects all the configuration changes that occurred on the target resources since the last time the CD process ran. It also associates these changes with the date and time when the CD process runs. After running CD, you can then produce a report (see *Compliance and Change Reporting on page 329*), outlining all such changes by date and time. This report comes seeded with installation.

Dell OpenManage Network Manager stores incremental changes as *RedcellConfigChangeRecords* by device/timestamp. The *ConfigChangeRecordsDAP* Database Aging Policy (DAP) manages how long the OpenManage Network Manager database retains these records. This DAP's default setting stores incremental records for 30 days, then archives or purges them. Reporting shows only records in the database; therefore, by default, the *Configuration Change Report* shows only resource changes made in the last 30 days, but no older. Change this default by changing the number of days to retain such records with the DAP.

The next section describes Change Determination Process Workflow.

# Change Determination Process Workflow

Change Manager seeds the Change Determination Process and ProScan group operations. You can configure this to run on groups of your choosing if you create a new Change Determination Process group operation.



This process records what is removed, updated or added since it last ran on a scanned device's configuration. If you run the Change Determination Process on equipment, it first backs up the devices' configuration(s), and stores those with the Change Determination label.

Change Determination Process then looks for Config Changed Flags, and if it finds such flags, indicating a change occurred on the device, it then compares the device's changed configuration (in the Change Determination label) to the one in the Current label, storing the difference for future reporting.

At its end, the Change Determination Process re-labels the configuration with the Change Determination label to the Current label, and it un-sets the Config Changed Flag on scanned resources so the flag will not signal change occurred when Change Determination runs again.

After running the Change Determination Process, you can run the Configuration Change report to display what changed for a defined period. The contents of that report depends on the report filter, and the specified period. This report lists changed attributes in the configurations.

You can also execute CD as a scheduled operation. Find it in the Schedules portlet, where it is disabled by default. Open, and enable it. CD runs with the *All Devices* group as its target. You can also execute CD as a target action of an Event Processing Rule, so it runs against the device that generated the trap triggering that Rule. (See Event Processing Rules on page 108.) In either case, Dell OpenManage Network Manager determines incremental configuration changes for resources by comparing the latest backup version against the version to which a resource's Change Determination label points.

Before making this comparison, Dell OpenManage Network Manager determines whether it made configuration changes that have not yet been backed up. If such changes exist, Dell OpenManage Network Manager backs up the resource configuration before running the CD process. Dell OpenManage Network Manager always flags configuration changes made (in Dell OpenManage Network Manager) between backups, clearing these flags following a config file backup.

Once the CD process compares configurations, and determines and stores the incremental configuration changes, it updates the resource's *Change Determination* label to point to the latest config file backup version.

Steps in the Change Determination Process are as follows:

- 1 Retrieve configuration file indicated by the Change Determination Label (if any).
- 2 Retrieve configuration file indicated by the Current Label (which should be the same as the device in the network has).
- 3 Compare these two files.
- 4 Write changes to History Records that will be used during Change Reporting.
- 5 Move Change Determination Label for this device to the configuration file pointed to by the Current Label.

If the Change Determination Label points to no configuration file for this device, it must be the very first time this device is processed by the Change Determination Process: It creates a Change Determination Label Item for this Device.

The compliant label contains a pointer to the last configuration file that was compliant for each device that has been through ProScan. If a device fails ProScan, you can automatically restore the last compliant configuration file, indicated by the compliant label.



To retrieve this information, see the instructions in Compliance and Change Reporting on page 329.



## How To:

### Run Change Determination

Follow these steps to run the Default Change Determination:

- 1 In the Schedules portlet, locate the Default Change Determination operation.
- 2 Right-click and select *Open*.
- 3 Configure the schedule

This runs Change Determination with the target group of *All Devices* (all discovered devices).

## Change Determination Defaults

By default, Change Determination can run against all devices without requiring the config change update flag be set or updated based on events tied to the Config Update Flag event processing rule/action.

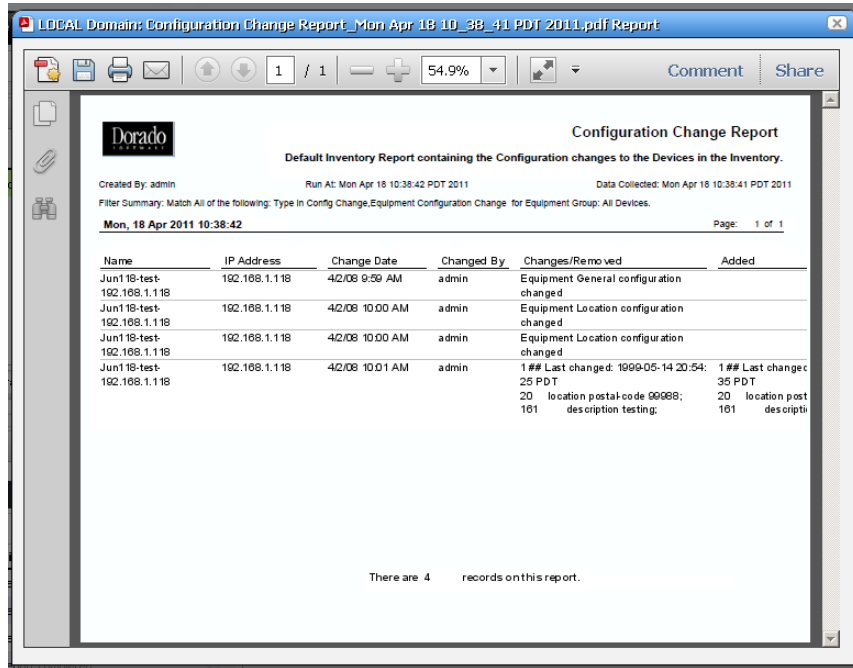
To disable the manual run-ability of the Change Determination process, uncomment the property in `\owareapps\changemgmt\lib\cm.properties` (or add it to `\owareapps\installprops\lib\installed.properties`).

```
#####  
# Change Determination Flag  
# Allows system to be flagged to only run  
# change determination against devices we  
# have received Config Change Event for.  
# Default Behavior is to run change determination  
# for All targets (the same as setting the below property = false)  
#com.dorado.changemgmt.change.determination.require.config.events=true
```

## Compliance and Change Reporting

The Compliance Policy Violation report is seeded when you have ProScan / Change Management in Dell OpenManage Network Manager. Inventory Compliance Attributes for reporting can also appear in report templates when you install ProScan. These report in-compliance or out-of-compliance, the last compliance date (when last compliant or not compliant), last config date (when configuration last changed), last checked date (when change was last determined).

You can also run the Change Determination Report that displays changes made to configurations.



See Reports on page 200 for more about reporting capabilities.

The Change Determination Report report displays detected changes based on a configuration change flag set when OpenManage Network Manager detects a change made to the device. To successfully execute this report, you must enable a scheduled Change Determination Process. The process must run before the reports has any contents. To run the process, go to the Schedules portlet, and schedule that change determination process.

### Reporting Limitations

The Configuration Change Report only reports on incremental configuration changes discovered in the CD process. Simply making changes to configurations and backing them up in OpenManage Network Manager does *not* ensure these appear in *Configuration Change Reports*. They appear in reports only after running the CD process.

The *Configuration Change Report* includes a Filter that you can alter at runtime. By default, the report filters on *Type* only. If you want more filter criteria—like device IP, and/or date ranges—you must edit the Report filter. To edit the filter, in the Reports manager, right click the *Configuration Change Report*, and select *Open*, then edit the filter in the *Filter* screen by selecting that node on the left.

 **Tip**

A recommended best practice is to execute the CD process as an operation run against multiple resources following a scheduled group backup of these resources. If you run backups every day, the *Configuration Change Report* then shows the daily changes, until they are purged from the database.

The application stores the specifics of what changed for future reporting.



## How To:

### Report on Change Determination

Follow these steps to produce regular change determination reports:

- 1 First, insure the devices you want to scan are discovered, and send change notifications to the application server.

Check your vendor's manuals to determine how to forward configuration change information to Dell OpenManage Network Manager for your system.

- 2 When Dell OpenManage Network Manager receives a configuration change notification, the device transmits an event to the OpenManage Network Manager mediation server. When received, this event automatically generates an event called OpenManage Network ManagerEquipmentConfigChangeNotification. Event history displays that notification.
- 3 When OpenManage Network Manager receives the OpenManage Network ManagerEquipmentConfigChangeNotification event, it can initiate (if enabled) an event processing rule called *Configuration Change*.

This processing rule triggers a flag in the OpenManage Network Manager database saying a change has occurred in the device's configuration and that OpenManage Network Manager should run change determination against the device when requested.

- 4 When you run OpenManage Network Manager's change determination process, it reviews the flag setting in the database and backs up a managed device if the flag indicates a change. This backup updates the OpenManage Network Manager system label *Current* which is then compared to the OpenManage Network Manager system *Change Determination* label. OpenManage Network Manager then writes the differences between the two labelled configurations to its database, where it is available for reporting purposes.
- 5 Once this occurs, the *Change Determination* label moves to point to the same configuration which is reflected by the *Current* label.

- 6 The report which can run to display these changes is OpenManage Network Manager's *Configuration Change Report*. It displays the name of the device in question, the IP address, date/time of change, who made the change, what was removed and what was added. You can schedule this report to run immediately after an Change Determination process too, so you can capture a history of changes.

## Storage Arrays

### Introducing Storage Arrays

This chapter describes Storage Arrays as they appears in Dell OpenManage Network Manager's web portal. These appear in the portlet described in Managed Resources on page 166, as well as the Storage Array Portlet, which offers storage-array-specific capabilities. The following sections describe these capabilities.

Storage arrays appear in the Storage Array Portlet when they are discovered. See Resource Discovery on page 152 for a description of that process.

### Storage Array Portlet

This portlet lets you manage storage arrays on your network.

Network Status	Equipment Name	IP Address	Vendor	Total Capacity (GB)
Online	NG_NAS_15.10.128.12.15	10.128.12.15	Netgear	4655

The summary portlet displays columns describing the listed arrays' *Status*, *Equipment Name*, *IP Address*, *Vendor*, and *Capacity*.

The following menu items are available from right-clicking in the portlet:

**Edit**—Select from the General, Authentication or Management Interface editors in the sub-menu. For information about the last two, see Managed Resources on page 166.

**Details**—This opens a screen for the selected storage array like the one described in Equipment Details on page 178.

**Resync**—Updates Dell OpenManage Network Manager with the latest information from the device.

**Delete**—Remove the selected service array from the list.

**Show Key Metrics**—Displays the key metrics for the selected array. See Key Metric Editor on page 289 for more about configuring these.

**Audit Trail**—Displays the audit trails for the selected storage array, as described in Audit Trail Viewer on page 92.

For additional information, you can click the plus in the upper right corner of this portlet to see the Storage Array Portlet Expanded.

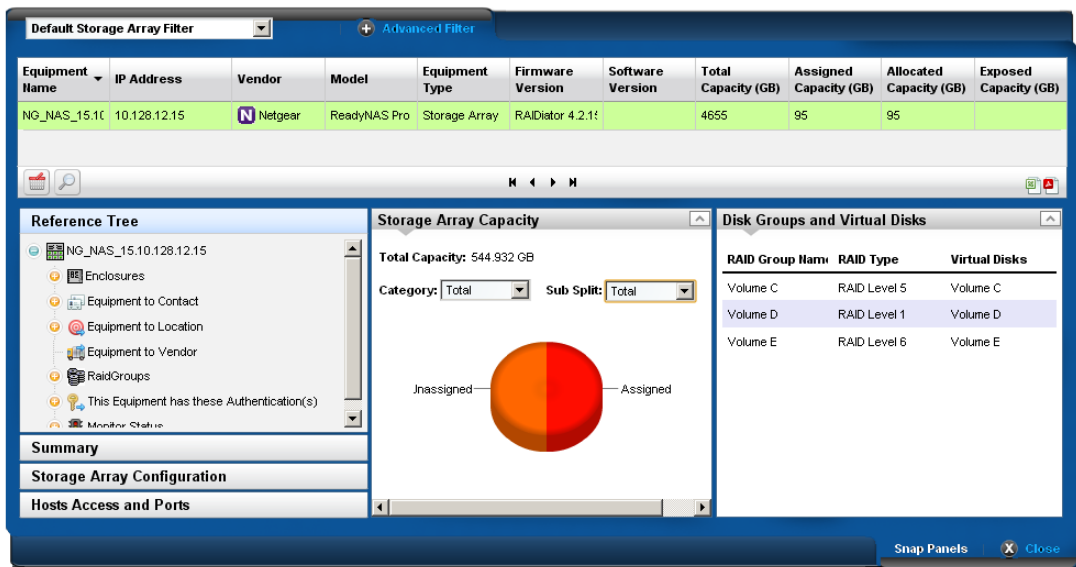


**Tip**

Storage arrays also appear in the Managed Resources portlet.

### Storage Array Portlet Expanded

The expanded portlet displays additional information about discovered storage arrays.



The expanded portlet adds columns for *Firmware Version*, *Software Version*, *Total Capacity (GB)*, *Assigned Capacity (GB)*, *Allocated Capacity (GB)*, and *Exposed Capacity (GB)*.

This screen also contains several Snap panels that contain information about the listed array you select. The first four are visible when you click their labels on the left of the screen.

- Reference Tree
- Summary
- Storage Array Configuration
- Host Access and Ports

- Storage Array Capacity
- Disk Groups and Virtual Disks

### Reference Tree

This panel displays the array’s connection to various components like Enclosures (including fans, power supplies, controllers and disk drives), Contacts, Locations, Vendors, Raid Groups, Authentications, and monitors.



### Tip

You can right-click some of the reference tree items to edit or otherwise act on them.

### Summary

This panel displays the following information about the selected array:

**STATUS**—Whether the array is online.

**DATA PROTECTION TYPES**—The data protection types on the array. For example, the RAID type.

**PROTOCOL**—The protocol to communicate with this array.

**CLONING OPTION**—Whether the array is cloned or not.

**SNAP SHOT OPTION**—Whether the array has a snap shot or not.

Reference Tree	
Summary	
<b>STATUS:</b>	Online
<b>DATA PROTECTION TYPES:</b>	RAID 0, RAID 1, RAID 5, Hot Spare
<b>PROTOCOL:</b>	Not Set
<b>CLONING OPTION:</b>	Not Cloning Option
<b>SNAP SHOT OPTION:</b>	Snap Shot Option
<b>POWER SUPPLIES:</b>	2
Storage Array Configuration	
Hosts Access and Ports	

### Storage Array Configuration

This panel displays the following information about the selected array:

**CONTROLLERS**—A count of the array’s controllers.

**MAX CONTROLLERS**—The array’s maximum number controllers.

**ENCLOSURES**—A count of the array’s enclosures.

**ENCLOSURES SUPPORTED**—The number of enclosures supported.

**PHYSICAL DISKS**—A count of the array’s physical disks.

**MAX DRIVES**—The number of physical disks this array can support.

**DRIVE TYPES**—The types of drives in the array (SATA, USB, and so on).

**VIRTUAL DISKS**—A count of the array’s virtual disks.

Reference Tree	
Summary	
Storage Array Configuration	
<b>CONTROLLERS:</b>	Not Applicable
<b>MAX CONTROLLERS:</b>	Not Applicable
<b>ENCLOSURES:</b>	Not Applicable
<b>ENCLOSURES SUPPORTED:</b>	Not Applicable
<b>PHYSICAL DISKS:</b>	5
<b>MAX DRIVES:</b>	6
<b>DRIVE TYPES:</b>	SATA, USB
<b>VIRTUAL DISKS:</b>	0
<b>MAX VIRTUAL DISKS:</b>	Not Applicable
Hosts Access and Ports	

**MAX VIRTUAL DISKS**— How many virtual disks the array can support.

### **Host Access and Ports**

This panel displays the following information about the selected array:

**CONFIGURED HOSTS**—The hosts configured for the array.

**MAX CONFIGURED HOSTS**—The maximum number of configured hosts the array supports.

**HOSTS TO VIRTUAL DISK MAPPINGS**—Connections between virtual disks and configured hosts.

**PORTS**—The number of ports within the array.

**MAX PORTS**—The maximum number of ports the array supports.

**PORT TYPES**—The type of ports the array supports (Ethernet iSCSI, and so on).

Reference Tree	
Summary	
<b>Storage Array Configuration</b>	
<b>Hosts Access and Ports</b>	
<b>CONFIGURED HOSTS:</b>	Not Applicable
<b>MAX CONFIGURED HOSTS:</b>	Not Applicable
<b>HOSTS TO VIRTUAL DISK MAPPINGS:</b> Not Applicable	
<b>PORTS:</b>	2
<b>MAX PORTS:</b>	2
<b>PORT TYPES:</b>	ETHERNET, iSCSI

### **Storage Array Capacity**

This panel displays a graph and the following information about the selected array:

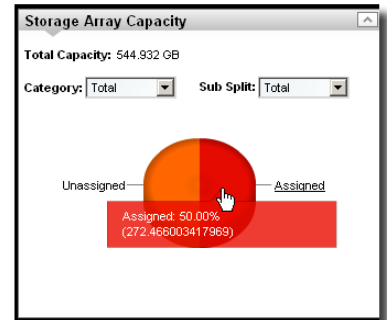
**Total Capacity**—The array's total capacity.

The following fields do not appear for all devices.

**Category**—Select the category of storage displayed in the graph. These include *Total*, *Assigned*, *Allocated*, and *Unexposed*.

**Sub Split**—Options include *Total*, *Assigned*, *Allocated* and *Unexposed*.

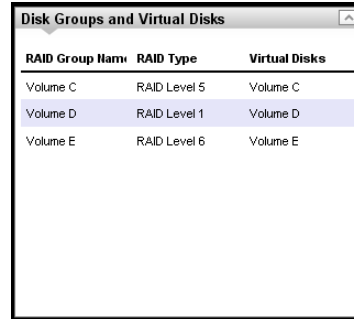
Hover the cursor over the graph to see the GB and percentage of the segment(s) displayed.





### Disk Groups and Virtual Disks

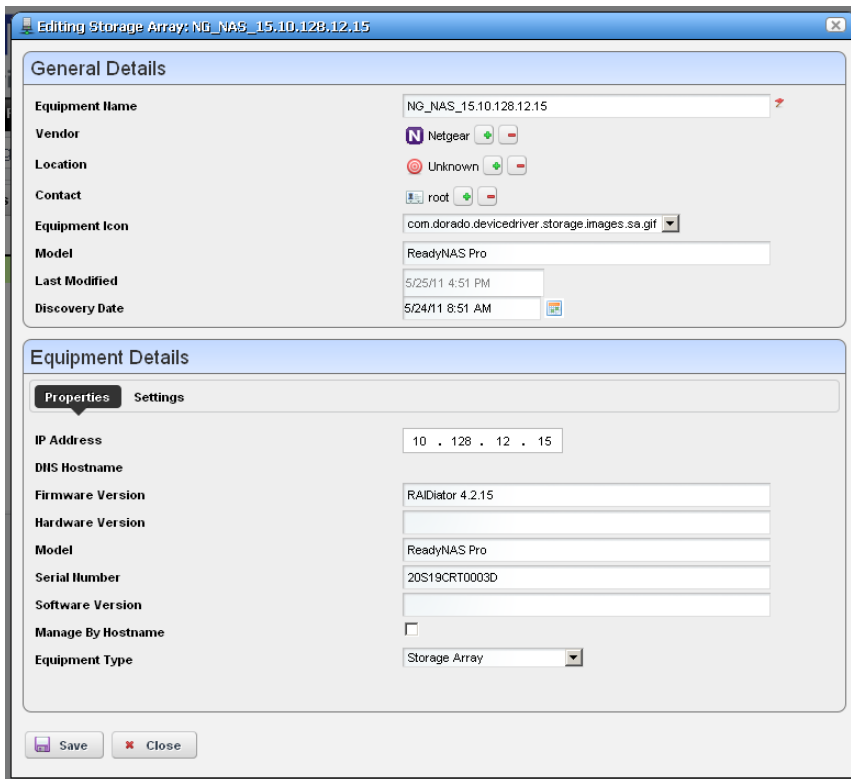
This displays the disk groups and virtual disks for the selected array. This lists the RAID Group Name, the RAID Type, and its Virtual Disk.



RAID Group Name	RAID Type	Virtual Disks
Volume C	RAID Level 5	Volume C
Volume D	RAID Level 1	Volume D
Volume E	RAID Level 6	Volume E

### General

This editor lets you configure general features of discovered storage arrays.



**Editing Storage Array: NG\_NAS\_15.10.128.12.15**

**General Details**

Equipment Name: NG\_NAS\_15.10.128.12.15

Vendor: Netgear

Location: Unknown

Contact: root

Equipment Icon: com.dorado.devedriver.storage.images.sa.gif

Model: ReadyNAS Pro

Last Modified: 5/25/11 4:51 PM

Discovery Date: 5/24/11 8:51 AM

**Equipment Details**

Properties Settings

IP Address: 10 . 128 . 12 . 15

DNS Hostname:

Firmware Version: RAIDiator 4.2.15

Hardware Version:

Model: ReadyNAS Pro

Serial Number: 20S19CRT0003D

Software Version:

Manage By Hostname:

Equipment Type: Storage Array

Save Close

This screen has the following fields:

#### General Details

**Equipment Name**—The identifier for the array.

**Vendor**—The brand of the array. Use the + or - buttons to select this if discovery did not automatically populate this field.

**Location**—The location of the array. Use the + or - buttons to select this if discovery did not automatically populate this field. See *Locations* on page 135 for information about configuring locations.

**Contact**—The contact for the array. Use the + or - buttons to select this if discovery did not automatically populate this field. See *Contacts on page 133* for information about configuring contacts.

**Equipment Icon**—The icon that appears in the portlet.

**Model**—The model of the array.

**Last Modified**—The date this array was last modified.

**Discovery Date**—The date this array was discovered.

### ***Equipment Details / Properties***

**IP Address**—The IP address for the array.

**DNS Hostname**—The DNS host for the array.

**Firmware Version**—The firmware version for the array.

**Hardware Version**—The hardware version for the array.

**Model**—The model of the array.

**Serial Number**—The serial number of the array.

**Software Version**—The software version for the array.

**Manage By Hostname**—Check to manage by hostname rather than IP address.

**Equipment Type**—The software version for the array.

## Equipment Details / Settings

The screenshot shows a web interface for 'Equipment Details' with a 'Settings' tab selected. The interface displays several fields for configuration:

Field	Value
System Object Id	1.3.6.1.4.1.8072.3.2.10.ReadyNASPro
Date created	05/24/2011 08:51
Creator	netgear
Install Date	<input type="text"/>
Administrative State	Not Determined
Operational State	Not Determined
Notes	<input type="text"/>

This tab has the following fields:

**System Object Id**—The Sys object ID of the array.

**Date Created**—The date the Dell OpenManage Network Manager record for the array was created.

**Creator**—The logged in user who created the record for the array.

**Install Date**—The date the array was installed.

**Administrative State**—The administrative state of the array (*Not Determined, Unlocked, Locked, Shutting Down*).

**Operational State**—The operational state of the array (*Not Determined, Enabled, Active, Busy, Disabled*).

**Notes**—Enter text to describe the array here.



## Actions and Adaptive CLI

The Actions Manager lets you manage actions like enabling monitors, file backups, resyncs and so on. These actions are typically limited in scope, and not that complex. On the other hand, it also manages Adaptive CLI (command-line interface) commands to run against devices which can be complex.

These commands amount to “mini-scripts” to query and configure those devices. In it, you can create commands to run against devices after the device driver has opened a connection to the devices. The driver handles logins, and general connection management. You can even initiate these actions with the application’s optional group operations—although if you delete a target group, the operation will not work. Many drivers seed pre-configured command that appear listed when you first open this manager. For a brief overview of creating and using these, see [How to: Create Adaptive CLI Example on page 369](#).

Adaptive CLI’s Attributes capabilities let you insert variables in scripts. See [Attributes on page 350](#) for the details. You can also assemble configurations made here as component Tasks to execute with other component Tasks. You can even use this capability to include Perls scripts within OpenManage Network Manager. See [Perl Scripts on page 368](#).

### Tip

You can have Actions maintain lists like ACLs, and when these change, in the Adaptive CLI script, push the updated list out to the appropriate devices.

Adaptive CLI commands let you map several vendor-specific commands to a single action, so you could, for example, query two types of devices throughout the network for their MAC addresses with a single action. Adaptive CLI actions can also help you debug more complex scripts that either query or configure devices.

The Adaptive CLI manager displays a list of *Configure* and *Show* commands (the *Command Type*) with a *Name*, *Description* and the *Last Run Date*. You can filter what appears in this manager with the fields at its top.

### NOTE:

The contents of the Action Portlet vary, depending on the various options you have installed.

## Using Adaptive CLI

You can quickly take a set of commands or configuration file snippet from a device, copy it directly into the Script editor, mark it up, and save it as a working CLI.

When using the CLI Format, The Adaptive CLI tool will prompt you to create new attributes based upon your script markup. This lets you quickly create a script and schema to create an ACLI. If you have attributes that are mainly simple String attributes, this is a very quick and automated approach.

## Using Perl in Adaptive CLI

If you need conditional logic that goes beyond simple scripting, you can use Perl in Adaptive CLI. The example below checks to see if a String Attribute is empty (null) or not. If the String attribute (`ShowCmdString`) has content, the show command with `ShowCmdString` as a parameter goes to the device. Otherwise, the Perl script skips or excludes this statement.

Embedded CLI Example:

```
[IF ShowCmdString]
    Show [ShowCmdString]
[ENDIF ShowCmdString]
```

You could use the CLI format for the above example, but if you need to check attributes of other types, besides String, then you must switch to Perl. For example:

Boolean `myFlag` equals True:

```
if ($myFlag)
{
    ...
}
```

Integer `myInt` greater than zero:

Example:

```
if ($myInt > 0)
{
    ...
}
```

To check whether a string is a particular value—like from a valid values list entry assigned to the String attribute—then you must also use Perl. The CLI format only can test if the String exists. It cannot validate its value when populated. For example: `EncapsulationType = "VLAN-CCC", "VLAN-TCC", ...` You can not do this check with the CLI Format: `[IF EncapsulationType = "VLAN-TCC"]`. Instead, use a Perl script with a statement like this:

```
If ($EncapsulationType eq "VLAN-TCC")
{
    print "set encapsulation $EncapsulationType\n";
}
```

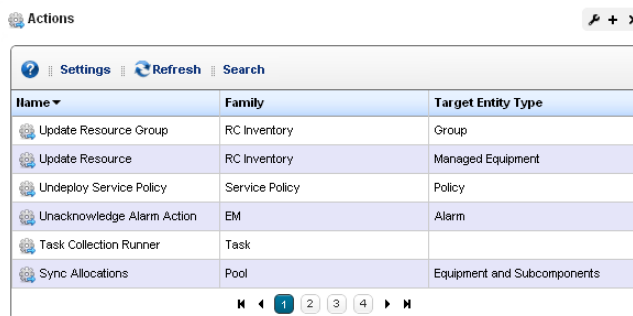
If any attributes in your script are a List (Collection), the only way to loop through the list's items during the Adaptive CLI execution is to use Perl. For example: Processing a List of Strings:

```
$count = 0;
foreach @MyCommandList)
{
    print ("MyCommandList[$count]\n");
    $count++
}
```

## Actions Portlet

The Actions Portlet lets you manage actions like Adaptive CLI, backups, change management actions, and so on. The list of actions available to your system depends on the exact configuration you have installed. This portlet is the primary access point for Adaptive CLI editing.

The summary portlet displays columns with the *Name*, *Family*, and *Target Entity Type* for the listed Action. The Family column describes the type of Action.



The screenshot shows the 'Actions' portlet interface. It features a title bar with 'Actions', a search icon, and window controls. Below the title bar is a toolbar with 'Settings', 'Refresh', and 'Search' buttons. The main content is a table with three columns: 'Name', 'Family', and 'Target Entity Type'. The table contains six rows of actions. At the bottom of the table is a pagination control showing page 1 of 4.

Name	Family	Target Entity Type
Update Resource Group	RC Inventory	Group
Update Resource	RC Inventory	Managed Equipment
Undeploy Service Policy	Service Policy	Policy
Unacknowledge Alarm Action	EM	Alarm
Task Collection Runner	Task	
Sync Allocations	Pool	Equipment and Subcomponents

### NOTE:

For ACLI to be fully functional, you must install Perl on your application server. See Perl on page 32 for more about this.

## Expanded Actions Portlet

The expanded portlet adds columns for *Description*, *Last Web Service ID*, *Access Level*, *Web Service Deployment*, and *Supports Groups*.

The screenshot shows the 'Actions' portlet in Dell OpenManage Network Manager. At the top, there are controls for 'Default Activities Filter', 'Advanced Filter', 'Search', 'Refresh', and 'Settings'. The main table displays a list of actions with columns for Name, Family, Target Entity Type, Description, Web Service ID, Access Level, Web Service Deployment, and Supports Groups. The 'Sync Allocations' row is highlighted in green. Below the table are three snap panels: 'Reference Tree' showing a tree view with 'Sync Allocations', 'Execution History' which is currently empty with the message 'No data is available to display', and 'Scheduled Actions' which shows a single schedule with a descriptor of 'test', a target count of 25, a status of 'Scheduled' (checked), and a next execution time of '8/16/11 1...'. At the bottom right, there are 'Snap Panels' and 'Close' buttons.

Name	Family	Target Entity Type	Description	Web Service ID	Access Level	Web Service Deployment	Supports Groups
Update Resourc...	RC Inventory	Group	Update Resource Gr...		Public	Undeployed	✘
Update Resource	RC Inventory	Managed Equipment	Update Resource		Public	Undeployed	✘
Undeploy Servic...	Service Policy	Policy	Undeploy Service Pol...		Public	Undeployed	✘
Unacknowledge ...	EM	Alarm	Unacknowledge Alarm		Public	Undeployed	✔
Task Collection R...	Task		Executes a task seq...		Public	Undeployed	✘
Sync Allocations	Pool	Equipment and Subc...	Sync Pool Allocations		Public	Undeployed	✘
Spawn Service ...	Service		Spawn Service Mem...		Public	Undeployed	✘
Service Undeploy	Service	Service	Undeploy Service		Public	Undeployed	✘

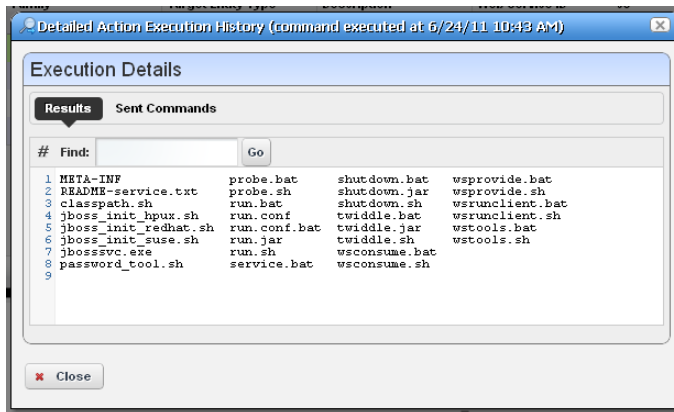
The expanded portlet also has snap panels to display Reference Tree connections between the selection and other elements within Dell OpenManage Network Manager, as well as an Execution History panel listing *Device Name(s)*, *Execution Date* and *Status* for the selected Action, and a Scheduled Actions panel cataloging any Schedules for the selected Action. Right-click a Schedule to edit, execute or delete it.



The Execution History snap panel displays history by device. Right-click to see the details of what occurred when the selected action ran against a particular device (*Execution Details*).

The Execution Details panel displays tabs showing the *Results* of running an Adaptive CLI, and the *Sent Commands*.

You can also *View Job* to see a screen like *the Audit Trail / Jobs Screen on page 91*, or *Delete* to remove a listed Action record from the list.



Right-click menus on the Actions portlet can include the following items (these vary, depending on the Action's family):

**New / Edit** — Lets you create or modify a selected action in the Adaptive CLI Editor, described below.

**Execute**—Execute the selected Action. This typically displays a target equipment selector screen, and a screen where you can configure any parameters necessary for execution, then a screen like the *Audit Trail / Jobs Screen on page 91*. Dell OpenManage Network Manager validates the parameters before executing the Adaptive CLI. If a parameter is invalid, for example a blank community name in the Dell PCT Set SNMP Community Settings Adaptive CLI, Dell OpenManage Network Manager logs a validation error to the audit trail. In this case the Adaptive CLI is not executed and leaves behind no history record.

Some Adaptive CLI scripts also let you *Preview* what is sent the device in a subsequent screen. This does not appear in the execution of Targetless, and Multi-target Adaptive CLIs.

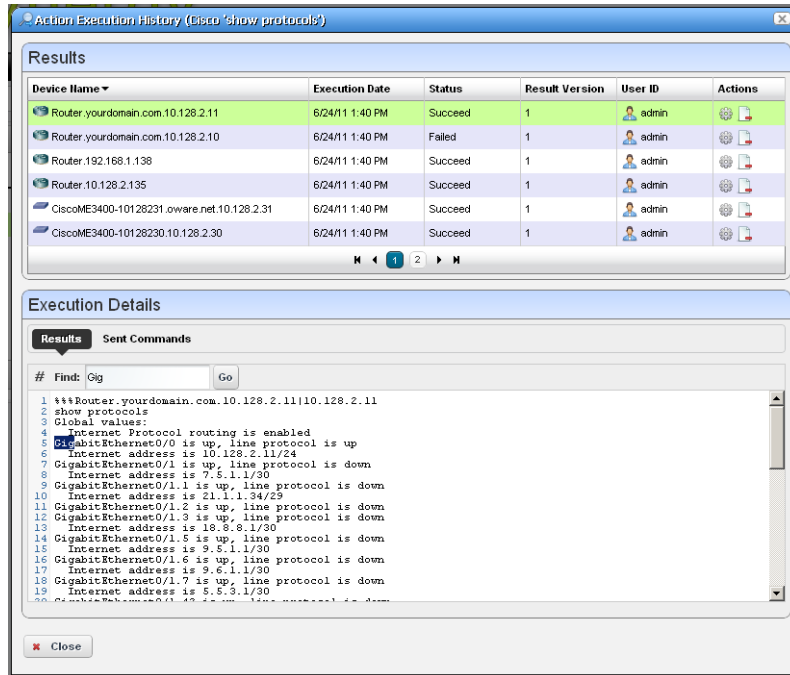
**Details**—Opens a screen displaying the Reference Tree, Execution History, and Action Details for the selected Action.

**Web Services**—You can elect to *Deploy / Undeploy* or *Export WSDL* to create a web service from the selected Action.

*Deploy / Undeploy Web Service*—Deploy or undeploy the selected activity as a web service.

*Export WSDL*—This exports the WSDL for the selected activity. You must select the file name and location. Web Services Description Language (WSDL) is an XML format for the description of network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information.

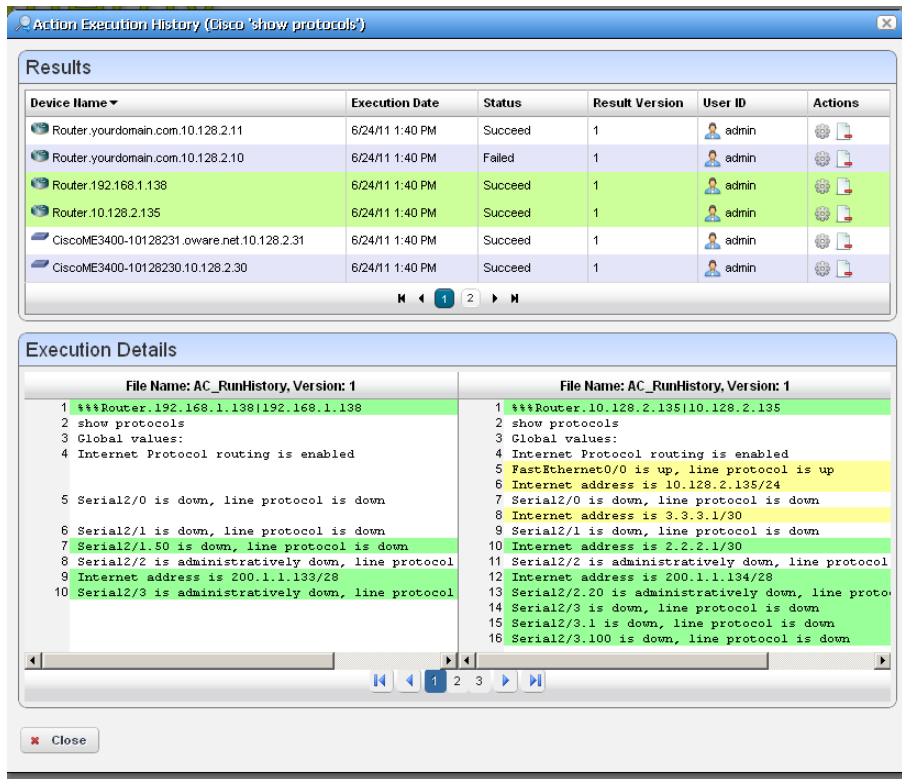
**History**—Displays the history of the selected action.



In the *Results* (top of screen panel) click to select the device for which you want additional information, and the *Execution Details* panel displays the *Results* of execution in one tab and the *Sent Commands* in another.

Notice that you can *Find* text within a result (click *Go* to repeat the find). You can also see the bottom panel if you right-click a single execution within the *Execution History* snap panel in the Expanded Actions Portlet.

If you select two executions in the top panel (or in the *Execution History* snap panel and right-click), a comparison appears.



This has the same color coding as you would see comparing configuration files. Lines that differ between the two Adaptive CLI results appear highlighted green. Lines that are missing in one, but that appear in another appear highlighted red. Added lines appear highlighted in yellow. Use the right/left arrows or the page numbers at the bottom of the screen to page through the side-by-side comparison.

**Audit**—Opens an Audit Trail Viewer for the selected Action. See Audit Trail Viewer on page 92 for details.

**Show Last Results**—Show the last execution details (like history for a single run).

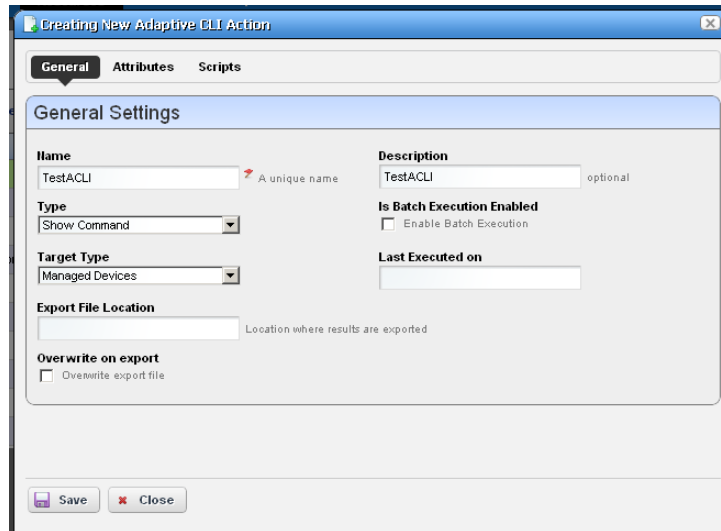
**Schedule**—Schedule the selected Action. See Scheduling Actions on page 369 for details.

**Delete**—Remove the selected Action from the list.

**Import / Export**—Import or Export a file representations of the ACLI action selected. Dell OpenManage Network Manager supports ACLI import / export only.

## Adaptive CLI Editor

This editor creates new Adaptive CLIs. When you click *New*, or *Edit* after selecting an existing command, the command editor screen opens. You can create *Configure Commands*, *External Commands*, and *Show Commands*.



The screenshot shows a window titled "Creating New Adaptive CLI Action". It has three tabs: "General", "Attributes", and "Scripts". The "General" tab is active, showing a "General Settings" section. This section contains several fields and checkboxes:

- Name:** A text box containing "TestACLI" with a red "X" icon and the text "A unique name".
- Description:** A text box containing "TestACLI" with the text "optional".
- Type:** A dropdown menu showing "Show Command".
- Target Type:** A dropdown menu showing "Managed Devices".
- Export File Location:** A text box with the text "Location where results are exported".
- Overwrite on export:** A checkbox labeled "Overwrite export file".
- Is Batch Execution Enabled:** A checkbox labeled "Enable Batch Execution".
- Last Executed on:** An empty text box.

At the bottom of the dialog are two buttons: "Save" and "Close".

The editor screen has the following tabs (the ones that appear depend on the type of command you are editing):

- General
- Attributes
- Scripts

### NOTE:

The Adaptive CLI Manager logs into devices in enable mode by default. For most configuration commands (and even some show commands), you must typically first set the device to its configuration mode.

### Tip

Dell OpenManage Network Manager validates entries. If saving fails, a red "X" appears next to required omitted entries.

Click *Save* to preserve the Adaptive CLI you have configured. Clicking *Close* does not save your configuration.

## General

The following are parameters to configure in this panel:

**Name**—A unique identifier for this action. For example: “Retrieve MyDevice MAC addresses.”

For a new action to appear on the right-click Action menu, begin its name with the vendor name. For example, *Force10-showversion* would appear under Actions in that menu. Otherwise, it appears under and Adaptive CLI classification.

**Description**—A text description of the action.

**Type**—Select a type from the pick list (*Configure*, *External* or *Show Command*).

### Tip

You can use Dell OpenManage Network Manager’s optional Proscan policies to scan Adaptive CLI show commands for compliance, and trigger actions (alarms, e-mail, and so on) based on their contents. See Chapter 9, Change Management – ProScan.

The *External* command refers to a script. Making this an ACLI means Dell OpenManage Network Manager can schedule such scripts or include them in a workflow. See External Commands on page 360 for more about these.

**Target Type**—Select a type of target from the pick list (*Card*, *Equipment and Subcomponents*, *Interfaces*, *Managed Devices*, *Ports*). Adaptive CLI targets can also be *None* (*Targetless*). On execution, if you create an Adaptive CLI type with port target, then the selection view panel lets you choose ports. When the Adaptive CLI type is *External* then Target Type can be *None*; otherwise it is not an option

**Export File Location**—This is a file name and path (C:\mypath\myfile) where you elect to store the result of an adaptive CLI execution. You may specify the variable *\$IPAddress* in the filename for pattern substitution.

**Overwrite on Export**—Check to overwrite the result file. This overwrites any existing results file with new results (if checked). If it is unchecked, the new results appends to the file.

**Is Batch Execution Enabled**—Check to allow consolidation of related Adaptive CLI scripts, provided the associated device driver supports such consolidation when provisioning a service.

Batching is valuable for instances like the following: if an Adaptive CLI-provisioned service has 10 sub-services, OpenManage Network Manager runs commands for the first service, then if it’s successful, commits, and logs off. Then OpenManage Network Manager repeats this procedure nine times more, logging on, committing and logging off for each command. If batching is turned on, then OpenManage Network Manager sends the 10 Adaptive CLIs to the device as a single unit before committing and logging off. (This logic does not apply if you are running a procedure against 10 devices.)

Batching is best practice, since if one line of a command fails, the device rolls back the entire block of commands. Cisco devices typically skip and do not commit failing lines.

**Last Executed On**—Displays the last execution date. This is blank for New Adaptive CLIs.

## Attributes

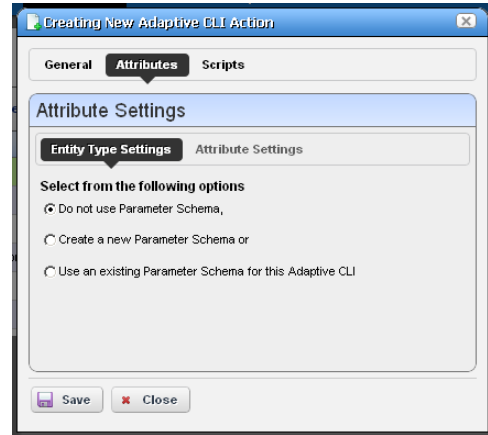
Adaptive CLI commands let you configure modifiable *Attributes* as part of the command you send to the selected equipment.

Use the radio buttons to select from the following options:

- Do not use Parameter Schema
- Create a new Parameter Schema
- Use an existing Parameter Schema for this Adaptive CLI

### Tip

Why share a schema rather than creating a new one with each Adaptive CLI? One reason is that creating an entity often requires a complementary script to remove it. In this case, the valid values, labels, and so on for the attributes are always going to be the same in both create and delete Adaptive CLIs; therefore, sharing the same schema is both safe and easy. Any delete script can mark unused attributes as “Not applicable.”



### Do not use Parameter Schema

This option does not save a set of standard attributes to re-use later. Go directly to the Scripts tab to create this type of Adaptive CLI.

### Create a new Parameter Schema

Click the *New* button and the schema screens appear.

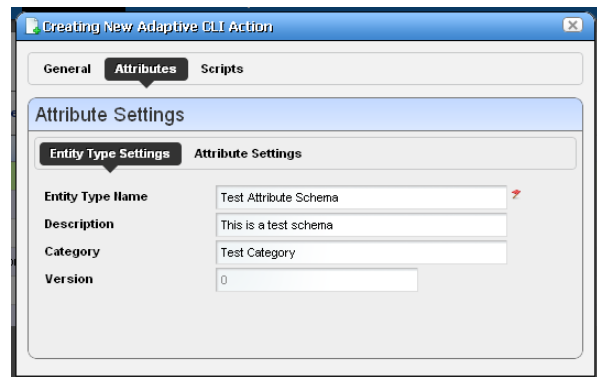
#### Entity Type Settings

The *Entity Type Settings* tab has the following fields:

**Entity Type Name**—An identifier for the schema.

**Description**—A text description for the schema.

**Category**—A category for the schema.



**Version**—An automatically-created version number.

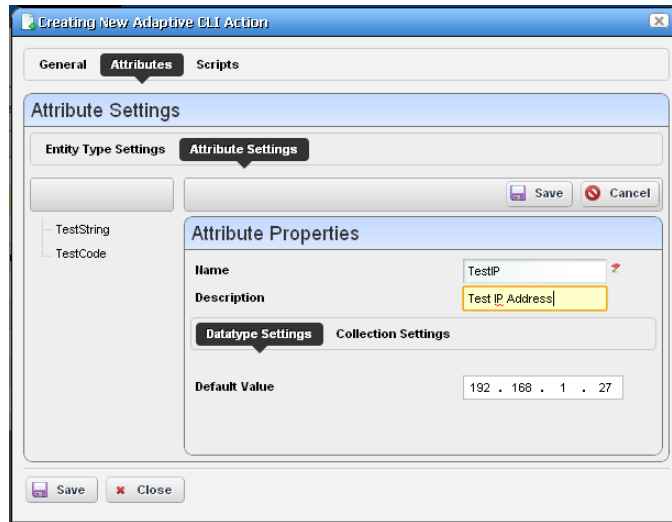
## Attribute Settings

Click the *New Attribute* button and select the attribute type and open editor panel and configure the attribute. Configured attributes appear in a tree to the left of the editor panel. Click a listed attribute to edit it after it has been created.

The editor panel has the following fields:

**Entity Type Name**—An identifier for the schema.

**Description**—A text description for the attribute.



The following tabs may appear, depending on the type of attribute you are configuring (some are absent). Additional fields may appear, depending on the attribute type you are configuring:

## Datatype Settings

**Default Value**—An optional default value for the attribute.

## Collection Settings

**Is Collection?**—Check to classify this attribute as a collection.

**Allow Duplicate Values**—Check to enable allowing duplicates.

**Allow Reordering**—Check to enable allowing reordering.

**Collection Min / Max Length**—Enter the minimum/maximum number of characters in this attribute.

## Properties

**Upper / Lower Case**—Check to validate on case.

**Case Insensitive**—Validation ignores case.

**Multi Line Text**—Check to enable multiline text.

**One Way Encrypt**—Check to encrypt.

**Truncate**—Truncate the attribute.

### Attribute Settings

You can create new attribute schemas. See Attribute Editor Panels below for information about different datatypes' fields. Once you create a set of attributes, they remain available for re-use as a schema, or collection of attributes. To identify schemas, enter the following fields:

**Label**—A unique, mandatory identifier for the collection of attributes.

**Description**—A text description of the entity.

Click *New* to create or select an attribute in the displayed tree and click *Edit* to open an editor where you can create or modify attributes. Select an attribute and click *Remove* to delete it from the list.

### Attribute Editor Panels

The following panels appears, depending on the attribute type selected from the pick list. The fields in the editor depend on this selection. Available types include *Boolean*, *Coded Value*, *Date*, *Decimal*, *IP Address*, *Integer*, *Long*, *Inventory Reference*, and *String*. The following fields appear for each of these types (omitting redundant fields):

#### NOTE:

Configure the data type of an attribute before you save a task. After attributes are in Scripts, you cannot change the data type.

### Boolean

**Default Value**—Check for *True*.

### Coded Value

**Default Coded Value**—Enter the default coded value. If an attribute a Coded Value then enter valid values in the format of NUMBER:Display Label. For example:

10:Hello World

20:Hello Moon

Without this pattern a validation error appears. Coded values become a Drop Down (Combo Selection) at runtime containing the Display labels within it (like Hello World, Hello Moon). Selecting one gives the script the numeric value (If users select Hello World, the value the script gets is 10)

The default appears by default in this list of alternatives. Enter any other alternatives below this field in the *Valid Values*.

**Valid Values**—Enter a valid value in the line above the table of valid values, then click the green + to add the value entered to the list. Click the *Remove* icon (the red -) to delete a selected value. These must be formatted like the *Default Coded Value*.



## Date

**Default Value**—Enter a default date, or use date icon to display a calendar where you can select one. Click off the calendar to make it disappear.

**Valid Values**—Enter valid date values above the list, and click the green plus to add them to the list.

## Decimal

**Default Value**—Enter a single or range of default decimal values.

**Constraints**—Enter a range of acceptable numbers separated by a colon. For example, Constraints = 2:4096. At runtime, a field where you can enter numbers. validates that entered numbers are between 2 and 4096 when running the Adaptive CLI. If you enter a number outside this range, a validation message appears and the attribute name turns red. You can also include several numbers or ranges separated by the pipe (|) character. If you specify a range, the lowest number must be to the left of the highest number. For example 9:99|999:1010.

**Valid Values**—Enter valid decimal range values, and click the green + (the red - removes them). You can manage these as described in Coded Value above.

## IP Address

See also Validating IP Address Variables on page 354.

**Default Value**—Enter a default IP Address.

**Valid Values**—Enter valid values as described in Coded Value above. Check *IP Mask*, *Subnet*, *Allow 32 Bit Mask*, and *Allow Any Valid Ip* in the *Properties* tab if you want the values entered to be those.

**Editable Valid Values**—Check to enable editing of default or entered IP addresses.

## Integer

**Default Value**—Enter a default integer.

**Constraints**—Enter a range of acceptable numbers separated by a colon. You can also include several numbers or ranges separated by the pipe (|) character. If you specify a range, the lowest number must be to the left of the highest number. For example 9:99|999:1010.

**Valid Values**—Enter ranges of valid values as described in Decimal above.

**Editable Valid Values**—Check to enable editing of default or entered integer.

## Long

**Default Value**—Enter a default long.

**Constraints**—Enter a range of acceptable numbers separated by a colon. You can also include several numbers or ranges separated by the pipe (|) character. If you specify a range, the lowest number must be to the left of the highest number. For example 9:99|999:1010.

**Valid Values**—Enter ranges of valid values as described in Decimal above.

### **Inventory Reference**

Select the *Reference Type* entity with the list that appears when you click the green plus (+), then use the side-by-side widget's arrows to move available attributes from *Available* to *Selected*. You can change the *Reference Type* by deleting it with the red minus (-), then selecting a new type with the green plus.

### **String**

**Default String**—Enter a default string.

**Valid Values**—Enter valid values as described in Coded Value above.

**Editable Valid Values**—Check to enable editing valid values.

**Constraint**—Enter the regular expression constraints, if any, on the string attribute.

**Constraint Description**—Enter the message to appear if the regular expression constraints are not met.

**Min / Max Length**—Enter the minimum / maximum number of characters in a valid string.

Click *Apply* to accept your edits for the attribute, or *Cancel* to abandon them.

### **Use an existing Parameter Schema for this Adaptive CLI**

Select this, and a *Select Existing* button appears. Clicking this button opens a selector where you can select from previously-configured attribute schemas (collections of attributes) to use in the Adaptive CLI you are configuring.

### **Validating IP Address Variables**

Programatically, IP address attributes support four extended properties: `IP_MASK`, `SUBNET`, `ALLOW_32_BIT_MASK`, and `ALLOW_ANY_VALID_IP`. The state of the first two largely defines Dell OpenManage Network Manager's responses.

**IP\_MASK**—Determines whether Dell OpenManage Network Manager accepts an IP address OR a subnet/subnet mask. The value accepted is an IP address attribute when false, subnet/subnet mask when true.

**SUBNET**—This property determines whether a subnet value must be provided or not, and controls display of the subnet portion of the widget. Valid subnet values are 1-31.

By default, when both of the above are false, the attribute only accepts valid IPv4 addresses. For example: 10.10.10.4

If `IP_MASK` is false and `SUBNET` is true then Dell OpenManage Network Manager accepts any valid IP address with a subnet specified. The address must be an IP within the specified subnet. For example, 10.10.10.4/24 is a valid entry whereas 10.10.10.0/24 is invalid since it represents the subnet id, not an actual address within the subnet.

If `IP_MASK` is true and `SUBNET` is false, then OpenManage Network Manager accepts one of the 32 valid subnet masks. The widget displays pick list for user to choose from. For example 255.255.255.0

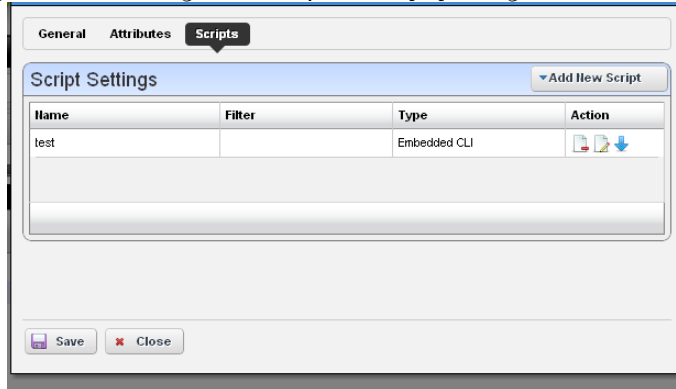
If `IP_MASK` is true and `SUBNET` is true, then OpenManage Network Manager accepts a subnet id (the first IP address within a subnet). For example 10.10.10.0/24, with 10.10.10.0 as the first address within the subnet spanning 10.10.10.0 to 10.10.10.254. Entering an IP address within the subnet, say 10.10.10.4/24, the attribute would convert that to 10.10.10.0/24

**ALLOW\_32\_BIT\_MASK**—Valid subnet values are between 1 and 31. To extend this to support a 32-bit subnet, which is essentially a single IP address (10.10.10.4/32), set the `ALLOW_32_BIT_MASK` property.

**ALLOW\_ANY\_VALID\_IP**—To accept either an IP address, IP address and subnet or subnet, then `IP_MASK` remains false, `SUBNET` is true. With the `ALLOW_ANY_VALID_IP` true, the subnet field is optional and OpenManage Network Manager disables any requirement that a subnet id be specified. Basically the only validation is that a valid IP address is entered. For example, in this configuration, 10.10.10.4, 10.10.10.4/24 and 10.10.10.0/24 would all be valid.

## Scripts

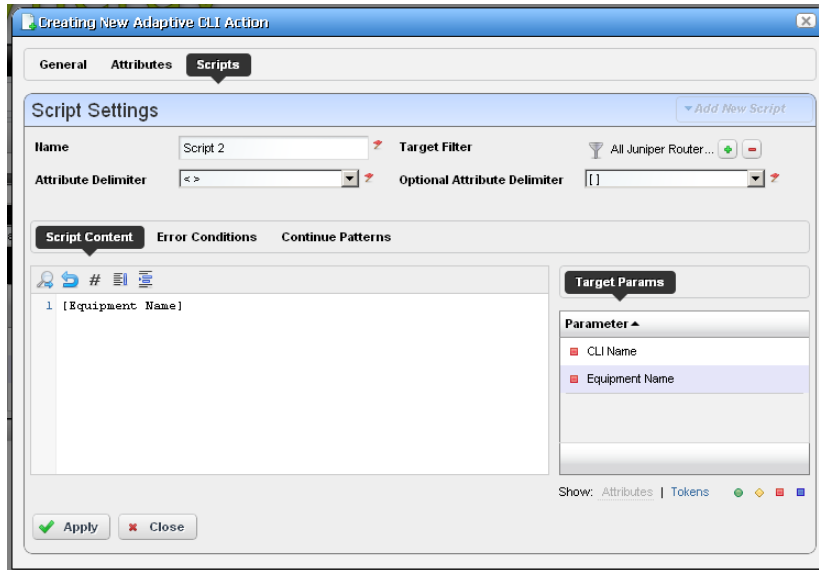
This screen manages the Adaptive CLI scripts created to query (show) devices or configure them. Dell OpenManage Network Manager runs only one script per target.



Notice you can order multiple scripts with the arrow(s) to the right of a listed script. Dell OpenManage Network Manager uses the first script's filter to match the target. In other words, suppose there are two scripts, the first with filter = target.type = SWITCH, and the second with no filter. Then only SWITCH devices run the first script and quit. All other devices will not run first script, but run the second script since that script has no filter.

## Script Settings

Click *Add New Script* to create a new item in those listed at the top of this screen, or select an item and click the *Edit* icon to its right to alter it. When you create a new script, you must select either *Embedded CLI* or *Perl*. Embedded CLI scripts are command-line interface (CLI) interactions. See Perl Scripts on page 368 for more about using Perl.



Clicking the *Delete* icon removes a selected item. Notice that the up/down buttons to the right of the list allow you to re-order selected items (they run from top first to bottom last).

See Attribute Appearance and Validation for a description of what constitutes a valid attribute.

**Name**—Enter an identifier for the script you are creating or altering.

**Target Filter**—Click the plus (+) to create a filter that describes the target for this script. For example, this filter could confine the action of the configured script to devices from a certain vendor, or only devices with an operating system version later than a certain number. Since you can have several scripts, those Adaptive CLIs with a single label (“Show Users,” for example) could therefore contain several scripts with syntax appropriate to a variety of devices and operating systems.

### ⚠ CAUTION:

Adaptive CLI supports only filters that select the Managed Equipment type of device.

**Attribute Delimiter**—The delimiter(s) you select from the pick list here surround the attributes you designate as mandatory. See Adaptive CLI Script Language Syntax on page 366 for more about these.

**Optional Attribute Delimiter**—The delimiter(s) you select from the pick list here surround the attributes you designate as optional. See Adaptive CLI Script Language Syntax on page 366 for more about these.

All but *Delete* open a script editor with the following panels:

- Script Content
- Error Conditions
- Continue Pattern
- Attributes Extraction

### Script Content

On the left, you can enter text, *Search* by clicking the magnifying glass, and use *Cut*, *Copy*, *Paste*, *Undo*, *Jump to Line #*, *reformat*. The *Attributes* appear under *Target Params* on the right of this text entry screen. Double-click an attribute to insert it unless you are writing a Perl script; this feature does not work for Perl. Right-click the previously-configured attributes in this panel to designate them as *Mandatory*, *Optional*, *Not Applicable* or *Non Configuration* in a context menu that appears when you right-click.

#### Tip

The *Non Configuration* attributes you select are not sent to the device with the script, but can serve to remind users of critical information. For example, you can make *Non Configuration* boolean attributes into a checklist for someone executing a script, and the history of this script records whether these checks were made when the script executed.

Notice that the *Search* also permits Regular expressions.

You can also enter two types of script language here. See Adaptive CLI Script Language Syntax on page 366 for a description of the internal *If* capabilities. If you need more elaborate scripting, you can also use Perl scripts to send text to devices. See *Perl Scripts on page 368* for a description of those capabilities.

## Error Conditions

The error condition lets you configure errors for your script.

The screenshot shows a web interface with three tabs: 'Script Content', 'Error Conditions', and 'Continue Patterns'. The 'Error Conditions' tab is active. It contains two error condition entries, each with a minus sign in a red circle to its left. Each entry has three fields: 'Error pattern' (text input), 'Error type' (dropdown menu), and 'Number of lines to check' (text input). The first entry has 'Test' in the pattern field, 'Error' in the type dropdown, and '100' in the lines field. The second entry has 'Test2' in the pattern field, 'Warning' in the type dropdown, and '40' in the lines field. At the bottom left of the panel is a button with a plus sign and the text 'Add new error condition'.

Click *Add new error conditions* to configure a condition at the bottom of this screen with the following fields:

**Error Pattern**—Enter a regular expression for the error.

**Error Type**—Select from the pick list of options (*Error*, *Warning*, *Ignore*).

**Number of lines to check**—Enter the number of lines of the script output to check for the pattern specified above, after each command execution. An error message is most likely to appear immediately right after the command is invoked.

## Continue Pattern

Like Error Conditions, this screen lets you enter conditions to which script execution can respond.

The Continue Pattern editor operates like the Error Conditions editor, but has slightly different fields.

**Continue Pattern**—If you expect the device output of a script to prompt to continue, you may add a *Continue Pattern* with a regular expression to parse.

**Answer**—This field specifies the *Answer* to the *Continue Pattern* prompt.

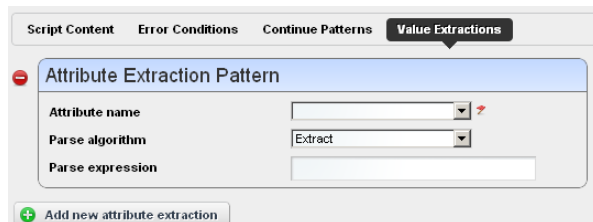
**Send New Line**—For some devices, a single key response without a new line would be sufficient; in such cases, you may need to uncheck the *Send New Line* option.

**Max Occurrences**—Indicates the maximum number of times respond to a prompt. The default value zero (0) indicates no limit.

The screenshot shows a web interface with three tabs: 'Script Content', 'Error Conditions', and 'Continue Patterns'. The 'Continue Patterns' tab is active. It contains one continue pattern entry, which has a minus sign in a red circle to its left. The entry has four fields: 'Continue pattern' (text input), 'Answer' (text input), 'Send new line' (checkbox), and 'Max occurrences' (text input). The 'Continue pattern' field is empty, the 'Answer' field is empty, the 'Send new line' checkbox is unchecked, and the 'Max occurrences' field contains '0'. At the bottom left of the panel is a button with a plus sign and the text 'Add new continue pattern'.

## Attributes Extraction

To support Adaptive Service and Active Monitor functions, Adaptive CLI provides a way for the user to define output schema attributes. This tab is active only if you have selected schema attributes previously in the Attributes portion of this editor.



This lets you *Add*, *Edit* or *Delete* extracted attributes, like Error Conditions’s editor, and configure them with the following fields:

**Attribute Name**—This field specifies the name of the extracted attribute. To specify the output value of an attribute, select it from the provided list.

**Attribute Type**—The data type of the attribute extracted. Only schema attributes of simple type String, Integer, Long, Float, Double, and Boolean are available to choose from.

**Parse Algorithm**—Select from the pick list (*Extract*, *Match*). For match algorithm, the result is either *true* or *false* for the Boolean attribute type, 0 or 1 for numeric types, or “*true*” or “*false*” for String type.



### NOTE:

Currently, Active Performance Monitor supports only numeric types.

**Parse Expression**—Enter a regular expression for Parse Expression and the Parse Algorithm (Extract or Match) used when evaluating the device output on a given script execution.

Click *Apply* to accept your edits, or *Cancel* to abandon them. Click *Add new attribute extraction* to add more such patterns to your script.

## Attribute Appearance and Validation

Invalid schema attribute names appear in the script in red italics. This indicates that you cannot use such attributes in the script.

Valid attribute names contain alphanumeric characters and underscore (\_). They must begin with either an underscore or a letter [A-Za-z].

All blank space characters in the schema attribute name are converted to underscore (\_) by default.

A schema attribute name that is invalid in Adaptive CLI may still be valid in other entities, so you can specify them in the schema but they are not usable by Adaptive CLI.

Click *Apply* to accept your edits for the script, or *Cancel* to abandon them.

## Comparison

Selecting (ctrl+clicking) two Adaptive CLI runs within the *Execution History* portlet lets you compare the two execution results. Right-click and select *Compare*.

Lines that differ between the two configurations appear highlighted green. Lines that are missing in one, but that appear in another appear highlighted red. Added lines appear highlighted in yellow. Use the right/left arrows at the bottom of this screen to page through the side-by-side comparison.

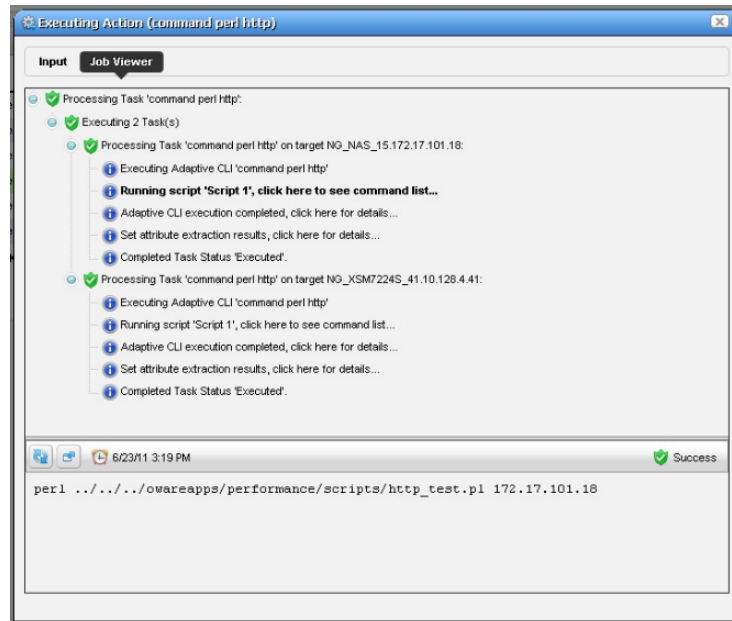
## External Commands

External commands are essentially scripts that run in the Dell OpenManage Network Manager environment. For example, you could run the DOS `dir` command (and schedule its execution).

You can execute external commands with a device as target, using device attributes as input parameters to the Adaptive CLI script. See some of the Seeded Scripts on page 362.

### Audit Trail

When you execute a script, the audit screen displays information about it.





## Results

Dell OpenManage Network Manager stores the results of running a script as lines the Execution Details snap panel. Right click the particular command run in the snap panel at the bottom of the Expanded Actions Portlet. Tabs show the Results, Sent Command, and Script and Parameters. When viewing a script run the results of running it appear target device-by-device.

The screenshot shows the 'Action Execution History (command per http)' window. The 'Results' section contains a table with the following data:

Device Name	Execution Date	Status	Result Version	User ID	Actions
NG_XSM7224S_41.10.128.4.41	6/23/11 3:19 PM	Succeed	6	admin	[Icons]
NG_NAS_15.172.17.101.18	6/23/11 3:19 PM	Succeed	2	admin	[Icons]
NG_XSM7224S_41.10.128.4.41	6/23/11 1:30 PM	Succeed	5	admin	[Icons]
NG_NAS_15.172.17.101.18	6/23/11 1:30 PM	Succeed	1	admin	[Icons]
NG_GSM7352Sv2_30.10.128.4.30	6/23/11 1:30 PM	Succeed	2	admin	[Icons]
NG_GSM7246V2_24.10.128.4.24	6/23/11 1:30 PM	Succeed	1	admin	[Icons]

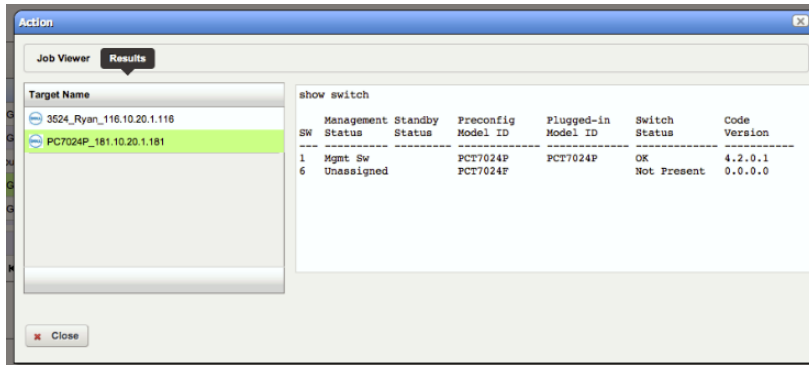
The 'Execution Details' section has tabs for 'Results', 'Sent Commands', and 'Script and Parameters'. The 'Results' tab is active, showing a search bar and a list of execution details. The details include a list of lines (1-19) and a table of parameters:

```
# Find: [ ] Go [ ]
1 ***NG_XSM7224S_41.10.128.4.41|10.128.4.41
2 (0) OK
3 HTTP/1.1 200 OK
4 Server: Web Server
5 Content-Type: text/html
6 Cache-Control: no-cache
7 Pragma: no-cache
8
9
10 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN
11 <html>
12
13 <HEAD>
14 <LINK REL=stylesheet HREF="/base/style.css" TYPE="text/cs:
15 <META http-equiv="Pragma" content="no-cache">
16 <META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=
17 <TITLE>NetGear XSM7224S</TITLE> <!-- Netgear Page Ti
18
19
```

Parameter Name | Value  
Result | 0

Close

Results can also appear in the audit screen messages and in the Results panel of the Action job viewer screen.



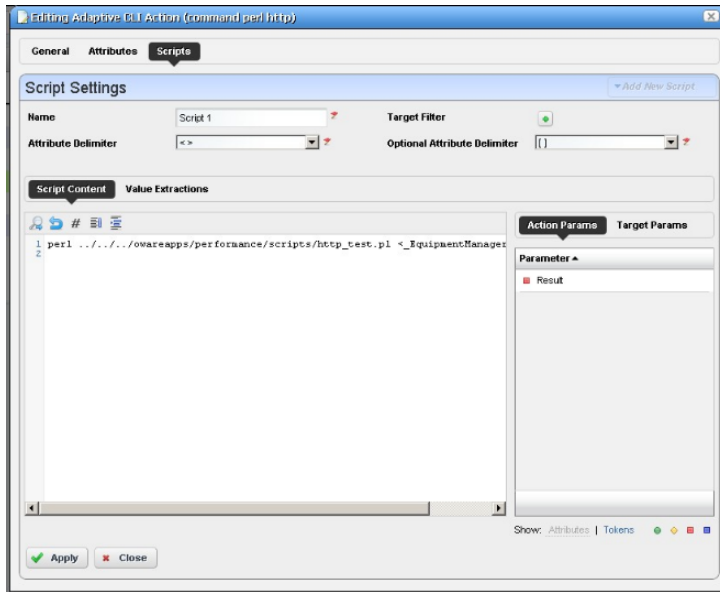
You can also extract parameters for these external commands as is described in Attributes Extraction on page 359.

## Seeded Scripts

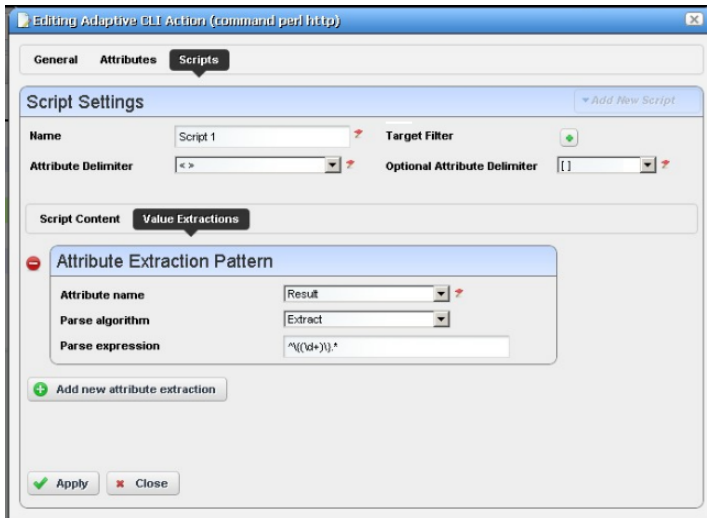
Several external perl scripts come with Dell OpenManage Network Manager as examples of the kind of commands you can execute. These are in `\owareapps\performance\scripts` under the installation root.

To run these, the scripts panel in the Adaptive CLI editor should contain something like the following:

```
perl ../../../../owareapps/performance/scripts/http_test.pl
```



Notice that these also include a parameter (*Result*) that contains values extracted.



Set up attribute extraction in the *Values Extraction* tab of the script editor.

### Script Names and Functions

`common.pl`—Common functions defined for scripts in this directory.

- `dns_test.pl`—Check if DNS can resolve the specified host name.
- `finger_test.pl`—Check if the finger service is running on a specified host.
- `ftp_test.pl`—Check the FTP service is running on a specified host.
- `http_test.pl`—Check the HTTP service is running on a specified host.
- `nnntp_test.pl`—Check if the NNTP service is running on a specified host. (Public NNTP server to test: news.aioe.org)
- `peping_test.pl`—Check if a target is pingable from the specified remote host.
- `pop3_test.pl`—Check if the POP3 service is running on a specified host.
- `smtp_test.pl`—Check if the SMTP service is running on a specified host.
- `telnet_test.pl`—Check if the TELNET service is running on a specified host.



## How To:

### Create a Monitor for an External Script

The following steps describe creating a monitor for an external command configured as an Adaptive CLI (ACLI).

#### Create the Adaptive CLI

- 1 Right click in the Actions portlet, and create a new *External Command* ACLI
- 2 Make a new attribute schema with attribute: Status (integer)
- 3 In Scripts, enter the following as Script Content:

```
perl
  "C:\Dorado\owareapps\performance\scripts\http_test.pl" [_EquipmentManage
  r_IP_Address]
```



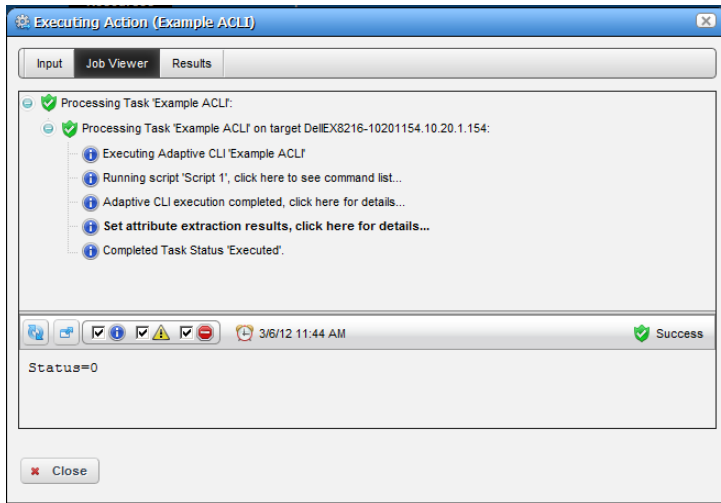
#### Tip

Several Perl scripts appear in this performance\scripts directory by default. You can try others in addition to the `http_test.pl` script.

- 4 In the Value Extraction panel enter the following:
 

```
^\{(\d+)\}.*
```
- 5 Click Apply
- 6 Click Save
- 7 Right click and *Execute* the ACLI to test it.

- 8 Look in Job Viewer for the results.




Click *Set attribute extraction results, click here* to see the results appear in the bottom panel. Notice also that you must check informational messages for all these to appear, and that several additional sets of messages besides the extraction results appear.

### Create a Monitor for the External Script Adaptive ACLI

Now that you have verified the script is working, you can create a monitor to see how this attribute is doing.

- 1 In the Monitors portlet, create a new ACLI Monitor
- 2 Uncheck *Update Network Status* (recommended since the ICMP monitor is already doing this)
- 3 In *Monitor Options* select your example monitor configured previously.
- 4 Confirm that *Monitor Attributes* displays the Status attribute configured previously.
- 5 In the *Conditions* tab of the Monitor Editor, create “Status Up” condition, with the severity of *Informational*, and check *Alert*.
- 6 Create a criterion which is  $Status = 0$ .
- 7 Save this condition
- 8 Create a new Condition called “Status Down”
- 9 The criterion is  $Status = 1$
- 10 Apply and Save

11 Save your monitor

 **NOTE:**

You may want to test your monitor, in which case, you may want to change the interval to 30 seconds.

12 Right-click to select *View Monitor Data*, and you can see the results of your efforts.

View Data for Monitor: Example ACLI Monitor [Return to previous](#)

Monitor Target	Polled Date/Time
● erx310-0.211.192.168.0.211	4/25/12 1:18 PM
● Router.yourdomain.com.10.128.2.11	4/25/12 1:18 PM
● Router.192.168.1.138	4/25/12 1:18 PM
● JuniperM5-10.128.3.15.10.128.3.15	4/25/12 1:18 PM
● DellSRX650.10.20.1.167	4/25/12 1:18 PM
● 6224_kinnick_73.10.20.1.73	4/25/12 1:18 PM
● DellSRX220h_166.10.20.1.166	4/25/12 1:18 PM
● CiscoME3400-10126231.oware.net.10.128.2.31	4/25/12 1:18 PM
● ciscoAD2435.10.128.2.50	4/25/12 1:18 PM
● erx310-0.211.192.168.0.211	4/25/12 1:10 PM
● Router.yourdomain.com.10.128.2.11	4/25/12 1:10 PM
● Router.192.168.1.138	4/25/12 1:10 PM
● JuniperM5-10.128.3.15.10.128.3.15	4/25/12 1:10 PM
● DellSRX650.10.20.1.167	4/25/12 1:10 PM

## Adaptive CLI Script Language Syntax

Here's the Adaptive CLI scripting language syntax:

- CLI script is a line-based syntax. In other words, each line's syntax has to be completed.
- CLI script supports primarily two features: Attributes and Conditional Blocks.

### Attributes

Each attribute in the script is marked by a delimiter. The following delimiters are supported:

<> [] {} () \$ % @ #

Think of Attribute delimiters as a pair of open/close markers surrounding a variable name. For single character Attribute delimiters, there is no closing marker (the close marker is empty).

Examples of Attributes are:

<var>, [var], {var}, (var), \$var, %var, #var, @var

The default mandatory delimiters are <>, and the default optional delimiters are [], but you can change those default settings. That means an Attribute variable like <var> may represent a mandatory or an optional Attribute depending on what are set as delimiters.

 **NOTE:**

Single delimiter symbols require a space after the attribute. These do allow values immediately before the symbol. Perl requires a space after the attribute, or the attribute's closing delimiter, but values immediately before single delimiters works.

Here is an example of a command line with a mandatory and optional Attribute:

```
show <mandatory> [optional]
```

If you set the <mandatory> Attribute to *interface* and do not set the [optional] one, then the resulting command would be this:

```
show interface
```

If you set the <mandatory> Attribute to *interface* and set [optional] to *brief* then the resulting command would be:

```
show interface brief
```

## Conditional Blocks

Every line in the script is presumably a command to be sent to the device, except for lines that denote either a beginning or ending of a conditional block.

The begin conditional block marker is tied to a Attribute and has the following syntax:

```
<optional-open-delimiter> IF optional-attribute <optional-close-delimiter>
```

The end conditional block marker has the following syntax:

```
<optional-open-delimiter> ENDIF optional-text < optional-close-delimiter>
```

Here is an example of a conditional block, where the Attribute delimiters are <>, optional delimiter is [], and the conditional Attribute variable is `set`:

```
[IF set]
    execute this command
    and execute this command
[ENDIF set]
```

If the Attribute `set` has a value then the block is evaluated; otherwise, it is ignored. The text after `ENDIF`, that is `set` or whatever is not required and it is ignored.

Nested conditional blocks are allowed.

# Perl Scripts

This section describes the details of using Perl scripts within Adaptive CLI. See Using Perl in Adaptive CLI on page 342 for more about why to use Perl.

The Perl output goes to the selected target device. Typically, this means creating lines like the following:

```
println("show $param");
```

or

```
print("show $param\n");
```

You must specify parameters within the script (like `$param`) in the screen described in Attributes on page 350. Unlike its internal scripts, Adaptive CLI does not automatically create attributes. You must also manually configure created attributes to be *Mandatory*, or *Optional* in that screen.

A few things to remember when using Perl:

- The normal output of your Perl scripts (to stdout) are the commands sent to a device by this application.
- If your script produces an error message (to stderr), the job fails with that message and all script outputs are ignored. You can validate a script before sending any command to the device by using `die(...)` and `warn(...)` functions in Perl to produce error messages to stderr. Such messages trigger the script's failure.
- For such scripts to operate correctly, you must have Perl installed on the directory path for all OpenManage Network Manager servers.
- Perl does not come with OpenManage Network Manager and must be installed on the server system independently for it to work with Adaptive CLI.
- You can install your version of Perl and set the `PATH` environment variable accordingly so that one can run `perl -v` from the command line (where the OpenManage Network Manager server is to be started). Adaptive CLI invokes that same `perl` command.

If for some reason Adaptive CLI, fails to invoke the default `perl` command, it reads the setting of `activeconfig.perl.exe=...` inside `owareapps/activeconfig/lib/ac.properties`, and uses that alternative command.

Note that the default `activeconfig.perl.prefix=` setting in `ac.properties` is prepended to every Perl script. It basically forces the script to use `strict` mode and provides a convenient `println` method for the user. Knowledgeable Perl users can change this default behavior setting but should be careful about it. Remember, best practice is to override properties as described in Overriding Properties on page 23.

- The standard output (using `println`) of the Adaptive CLI Perl script represents the command set that is to be sent to the device. For convenience, a `println` subroutine is embedded with the script.





## How To:

### Create Adaptive CLI Example

The following describes the basics of creating and using Adaptive CLIs.

- 1 Create a new Adaptive CLI. Right-click and select *New*.
- 2 In the *Attributes* panel, create attributes named *required* and *optional*.
- 3 In the *Script* panel define the Attribute Delimiter (< >) and Optional Attributes Delimiter ([ ]) and enter the following three scripts:  

```
show run  
show <Required>  
show [Optional]
```
- 4 Save this Adaptive CLI execute it with *action > Execute*.
- 5 When executing, select a target.
- 6 Click *Next*. The Show Run command results appear. These are searchable with the job screen.

## Scheduling Actions

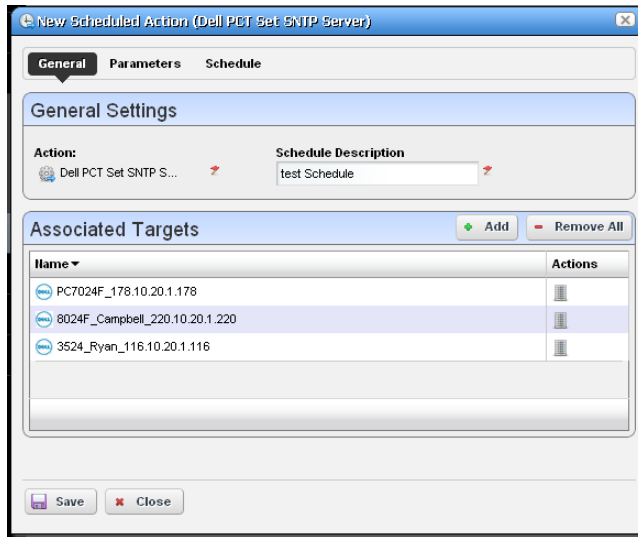
You can schedule actions with a right-click in the Actions Portlet or the Schedules Portlet. This opens an editor with the following screens:

- General
- Parameters
- Schedule

See Schedules Portlet on page 95 for more scheduling actions with that portlet. Schedules created in the Actions Portlet also appear in the Schedules Portlet.

## General

This screen lets you identify the scheduled item and its targets.



This has the following fields:

### General Settings

**Action**—Identifies the action being scheduled.

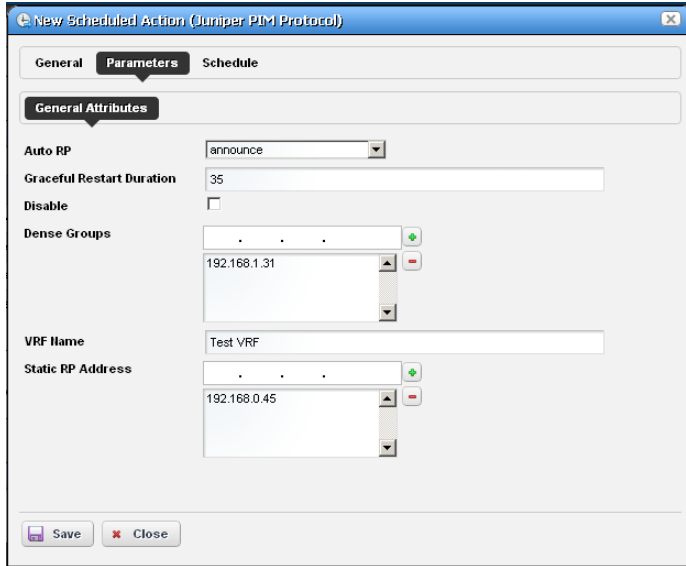
**Schedule Description**—Identifies the schedule.

### Associated Targets

Click the *Add* button to select target equipment. You can remove listed equipment with the icon to the right of listed items or with the *Remove All* button.

## Parameters

This screen's configuration depends on the selected action you are scheduling. Many actions have no parameters, so this tab is disabled. Enter the parameters for the action you are scheduling.



The screenshot shows a dialog box titled "New Scheduled Action (Juniper PIM Protocol)" with three tabs: "General", "Parameters", and "Schedule". The "Parameters" tab is active. Under the "General Attributes" sub-tab, the following fields are visible:

- Auto RP:** A dropdown menu set to "announce".
- Graceful Restart Duration:** A text input field containing "35".
- Disable:** A checkbox that is currently unchecked.
- Dense Groups:** A list box containing "192.168.1.31". Above the list is a text input field with three dots, and to the right are a green plus icon and a red minus icon.
- VRF Name:** A text input field containing "Test VRF".
- Static RP Address:** A list box containing "192.168.0.45". Above the list is a text input field with three dots, and to the right are a green plus icon and a red minus icon.

At the bottom of the dialog are "Save" and "Close" buttons.

### Tip

Hover the cursor over fields to make their description appear in a tooltip.

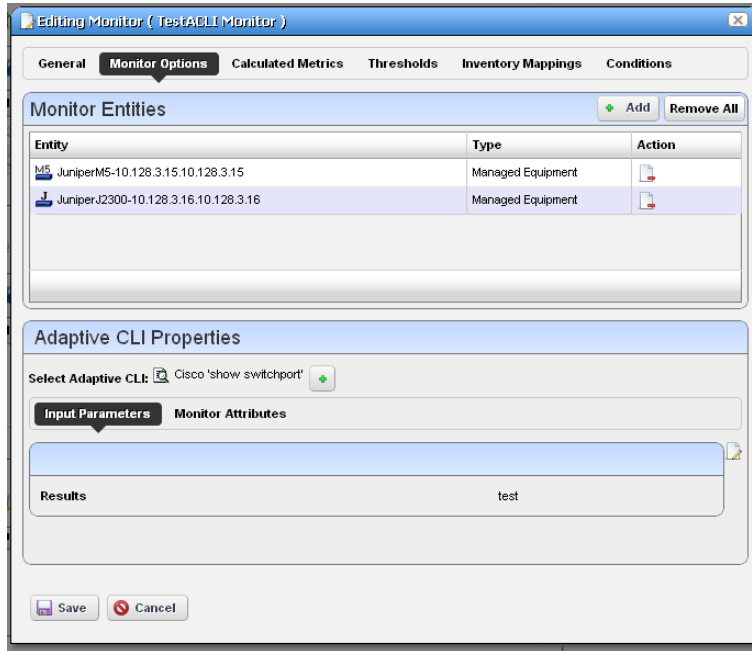
## Schedule

This screen is a standard scheduler screen, as described in Schedules on page 95.

# Active Performance Monitor Support

You can monitor Adaptive CLI execution results with Active Performance Monitor. To do this, you must select Adaptive CLI as the monitored type when creating a new performance monitor (see Resource Monitors on page 245), then select a target entities (with the *Add* button in the top

panel) and a particular Adaptive CLI (with the green plus [+]) in the Adaptive CLI Properties panel at the bottom of this screen. Click the *Edit* (page) icon to select the *Input Parameters* to monitor once you have selected an Adaptive CLI.



The user can choose an Adaptive CLI to monitor and may have to configure both its input values and metric type for each output attribute. The Input data depends on what is configured in the Adaptive CLI attributes.

### Input Parameters

In Active Monitoring, all attributes of the schema appear in the *Input Data* for user-entered values. You must enter the data necessary for all selected targets' scripts. To enter data, click *Edit* and then enter values. Clicking *Apply* switches the panel back to read-only mode.

#### NOTE:

You must click Save to preserve input or output data configurations.

## Monitor Attributes

Configure Adaptive CLI output attributes for monitoring in this tab in the lower panel of the Monitor Editor screen. You can monitor only exposed attributes of numeric or boolean types. To change metric type, select the row and click the *Edit* button to its right.



The screenshot shows a dialog box titled "Active CLI Properties". It has four rows of configuration options: "Attribute Name" with a text input field containing "Show-Results"; "Attribute Type" with a dropdown menu showing "String"; "Enabled" with an unchecked checkbox; and "Metric Type" with a dropdown menu showing "Gauge". At the bottom of the dialog are two buttons: "Save" (with a floppy disk icon) and "Cancel" (with a red X icon).

An Adaptive CLI Properties screen appears that reminds you of the *Attribute Name*, and *Attribute Type*, where you can *Enable* the attribute monitoring, and select *Gauge*, *Counter* or *Boolean* buttons to the right of this panel to configure the metric type of the selected output data.

These attributes default to the metric type *Gauge*. Adaptive CLI is where you define these attributes, but you must select their metric type settings on this screen if it is something other than the default.

Click *Save* to preserve your configuration, or *Cancel* to abandon it and close the editor screen.

## Adaptive CLI Records Archiving Policy

You can use OpenManage Network Manager's archiving feature to preserve Adaptive CLI information. Click the Redcell > Database Archiving Policy (DAP) node of the Control panel, and click the default *Adaptive CLI DAP* and click the edit button on its right.



The screenshot shows a dialog box titled "Editing Adaptive CLI Aging Policy". It has two tabs: "General" and "Options", with "Options" selected. Under "Options", there are three settings: "Keep History for this many days" with a text input field containing "30"; "Delete history associated with Negate command" with an unchecked checkbox; and "Archive deleted records" with a checked checkbox. At the bottom are two buttons: "Apply" (with a green checkmark icon) and "Cancel" (with a red X icon).

After filling in the *General Info* tab, the *Parameters* screen lets you configure the following:

**Keep History**—Enter the number of days to retain the history in the database.

**Delete history associated with Negate command**—Check to remove archived records associated with *Negate* (described under *General* on page 349).

**Archive Deleted Records**—Check to have deleted archived records saved as a file (configured in the *General Info* parameters too).



# Glossary

**ACCESS CONTROL** — Refers to mechanisms and policies that restrict access to computer resources. An access control list (ACL), for example, specifies what operations different users can perform on specific files and directories.

**ALARM** — A signal alerting the user to an error or fault. Alarms are produced by events. Alarms produce a message within the Alarm Window.

**API** — Application Programming Interface—A set of routines used by the application to direct the performance of procedures by the computer's operating system.

**AUTHENTICATION** — The process of determining the identity of a user that is attempting to access a network. Authentication occurs through challenge/response, time-based code sequences or other techniques. See CHAP and PAP.

**AUTHORIZATION** — The process of determining what types of activities or access are permitted on a network. Usually used in the context of authentication: once you have authenticated a user, they may be authorized to have access to a specific service.

**COS** — Class of Service—Describes the level of service provided to a user. Also provides a way of managing traffic in a network by grouping similar types of traffic.

**DATABASE** — An organized collection of Oware objects.

**DEPLOYMENT** — The distribution of solution blades throughout the domain.

**DIGITAL CERTIFICATE** — A digital certificate is an electronic “credit card” that establishes your credentials when doing business or other transactions on the Web. It is issued by a certification authority (CA). It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting and decrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real.

**DOMAIN** — A goal-oriented environment that can include an industry, company, or department. You can use Oware to create solutions within your particular domain.

**ENCRYPTION** — Scrambling data in such a way that it can only be unscrambled through the application of the correct cryptographic key.

**EQUIPMENT** — A network device managed by the system.

**ETHERNET TRUNK** — An Ethernet Trunk service represents a point-to-point connection between two ports of two devices. Ethernet frames transported by the connection are encapsulated according to IEEE 802.1Q protocol. The each tag ID value in 802.1Q encapsulated Ethernet frames distinguishes an Ethernet traffic flow. Thus, an Ethernet trunk can aggregate multiple Ethernet VLANs through a same connection which is why “trunk” describes these.

**ETHERNET TRUNK PORT** — An Ethernet trunk port is a port that terminates a point-to-point Ethernet trunk. Since Ethernet trunk is a point-to-point connection, each Ethernet trunk contains two Ethernet trunk ports.

**ETHERNET SERVICE** — An Ethernet service represents a virtual layer broadcast domain that transports or transmits Ethernet traffic entering from any one endpoint to all other endpoints.

Often, this is a VLAN service across multiple devices.

An Ethernet service may or may not use Ethernet trunk, depending on the desired connection between two neighboring devices. If the connection is exclusively used for this Ethernet service, no Ethernet trunk is needed. On the other hand, if the connection is configured as an aggregation which can be shared by multiple Ethernet services, an Ethernet trunk models such a configuration.

Each Ethernet service can have multiple Ethernet Access Ports through which Ethernet traffic flows get access to the service.

**ETHERNET ACCESS SERVICE** — Since an Ethernet trunk can be shared by multiple Ethernet Services, each Ethernet Service relates to a shared trunk via a unique Ethernet Access component.

Because Ethernet trunk is a point-to-point connection, there are two Ethernet Access Services per trunk per Ethernet service instance.

**ETHERNET ACCESS POINT** — These represent the access points through which Ethernet frames flow in and out of an Ethernet service.

For an Ethernet Service that uses an Ethernet Trunk Service, an Ethernet Access Port must be associated with either one of the two Ethernet Access Services.

**EVENT** — Notification received from the NMS (Network Management System). Notifications may originate from the traps of network devices or may indicate an occurrence such as the closing of a form. Events have the potential of becoming alarms.

**EVENT DEFINITION** — Parameters that define what an event does. For example, you can tell Oware that the event should be to wait for incoming data from a remote database, then have the Oware application perform a certain action after it receives the data.

**EVENT INSTANCE** — A notification sent between two Oware components. An event instance is the action the event performs per the event definition.

**EVENT TEMPLATE** — Defines how an event is going to be handled.

**EVENT THRESHOLD** — Number of events within a given tomfooleries that must occur before an alarm is raised.

**EXPORTING** — Saving business objects, packages, or solution blades to a file for others to import.



**FILTER** — In network security, a filter is a program or section of code that is designed to examine each input or output request for certain qualifying criteria and then process or forward it accordingly.

**GUI** — Graphical User Interface

**ISATAP** — The Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) is an IPv6 transition mechanism which is defined as a tunneling IPv6 interface and is meant to transmit IPv6 packets between dual-stack nodes on top of an IPv4 network.

**KEY** — In cryptography, a key is a variable value that is applied using an algorithm to a string or block of unencrypted text to produce encrypted text. The length of the key generally determines how difficult it will be to decrypt the text in a given message.

**KEY MANAGEMENT** — The establishment and enforcement of message encryption and authentication procedures, in order to provide privacy-enhanced mail (PEM) services for electronic mail transfer over the Internet.

**MANAGED OBJECT** — A network device managed by the system.

**MEDIATION** — Communication between this application and external systems or devices, for example, printers. Mediation services let this application treat these devices as objects.

**MEDIATION AGENT** — Any communication to and from equipment is handled by the Mediation Agent. This communication includes SNMP requests, ASCII requests, and unsolicited ASCII messages. In addition, the Mediation Agent receives and translates emitted SNMP traps and converts them into events.

**MEG** — Maintenance Entity Group

**MEP** — Maintenance End Point

**MIB** — Management Information Base. A database (repository) of equipment containing object characteristics and parameters that can be monitored by the network management system.

**OAM** — Operation, Administration and Maintenance

**OID** — Object ID.

**OSPF** — Open Shortest Path First routing protocol.

**POLICY** — A rule made up of conditions and actions and associated with a profile. Policy objects contain business rules for performing configuration changes in the network for controlling Quality of Service and Access to network resources. Policy can be extended to perform other configuration functions, including routing behavior, VLAN membership, and VPN security.

**POLICY ENFORCEMENT POINTS (PEP)** — In a policy enforced network, a policy enforcement point represents a security appliance used to protect one or more endpoints. PEPs are also points for monitoring the health and status of a network. PEPs are generally members of a policy group.

**POLICY ROUTING** — Routing scheme that forwards packets to specific interfaces based on user-configured policies. Such policies might specify that traffic sent from a particular network should be routed through interface, while all other traffic should be routed through another interface.

**POLICY RULES** — In a policy enforced network (PEN), policy rules determine how the members and endpoint groups of a policy group communicate.

**PPTP (POINT-TO-POINT TUNNELING PROTOCOL)** — Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables the secure transfer of data from a remote client to a private enterprise server by creating a virtual private network (VPN) across TCP/IP-based data networks. PPTP supports on-demand, multi-protocol, virtual private networking over public networks, such as the Internet.

**PRIVATE KEY** — In cryptography, a private or secret key is an encryption/decryption key known only to the party or parties that exchange secret messages. In traditional secret key cryptography, a key would be shared by the communicators so that each could encrypt and decrypt messages. The risk in this system is that if either party loses the key or it is stolen, the system is broken. A more recent alternative is to use a combination of public and private keys. In this system, a public key is used together with a private key.

**PROFILE** — A profile is an abstract collection of configuration data that is utilized as a template to specify configuration parameters to be applied to a device as a result of a policy condition being true.

**PUBLIC KEY** — A public key is a value provided by some designated authority as a key that, combined with a private key derived from the public key, can be used to effectively encrypt and decrypt messages and digital signatures. The use of combined public and private keys is known as asymmetric encryption. A system for using public keys is called a public key infrastructure (PKI).

**QoS** — Quality of Service. In digital circuits, it is a measure of specific error conditions as compared with a standard. The establishment of QoS levels means that transmission rates, error rates, and other characteristics can be measured, improved, and, to some extent, guaranteed in advance. Often related to Class of Service (CoS).

**RADIUS** — RADIUS (Remote Authentication Dial-In User Service) is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share.

**RIP** — Routing Information Protocol

#### **SELF-SIGNED CERTIFICATE**

A self-signed certificate uses its own certificate request as a signature rather than the signature of a CA. A self-signed certificate will not provide the same functionality as a CA-signed certificate. A self-signed certificate will not be automatically recognized by users' browsers,

and a self-signed certificate does not provide any guarantee concerning the identity of the organization that is providing the website.

**SMTP** — Simple Mail Transfer Protocol.

**SNMP** — Simple Network Management Protocol. Network management protocol used almost exclusively in TCP/IP networks. SNMP provides the means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

**SPANNING TREE PROTOCOL (STP)** — The inactivation of links between networks so that information packets are channeled along one route and will not search endlessly for a destination.

**SSH (SECURE SHELL)** — A protocol which permits secure remote access over a network from one computer to another. SSH negotiates and establishes an encrypted connection between an SSH client and an SSH server.

**SSL (SECURE SOCKETS LAYER)** — A program layer created by Netscape for managing the security of message transmissions in a network. Netscape's idea is that the programming for keeping your messages confidential ought to be contained in a program layer between an application (such as your Web browser or HTTP) and the Internet's TCP/IP layers. The “sockets” part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer.

**TRAP (SNMP TRAP)** — A notification from a network element or device of its status, such as a server startup. This notification is sent by an SNMP agent to a Network Management System (NMS) where it is translated into an event by the Mediation Agent.

**TRAP FORWARDING** — The process of re-emitting trap events to remote hosts. Trap Forwarding is available from the application through Actions and through the Resource Manager.

**VLAN** — A virtual local area network (LAN), commonly known as a VLAN, is a group of hosts with a common set of requirements that communicate as if they were attached to the Broadcast domain, regardless of their physical location. A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are not located on the same network switch. Network reconfiguration can be done through software instead of physically relocating devices.



# Index

## Numerics

32-bit Linux Libraries 18

## A

A Note About Performance  
13

About Box 72

Access Control 375

ACLI needs Perl 32

Acrobat 19

Action Job Screen Results  
panel 362

Actions 116, 343

Active Performance Monitor  
SNMP Performance  
Monitoring 262  
SNMP Performance  
Monitoring Ex-  
ample 262

Active Performance Monitor  
Support 371

Adaptive CLI 343

Attribute Appearance  
and Validation  
359

Attributes 350

Conditional Blocks 367

General 349

Monitor Attributes 373

Non Configuration at-  
tributes 357

Perl Scripts 368

Scripts 355

Adaptive CLI Editor 348

Adaptive CLI Script Lan-  
guage Syntax 366

Additional Products 11

Administration Overview 15

Aging Policies Editor 52

Aging Policies Options 54

Alarm 375

Alarm Email 104

Alarms 99

Alarm State 102

Assigned User 102

Date Assigned 102

Date Closed 102

Date Opened 100

Email 104

Entity Type 100

In Equipment Detail 181

In Topology 219

Notification Instance  
102

Service Effecting 100

Snap Panels 104

Suppression 170

Amigopod 27

API 375

Top 276

Attributes Extraction 359

Audit Trail 93

Audit Trail Screen 91

Audit Trail Snap Panels 94

Authentication 24, 375

Authentication Editor 144

Authentication Portlet 143

Authentication Snap Panel  
145

Authorization 375

## B

Back button 72

Backups

Latest Configurations  
277

Basic Network Consider-  
ations 22

Branding Reports 206

Breadcrumb trail 179

## C

Change Determination 328

Change Management  
Compliance Policy Vio-  
lation report 309

Change Management / ProS-  
can 303

Change Manager

Use paradigms 303

Changing the Session Time-  
out Period 33

Chat / Conferencing 76

Common Menu Items 86

Common Setup Tasks 68

Compliance Policy Summa-  
ry 308

Compliant label 328

Condition Override(s) 210

Configuration File Editor 231  
 Configuration Files 229  
 Configure Alarm E-mail 103  
 Contacts Editor 134  
 Contacts Portlet 133  
 Container Editor 148  
 Container Manager 146  
 Container Manager Expanded 146  
 Container View 147  
 Containers  
     Portlets filtered 147  
 Continue Pattern 358  
 Control Panel 34  
 CoS 375  
 Creating a new label 226  
 Creating or Modifying a ProScan Policy 310  
 Creating or Modifying ProScan Policy Groups 325  
 Custom Action 122  
 Custom attributes 45  
 Custom Debug 73  
 Customizing Report Logos 206  
**D**  
 DAP 50  
 DAP SubPolicies 53  
 dapviewer 58  
 Dashboard Editor 281  
 Dashboard View Selection 280  
 Dashboard Views 277  
 DATA (Topology) 214  
 DATA / VIEW SETTINGS (Topology) 213  
 Data Configuration 45  
 Database 375  
 Database Aging Policies 50  
 Database Aging Sub-Policies 55  
 Database Backup 61  
 Deploy OS 238  
 Deployment 375  
 Details 185  
 Digital Certificate 375  
 Direct Access 188  
 Discovering hostnames 156  
 Discovery Profile  
     Actions 158  
     General 154  
     Inspect 66, 159  
     Network 66, 156  
     Results 67, 161  
 Discovery Profile Editor 65, 154  
 Discovery Profiles 153  
 Discovery Profiles Expanded 161  
 DISPLAYED LEVELS (Topology) 210  
 DNS 23  
 Dock 73  
 Domain 375  
 Domain Name Servers 23  
 Dynamic Group 165  
**E**  
 Edit Custom Attributes 89  
 Email Action 120  
 Email Action Variables 122  
 Encryption 375  
 Equipment 375  
 Equipment Details 178  
 Equipment Icons 166  
 Equipment Name 102  
 Error Condition 358  
 Ethernet Access Point 376  
 Ethernet Access Service 376  
 Ethernet Service 376  
 Ethernet Trunk 375  
 Ethernet Trunk Port 376  
 Event 376  
 Event Definition 376  
 Event Definition Editor 128  
 Event Definitions 128  
     Correlations 132  
     General 129  
     Message Template 131  
 Event History Portlet 106  
 Event History Snap Panels 108  
 Event Instance 376  
 Event processing filters 112  
 Event Processing Rules 108  
 Event Template 376  
 Event Threshold 376  
 Executing Change Determination 328  
 Expanded Actions Portlet 344  
 Expanded Alarm Portlet 101  
 Expanded Audit Trail Portlet 94  
 Expanded Authentication Portlet 145  
 Expanded Event History Portlet 107

Expanded Location Portlet 137  
 Expanded OS Images portlet. 234  
 Expanded Portlets 82  
 Expanded Reports Portlet 203  
 Expanded Resource Monitor 247  
 Expanded Vendor Portlet 140  
 Export / Import 86  
 Exporter Registration 296  
 Exporting 376  
**F**  
 FAQ  
     Portal database backup / restore 62  
 Feedback 13  
 File Handles 31  
 File Management 223  
 File Server Editor 222  
 File server port conflict 70  
 File Servers Portlet 221  
 Filter 12, 377  
 Filter / Settings (Rule Editor) 112  
 Filter Management 48  
 Firewall Issues 25  
 Firewall requirements 30  
 Fixed IP Address 24  
 Flash 19  
 Flash for 64-bit browsers 19  
 Forward Northbound 117  
 FTP Protocol Selection 70

**G**  
 General (Rule Editor) 111  
 Getting Started 27  
 Graphs 77  
 Group Operations 225  
 GUI 377  
**H**  
 Heap 28, 29  
 Help / Tooltips 72  
 How to  
     Add / Remove Columns 84  
     Add User Roles 40  
     Add Users 36  
     Backup Configurations 225  
     Configure ProScan Groups 304  
     Configure Resource Level Permissions 59  
     Create a Container for each Customer 60  
     Create a Custom Dashboard View 282  
     Create a Key Metrics Monitor 264  
     Create a Monitor for an External Script 364  
     Create a Monitor Report 265  
     Create A Performance Template 286  
     Create a Report Tem-

plate 195  
 Create a Simple Dashboard View 279  
 Create a topology view 207  
 Create a Visualization 207  
 Create Adaptive CLI Example 369  
 Create an ICMP Monitor 263  
 Create an SNMP Interface Monitor 262  
 Create Event Processing Rules 109  
 Create Source Group Criteria 316  
 DAP Workflow 51  
 Deploy an OS Image 239  
 Discover Resources 152  
 Discover Your Network 65  
 Do Change Management (Example) 305  
 Edit Discovery Profiles 154  
 Filter Expanded Portlet Displays 85  
 Register a License 64  
 Report on Change Determination 331  
 Restore a single configuration to many target devices 241  
 Restore Configurations

- 227
- Run Change Determination 329
- Set Unix Permissions 31
- Share a Resource 88
- Use “How To” 12
- Use Containers 147
- Use Traffic Flow Analyzer 295
- I**
- ICMP Monitor 267
- IIS 29
- Import / Export 86
- Installation and Startup 28
- Installing Perl 32
- Interfaces 180
- Interfaces > Details 180
- Internet Information Services 29
- Introducing Storage Arrays 333
- IP address changes 24
- ISATAP 377
- J**
- Java 19
- K**
- Key 377
- Key Features 9
- Key Management 377
- Key Metric Editor 289
- Key Metrics Monitor 268
- L**
- Labels 224
- Level 1 Filters 210
- Level 2 Filters 210
- Level 3 Filters 210
- License 12
- License Viewer 63
- Link Discovery 176
- Location Editor 136
- Location Manager
  - Address 136
  - Parent location 136
- Location, updates 138
- Locations Portlets 135
- Locations Snap Panels 137
- M**
- Mail hosts 41
- Managed Object 377
- Managed Resource Groups 162
- Managed Resources 68
- Managed Resources Expanded 173
- Managed Resources Portlet 166
- Managing Windows systems 29
- Mandatory Fields 81
- Map Context
  - Portlets filtered 147
- Map Context without Containers 152
- mass deployments 237
- Match Regex for each line 315
- Mediation 46, 377
- Mediation Agent 377
- MEG 377
- Memory Footprint 28
- Menu 102
- Menu Bar 77
- Menu Options 153
- MEP 377
- MIB 377
- MIB Browser 188
- Migrating heartbeats 253
- Minimum hardware 16
- Monitor Editor 251
  - Calculated Metrics 254
  - Conditions 260
  - Inventory Mappings 259
  - Monitor Options 254
  - Thresholds 256
- Monitor Graph Background 259
- Monitor Options Type Specific Panels 266
- Monitors 276
- Monitors and Discovery 243
- Multiple Performance Templates 289
- N**
- Name Resolution 23
- Navigation 71
- Netrestore File Servers 70
- Network Basics 22
- Network Considerations 22
- Network Requirements 23
- Network Topology 207
- New link creation 175
- newlink ConfigImageEditor 236
- Non Configuration attributes 357
- O**
- OAM 377
- OID 377



OS Image Editor 235  
OS Images Portlet 233  
OSPF 377  
Portal > 42  
Overall Compliance 307  
**P**  
PDF 90  
Performance Dashboard 279  
Performance Dashboard  
Portlet 279  
Performance Indicators 179  
Performance Note 13  
Perl 32  
Perl / Java (Groovy) Lan-  
guage Policies 322  
Permissions when installing  
to Unix 31  
Policy 377  
Policy Enforcement Points  
(PEP) 377  
Policy routing 378  
Policy Rules 378  
Port Details 192  
Port Expanded 193  
Portal > Roles 41  
Portal > Settings 41  
Portal > Users 36  
Portal Database Backup 62  
Portal Database Restore 62  
Portal Overview 71  
Portlet Instances 81  
Portlet Level Permissions 58  
Portlets 78  
Ports > Details 181, 183  
Ports Expanded 193  
Ports Portlet 191

Ports required 30  
Post-processing rules 114  
PPTP (Point-to-Point Tun-  
neling Protocol) 378  
Printing manager contents  
87  
Private Key 378  
Profile 378  
ProScan 303  
    Compliance Reporting  
        329  
    count number of occur-  
        rences 315  
    Editor - Compliance 313  
    Editor - General 310  
    Java (Groovy) 323  
    Perl 322  
    Supported Regular Ex-  
        pressions 320  
    Use Cases 303  
    Use paradigms 303  
ProScan Editor 310  
ProScan Manager 306  
Proscan Monitor 269  
Proscan Policy Group Editor  
325  
Protocols Used 23  
Public / Private Page Behav-  
ior 40  
Public Key 378  
**Q**  
QoS 378  
Quick Navigation 62  
Quick Start 27  
Quickstart 15

**R**  
RADIUS 378  
RCSynergy 35  
Recommended Operating  
System Versions 16  
Recorder / Page turn icons  
84  
Redcell > Mediation 46  
Refresh 72  
Refresh Monitor Targets 276  
re-index 34  
Report Template Editors 196  
Report Templates 195  
Reports  
    Customizing Logos 206  
    Portlet 200  
    Snap Panels 203  
Repositories 57  
Resolve DNS Hostnames  
Activity 156  
Resource Discovery 152  
Resource Icons 166  
Resource Management Port-  
lets 143  
Resource Monitor Snap Pan-  
els 247  
Resource Monitors Portlet  
245  
Restoring Database 61  
Retention Policies 248  
Return to previous 72  
RIP 378  
Rule Editor 111  
    Actions 116  
**S**  
Saving Views 213

Schedule Refresh Monitor  
 Targets 276  
 Schedules 95  
 Schedules Portlet 95  
 Scheduling 95  
 Scheduling Actions 186  
 Scheduling Monitor Target Refresh 276  
 Scheduling Refresh Monitor Targets 276  
 Screen resolution 19  
 Screen width in pixels 20  
 Search in Portlets 81  
 Search Indexes 34  
 Self-signed Certificate 378  
 Server 49  
 Server Statistics 244  
 Sharing 87  
 Show Performance Templates 286  
 Show Versions 72  
 Site Map portlet 77  
 Sizing memory 28  
 SMTP 379  
 SMTP Configuration 69  
 Snap Panels 83  
 SNMP 379  
 SNMP Interface Monitor 273  
 SNMP Interface Monitor Example 262  
 SNMP Monitor 270  
 SNMP Table Monitor 274  
 Solaris Prerequisites 30  
 Sorting 82  
 Spanning Tree Protocol (STP) 379  
 SSH (Secure Shell) 379  
 SSL (Secure Sockets Layer) 379  
 Starting Web Client 33  
 Static Group 164  
 Status Bar Messaging 75  
 Storage  
     Array Capacity 336  
     Disk Groups and Virtual Disks 337  
     General 337  
     Host Access and Ports 336  
     Reference Tree 335  
     Storage Array Configuration 335  
     Summary 335  
 Storage Array Portlet 333  
 Storage Array Portlet Expanded 334  
 Storage Arrays 333  
 Sub-Policies 55  
 Supported Operating System Versions 16  
 Supported PowerConnect Models 24  
 Supported Web Browsers 19  
 Syslog Escalation Criteria 115  
 System Basics 15  
 System requirements 15  
**T**  
 Terminal 190  
 The Back Button 72  
 Threshold Graph Back-  
     ground 259  
 Tooltips 72  
 Top [Asset] Monitors Portlets 276  
 Top Configuration Backups Portlet 277  
 Topology 207  
     Actions 209  
     Balloon 216  
     Circular 218  
     Configuring Views 208  
     Data 214  
     Data / View Settings 213  
     Displayed Levels 210  
     Layout 216  
     Orthogonal 217  
     OVERVIEW 219  
     Radial 217  
     STYLE OPTIONS 211  
     ZOOM 210  
 Topology, saving 213  
 Traffic Flow Portlet  
     Drill Down 299  
 Traffic Flow Portlets 296  
     Search 301  
 Trap (SNMP Trap) 379  
 Trap Forwarding 379  
 Trap Forwarding Process 118  
 Troubleshooting  
     Users and Organizations 34  
**U**  
 Uninstalling 32  
 Update Location 138  
 Updating Your License 12

Upgrade licenses from previous version 12

**V**

Vendors Portlet 139

Vendors Snap Panel 141

View as PDF 90

Visualization 207

- Actions 209
- Alarms 219
- Balloon 216
- Basic Spring 219
- Circular 218
- Configuring Views 208
- Data / Node Finder 213
- Displayed Levels 210
- Graph Inventory 214
- Hierarchical-Cyclic 218
- Icons 215
- LAYOUT 216
- Layout 216
- Saving Views 213
- STYLE OPTIONS 211
- View Details 213
- ZOOM 210

Visualize My Network 207

VLAN 379

**W**

WBEM 26

- root login 27

WBEM Prerequisites 27

Web-Based Enterprise Management 26

Why share a schema? 350

Windows Management Interface 24

Windows Server 2008 16

Windows Terminal Server 16

