

SolarWinds® Orion®

Network Performance Monitor Administrator Guide



ORION NETWORK PERFORMANCE MONITOR

Copyright© 1995-2010 SolarWinds, Inc. all rights reserved worldwide. No part of this document may be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the written consent of SolarWinds All right, title and interest in and to the software and documentation are and shall remain the exclusive property of SolarWinds and its licensors. SolarWinds®, the SolarWinds logo, ipMonitor®, LANsurveyor®, and Orion® are among the trademarks or registered trademarks of the company in the United States and/or other countries. All other trademarks contained in this document and in the Software are the property of their respective owners.

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON SOFTWARE AND DOCUMENTATION FURNISHED HEREUNDER INCLUDING WITHOUT LIMITATION THE WARRANTIES OF DESIGN, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL SOLARWINDS, ITS SUPPLIERS OR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY EVEN IF SOLARWINDS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Microsoft®, Windows 2000 Server®, Windows 2003 Server®, and Windows 2008 Server® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Graph Layout Toolkit and Graph Editor Toolkit © 1992 - 2001 Tom Sawyer Software, Oakland, California. All Rights Reserved.

Portions Copyright © ComponentOne, LLC 1991-2002. All Rights Reserved.

Orion Network Performance Monitor Administrator Guide, Version 10.0, 5.11.2010

About SolarWinds

SolarWinds, Inc develops and markets an array of network management, monitoring, and discovery tools to meet the diverse requirements of today's network management and consulting professionals. SolarWinds products continue to set benchmarks for quality and performance and have positioned the company as the leader in network management and discovery technology. The SolarWinds customer base includes over 45 percent of the Fortune 500 and customers from over 90 countries. Our global business partner distributor network exceeds 100 distributors and resellers.

Contacting SolarWinds

You can contact SolarWinds in a number of ways, including the following:

Team	Contact Information
Sales	sales@solarwinds.com www.solarwinds.com 1.866.530.8100 +353.21.5002900
Technical Support	www.solarwinds.com/support
User Forums	www.thwack.com

Conventions

The documentation uses consistent conventions to help you identify items throughout the printed and online library.

Convention	Specifying
Bold	Window items, including buttons and fields.
<i>Italics</i>	Book and CD titles, variable names, new terms
Fixed font	File and directory names, commands and code examples, text typed by you
Straight brackets, as in [value]	Optional command parameters
Curly braces, as in {value}	Required command parameters
Logical OR, as in value1 value2	Exclusive command parameters where only one of the options can be specified

SolarWinds Orion Network Performance Monitor Documentation Library

The following documents are included in the SolarWinds Orion Network Performance Monitor documentation library:

Document	Purpose
Administrator Guide	Provides detailed setup, configuration, and conceptual information.
Evaluation Guide	Provides an introduction to Orion Network Performance Monitor features and instructions for installation and initial configuration.
Page Help	Provides help for every window in the Orion Network Performance Monitor user interface
Quick Start Guide	Provides installation, setup, and common scenarios for which Orion Network Performance Monitor provides a simple, yet powerful, solution.
Release Notes	Provides late-breaking information, known issues, and updates. The latest Release Notes can be found at www.solarwinds.com .

Contents

<i>About SolarWinds</i>	<i>iii</i>
<i>Contacting SolarWinds</i>	<i>iii</i>
<i>Conventions</i>	<i>iv</i>
<i>SolarWinds Orion Network Performance Monitor Documentation Library</i>	<i>iv</i>

Chapter 1

Introduction	1
<i>Why Install SolarWinds Orion NPM</i>	<i>1</i>
<i>Benefits of Orion Network Performance Monitor</i>	<i>2</i>
<i>Key Features of Orion Network Performance Monitor</i>	<i>2</i>
<i>Networking Concepts and Terminology</i>	<i>5</i>
<i>Internet Control Message Protocol (ICMP)</i>	<i>5</i>
<i>Simple Network Management Protocol (SNMP)</i>	<i>6</i>
<i>SNMP Credentials</i>	<i>6</i>
<i>Management Information Base (MIB)</i>	<i>7</i>
<i>How Orion Network Performance Monitor Works</i>	<i>7</i>

Chapter 2

Installing SolarWinds Orion Network Performance Monitor	9
<i>Licensing Orion Network Performance Monitor</i>	<i>9</i>
<i>Orion NPM Requirements</i>	<i>10</i>
<i>Orion NPM Server</i>	<i>10</i>
<i>Orion Database Server (SQL Server)</i>	<i>11</i>
<i>Requirements for Virtual Machines and Servers</i>	<i>12</i>
<i>SNMP Requirements for Monitored Devices</i>	<i>12</i>
<i>Server Sizing</i>	<i>13</i>
<i>Enabling Microsoft Internet Information Services (IIS)</i>	<i>13</i>
<i>Enabling IIS on Windows Server 2003 and Windows XP</i>	<i>14</i>
<i>Enabling IIS on Windows Vista and Windows Server 2008</i>	<i>14</i>
<i>Enabling IIS on Windows 7</i>	<i>15</i>
<i>Installing Orion Network Performance Monitor</i>	<i>15</i>
<i>Completing an Orion NPM Installation</i>	<i>16</i>
<i>Completing the Orion Configuration Wizard</i>	<i>18</i>

- Upgrading Orion Network Performance Monitor* 20
- Maintaining Licenses with License Manager* 22
 - Installing License Manager* 22
 - Using License Manager* 22
- Enabling Secure Channels with SSL* 23

Chapter 3

- Discovering and Adding Network Devices** **25**
- Network Discovery Using the Network Sonar Wizard* 25
- Using the Network Sonar Results Wizard* 30
- Importing a List of Nodes Using a Seed File* 31
- Managing Scheduled Discovery Results* 32
- Using the Discovery Ignore List* 33

Chapter 4

- Managing the Orion Web Console** **35**
- Logging in for the First Time as an Administrator* 35
- Using the Web Console Notification Bar* 35
- Navigating the Orion Web Console* 36
 - Using Web Console Tabs* 36
 - Using Web Console Breadcrumbs* 37
- Administrative Functions of the Orion Web Console* 37
 - Changing an Account Password* 38
 - Orion Website Administration* 38
 - Viewing Secure Data on the Web* 41
 - Handling Counter Rollovers* 42
- Orion Network Performance Monitor Thresholds* 43
 - Orion General Threshold Types* 43
 - Network Performance Monitor Threshold Types* 44
 - Setting Orion NPM Thresholds* 45
- Customizing Views* 46
 - Creating New Views* 46
 - Editing Views* 46
 - Configuring View Limitations* 48
 - Copying Views* 48

<i>Deleting Views</i>	49
<i>Views by Device Type</i>	49
<i>Resource Configuration Examples</i>	49
<i>Creating and Editing External Website Views</i>	59
<i>Customizing the Orion Web Console</i>	59
<i>Customizing Web Console Menu Bars</i>	59
<i>Changing the Web Console Color Scheme</i>	61
<i>Changing the Web Console Site Logo</i>	61
<i>Configuring the Available Product Updates View</i>	62
<i>Updating your Orion Installation</i>	62
<i>Orion Web Console and Chart Settings</i>	63
<i>Web Console Settings</i>	63
<i>Chart Settings</i>	64
<i>Discovery Settings</i>	65
<i>Using Node Filters</i>	65
<i>Custom Charts in the Orion Web Console</i>	66
<i>Customizing Charts in the Orion Web Console</i>	66
<i>Custom Interface Charts</i>	68
<i>Custom Node Charts</i>	69
<i>Custom Volume Charts</i>	70
<i>Custom Chart View</i>	71
<i>Integrating SolarWinds Engineer's Toolset</i>	72
<i>Configuring a Toolset Integration</i>	72
<i>Adding Programs to a Toolset Integration Menu</i>	73
<i>Accessing Nodes Using HTTP, SSH, and Telnet</i>	74
<i>Using Integrated Remote Desktop</i>	74
<i>Managing Orion Web Console Configurations</i>	75
<i>Creating a Web Console Configuration Backup</i>	75
<i>Restoring a Web Console Configuration Backup</i>	76
<i>Clearing a Web Console Configuration</i>	76

Chapter 5

Managing Devices in the Web Console	77
<i>Network Overview</i>	77
<i>Adding Devices for Monitoring in the Web Console</i>	78
<i>Deleting Devices from Monitoring</i>	81

Viewing Node and Interface Data in Tooltips..... 82

Editing Device Properties..... 83

Promoting a Node from ICMP to SNMP Monitoring..... 84

Viewing Node Resources..... 85

Setting Device Management States..... 86

Assigning Pollers to Monitored Devices..... 87

Unscheduled Device Polling and Rediscovery 88

Remotely Managing Monitored Interfaces 88

Monitoring Windows Server Memory 89

Scheduling a Node Maintenance Mode Time Period 89

Chapter 6

Managing Web Accounts **91**

Creating New Accounts..... 91

Editing User Accounts..... 92

User Account Access Settings..... 92

Setting Account Limitations 93

Defining Pattern Limitations..... 94

Setting Default Account Menu Bars and Views 95

Configuring an Account Report Folder 96

Configuring Audible Web Alerts..... 97

Chapter 7

Managing Orion NPM Polling Engines..... **99**

Viewing Polling Engine Status 99

NetPerfMon Engine 99

Status Pollers..... 100

Packet Queues 100

Statistics Pollers 100

Configuring Polling Engine Settings..... 101

Orion Polling Settings 101

Calculating Node Availability 105

Calculating a Baseline 105

Setting the Node Warning Interval..... 106

<i>Polling Engine Tuning</i>	106
<i>Estimating a Good Value</i>	107
<i>Setting the Maximum Polls per Second</i>	108
<i>Using the Polling Engine Load Balancer</i>	108

Chapter 8

Monitoring EnergyWise Devices	111
<i>What is EnergyWise?</i>	111
<i>EnergyWise Terminology</i>	111
<i>Monitoring EnergyWise Devices with Orion NPM</i>	113
<i>EnergyWise Summary View and Resources</i>	114
<i>Additional EnergyWise Resources</i>	115
<i>Adding the EnergyWise Summary View</i>	117
<i>Managing EnergyWise Interface Entity Power Levels</i>	117

Chapter 9

Monitoring VMware ESX Servers	119
<i>Monitoring VMware ESX Servers with Orion NPM</i>	119
<i>Requirements for Monitoring ESXi and ESX Servers</i>	119
<i>Enabling SNMP on VMware ESXi and ESX Servers</i>	120
<i>Enabling SNMP on VMware ESXi</i>	120
<i>Enabling SNMP on ESX Server version 3.5</i>	121
<i>Enabling SNMP on ESX Server Version 4.0</i>	123
<i>Creating ESX Server Credentials for Orion NPM</i>	125
<i>Managing VMware Credentials in the Web Console</i>	126
<i>Adding ESX Servers for Monitoring</i>	126

Chapter 10

Monitoring Wireless Networks	127
<i>Getting Started</i>	127
<i>Migrating Data from the Wireless Networks Module</i>	127
<i>Viewing Wireless Data</i>	127
<i>Removing a Wireless Device</i>	128

Chapter 11

Monitoring Network Events..... 129

Viewing Event Details in the Web Console..... 129

Acknowledging Events in the Web Console 130

Viewing Event Details in System Manager 130

Acknowledging Network Events in System Manager 131

Chapter 12

Creating and Managing Alerts 133

Alerts Predefined by Default 133

Viewing Alerts in the Orion Web Console 134

Viewing Alerts in Orion NPM System Manager 134

Configuring Basic Alerts..... 135

Creating a New Basic Alert..... 136

Editing the Name of an Existing Basic Alert 136

Selecting the Monitored Property of a Basic Alert..... 137

Selecting the Network Objects Monitored by a Basic Alert 137

Setting the Alert Trigger of a Basic Alert 138

Setting the Time of Day for a Basic Alert..... 138

Setting the Alert Suppression for a Basic Alert..... 138

Selecting the Actions of a Basic Alert..... 139

Testing a Basic Alert 140

Configuring Basic Alert Copies 141

Changing the Name of a Copied Alert..... 141

Changing the Monitored Property of a Copied Alert..... 141

Changing Network Objects Monitored by a Copied Alert 142

Changing the Alert Trigger of a Copied Alert..... 142

Changing the Time of Day of a Copied Alert..... 143

Changing the Alert Suppression of a Copied Alert..... 143

Changing the Actions of a Copied Alert..... 144

Deleting a Basic Alert..... 144

Deactivating a Basic Alert 145

Creating and Configuring Advanced Alerts..... 145

Creating a New Advanced Alert..... 145

Naming, Describing, and Enabling an Advanced Alert..... 146

Setting a Trigger Condition for an Advanced Alert..... 146

<i>Setting a Reset Condition for an Advanced Alert</i>	148
<i>Setting a Suppression for an Advanced Alert</i>	149
<i>Setting the Monitoring Period for an Advanced Alert</i>	150
<i>Setting a Trigger Action for an Advanced Alert</i>	151
<i>Setting a Reset Action for an Advanced Alert</i>	152
<i>Alert Escalation</i>	153
<i>Understanding Condition Groups</i>	153
<i>Using the Advanced Alert Manager</i>	154
<i>Adding Alert Actions</i>	158
<i>Available Alert Actions</i>	158
<i>Send an E-mail / Page</i>	158
<i>Playing a Sound</i>	161
<i>Logging Alerts to a File</i>	162
<i>Logging an Alert to the Windows Event Log</i>	164
<i>Sending a Syslog Message</i>	166
<i>Executing an External Program</i>	169
<i>Executing a Visual Basic Script</i>	170
<i>E-mailing a Web Page</i>	171
<i>Changing a Custom Property</i>	173
<i>Using Text to Speech Output</i>	174
<i>Sending a Windows Net Message</i>	175
<i>Sending an SNMP Trap</i>	176
<i>Using GET or POST URL Functions</i>	177
<i>Acknowledging Advanced Alerts in the Web Console</i>	177
<i>Acknowledging Advanced Alerts in System Manager</i>	178
<i>Escalated Alerts</i>	178
<i>Escalated Alert Example</i>	178
<i>Creating a Series of Escalated Alerts</i>	179

Chapter 13

Creating Network Maps	183
------------------------------------	------------

Chapter 14

Creating Reports	185
<i>Viewing Reports</i>	185
<i>Viewing Reports in the Orion Web Console</i>	185
<i>Viewing Reports in the Orion NPM Report Writer</i>	186

<i>Predefined Reports</i>	186
<i>Availability</i>	186
<i>Current Interface Status</i>	187
<i>Current Node Status</i>	187
<i>Current Volume Status</i>	188
<i>Daily Node Availability</i>	188
<i>EnergyWise Reports</i>	188
<i>Events</i>	191
<i>Historical Cisco Buffer Miss Reports</i>	192
<i>Historical CPU and Memory Reports</i>	192
<i>Historical Response Time Reports</i>	192
<i>Historical Traffic Reports</i>	193
<i>Historical VMware ESX Server Reports</i>	194
<i>Historical Volume Usage Reports</i>	195
<i>Inventory</i>	195
<i>Wireless Reports</i>	196
<i>Getting Started with Report Writer</i>	198
<i>Preview Mode</i>	198
<i>Design Mode</i>	199
<i>Creating and Modifying Reports</i>	199
<i>General Options Tab</i>	199
<i>Select Fields Options Tab</i>	200
<i>Filter Results Options Tab</i>	201
<i>Top XX Records Options Tab</i>	201
<i>Time Frame Options Tab</i>	202
<i>Summarization Options Tab</i>	202
<i>Report Grouping Options Tab</i>	202
<i>Field Formatting Options Tab</i>	203
<i>Customizing the Report Header and Footer Image</i>	203
<i>Exporting Reports</i>	203
<i>Example Report</i>	204
<i>Using Orion Report Scheduler</i>	206
<i>Creating a Scheduled Report Job</i>	206
<i>Using Orion Report Scheduler with HTTPS</i>	207
<i>Reports and Account Limitations</i>	208

Chapter 15

Monitoring Syslog Messages	211
<i>Syslog Messages in the Web Console</i>	211
<i>Syslog Resources</i>	212
<i>Viewing Syslog Messages in the Web Console</i>	213
<i>Acknowledging Syslog Messages in the Web Console</i>	214
<i>Using the Syslog Viewer</i>	214
<i>Viewing and Acknowledging Current Messages</i>	214
<i>Searching for Syslog Messages</i>	215
<i>Syslog Server Settings</i>	215
<i>Configuring Syslog Viewer Filters and Alerts</i>	216
<i>Available Syslog Alert Actions</i>	218
<i>Forwarding Syslog Messages</i>	220
<i>Syslog Alert Variables</i>	221
<i>Syslog Date/Time Variables</i>	221
<i>Other Syslog Variables</i>	222
<i>Syslog Message Priorities</i>	222
<i>Syslog Facilities</i>	222
<i>Syslog Severities</i>	223

Chapter 16

Monitoring SNMP Traps	225
<i>The SNMP Trap Protocol</i>	225
<i>Viewing SNMP Traps in the Web Console</i>	225
<i>Using the Trap Viewer</i>	226
<i>Viewing Current Traps</i>	226
<i>Searching for Traps</i>	227
<i>Trap Viewer Settings</i>	227
<i>Configuring Trap Viewer Filters and Alerts</i>	228
<i>Available Trap Alert Actions</i>	230
<i>Trap Alert Variables</i>	231
<i>Trap Date/Time Variables</i>	232
<i>Other Trap Variables</i>	232

Chapter 17

Monitoring MIBs with Universal Device Pollers 235

Downloading the SolarWinds MIB Database 235

Creating Universal Device Pollers 236

Assigning Pollers to Nodes or Interfaces 240

Disabling Assigned Pollers..... 241

Duplicating an Existing Poller..... 242

Importing MIB Pollers..... 242

Exporting Universal Device Pollers 243

Transforming Poller Results..... 244

Available Poller Transformations 244

Creating a Poller Transformation..... 245

Viewing Universal Device Poller Statistics..... 249

Creating Alerts for Universal Device Pollers 249

Chapter 18

Creating Custom Properties 251

Creating a Custom Property..... 251

Removing a Custom Property..... 252

Editing Custom Properties 253

Using Filters in Edit View 253

Creating Custom Properties Filters 253

Removing Custom Properties Filters..... 254

Importing Custom Property Data..... 255

Custom Property Editor Settings..... 256

Chapter 19

Creating Account Limitations 257

Using the Account Limitation Builder 257

Creating an Account Limitation..... 257

Deleting an Account Limitation 258

Chapter 20

Using Orion System Manager	259
<i>Starting System Manager</i>	<i>259</i>
<i>Finding Nodes in the Node Tree.....</i>	<i>259</i>
<i>Grouping Nodes in the Node Tree.....</i>	<i>260</i>
<i>Viewing Network Details</i>	<i>260</i>
<i>Network Performance Monitor Settings.....</i>	<i>260</i>
<i>Charts Settings.....</i>	<i>261</i>
<i>Node Tree Settings</i>	<i>261</i>
<i>Creating XML Snapshots.....</i>	<i>262</i>
<i>Viewing Alerts in System Manager.....</i>	<i>262</i>
<i>Viewing Basic Alerts in System Manager</i>	<i>263</i>
<i>Viewing Advanced Alerts in System Manager</i>	<i>263</i>
<i>Viewing Charts.....</i>	<i>265</i>
<i>Predefined Charts in Orion System Manager</i>	<i>265</i>
<i>Customizing Charts.....</i>	<i>268</i>

Chapter 21

Managing the Orion NPM Database.....	269
<i>Using Database Manager.....</i>	<i>269</i>
<i>Adding a Server.....</i>	<i>269</i>
<i>Creating Database Backups</i>	<i>270</i>
<i>Restoring a Database</i>	<i>270</i>
<i>Compacting your Database.....</i>	<i>271</i>
<i>Compacting Individual Tables.....</i>	<i>272</i>
<i>Viewing Database Details</i>	<i>272</i>
<i>Viewing Table Details.....</i>	<i>273</i>
<i>Editing Database Fields</i>	<i>274</i>
<i>Detaching a Database.....</i>	<i>275</i>
<i>Creating a Database Maintenance Plan</i>	<i>275</i>
<i>Using SQL Server Management Studio</i>	<i>276</i>
<i>Database Maintenance.....</i>	<i>278</i>
<i>Running Database Maintenance.....</i>	<i>278</i>
<i>Migrating your Database</i>	<i>279</i>

Chapter 22

Monitoring Network Application Data 281

Chapter 23

Managing IP Addresses..... 283

Chapter 24

Monitoring NetFlow Traffic Analysis Data..... 285

Chapter 25

Managing IP Service Level Agreements 287

Why Install Orion Network Performance Monitor..... 287

What Orion Network Performance Monitor Does..... 287

Chapter 26

Orion Hot Standby Engine 289

Installing a Hot Standby Engine 290

Configuring a Hot Standby Engine..... 292

Testing a Hot Standby Engine 293

Chapter 27

Using Additional Polling Engines..... 295

Additional Polling Engine System Requirements..... 295

Installing an Additional Polling Engine 295

Upgrading an Additional Polling Engine..... 296

Configuring an Additional Polling Engine..... 296

Custom Properties on Additional Polling Engines..... 297

Copying Basic Alerts to an Additional Polling Engine..... 297

Chapter 28

Using an Orion Additional Web Server 299

Appendix A

Software License Key 303

Appendix B

Status Icons and Identifiers	305
<i>Status Indicators</i>	305
<i>Status Rollup Mode</i>	306

Appendix C

Alert Variables and Examples	309
<i>Variable Modifiers</i>	309
<i>Basic Alert Engine Variables</i>	309
<i>Buffer Errors</i>	309
<i>Interfaces</i>	310
<i>Interface Errors</i>	310
<i>Interface Status</i>	311
<i>Interface Polling</i>	311
<i>Interface Traffic</i>	311
<i>Nodes</i>	312
<i>Node Polling</i>	313
<i>Node Statistics</i>	313
<i>Node Status</i>	313
<i>Object Types</i>	313
<i>Volumes</i>	314
<i>Volume Polling</i>	314
<i>Volume Statistics</i>	314
<i>Volume Status</i>	314
<i>Date/Time</i>	315
<i>Alert-specific</i>	315
<i>Example Messages Using Variables</i>	316
<i>Basic Alert Engine Suppression Examples</i>	316
<i>Dependent Node Alert Suppression Example</i>	318
<i>Failure of Load Balancing Alert</i>	319
<i>Advanced Alert Engine Variables</i>	321
<i>General</i>	321
<i>Universal Device Poller</i>	321
<i>Date/Time</i>	322
<i>SQL Query</i>	323
<i>Node Status Variables</i>	323
<i>Interface Poller Variables</i>	324
<i>Node Poller Variables</i>	326
<i>Interface Variables</i>	328
<i>Node Variables</i>	330

- Volume Variables..... 333
- Wireless Node Variables 334
- Syslog Alert Variables 334
 - Syslog Date/Time Variables 334
 - Other Syslog Variables 335
- Trap Alert Variables 335
 - Trap Date/Time Variables..... 335
 - Other Trap Variables 336

Appendix D

- 95th Percentile Calculations 339**

Appendix E

- Configuring Automatic Login 341**
 - Passing Login Information Using URL Parameters 341
 - Using Windows Pass-through Security..... 342
 - Using the DirectLink Account..... 344

Appendix F

- Regular Expression Pattern Matching 345**
 - Characters..... 345
 - Character Classes or Character Sets [abc] 345
 - Anchors 346
 - Quantifiers 347
 - Dot..... 348
 - Word Boundaries 348
 - Alternation 348
 - Regular Expression Pattern Matching Examples..... 348

Appendix G

- Troubleshooting 351**
 - Back Up Your Data 351
 - Verify Program Operation 351

<i>Stop and Restart</i>	351
<i>Run the Configuration Wizard</i>	351
<i>Adjusting Interface Transfer Rates</i>	352
<i>Using Full Variable Names</i>	352
<i>Working with Temporary Directories</i>	352
<i>Moving the SQL Server Temporary Directory</i>	352
<i>Redefining Windows System Temporary Directories</i>	353

Index

Index	355
--------------------	------------

Chapter 1

Introduction

Orion Network Performance Monitor (Orion NPM) delivers comprehensive fault and network performance management that scales with rapid network growth and expands with your network monitoring needs, allowing you to collect and view availability and realtime and historical statistics directly from your web browser. While monitoring, collecting, and analyzing data from routers, switches, firewalls, servers, and any other SNMP-enabled devices, Orion NPM successfully offers you a simple-to-use, scalable network monitoring solution for IT professionals juggling any size network. Users find that it does not take a team of consultants and months of unpleasant surprises to get Orion NPM up and running because the Orion NPM experience is far more intuitive than conventional, complex enterprise network management systems. Because it can take less than an hour to deploy and no consultants are needed, Orion NPM provides quick and cost-effective visibility into the health of network devices, servers, and applications on your network, ensuring that you have the realtime information you need to keep your systems running at peak performance.

Why Install SolarWinds Orion NPM

Out of the box, Orion NPM monitors the following critical performance metrics for devices on your network:

- Network availability
- Bandwidth capacity utilization
- Buffer usage and errors
- CPU and memory utilization
- Interface errors and discards
- Network latency
- Node, interface, and volume status
- Volume usage

These monitoring capabilities, along with a fully customizable web-based interface, alerting, reporting engines, and flexible expansion capabilities, make SolarWinds Orion Network Performance Monitor the easiest choice you will make involving your network performance monitoring needs.

Benefits of Orion Network Performance Monitor

Consider the following benefits of Orion Network Performance Monitor.

Out-of-the-box Productivity

Automatic discovery and wizard-driven configuration offer an immediate return on your investment. Within minutes of installing Orion NPM, you can be monitoring your critical network devices.

Easy to Understand and Use

Orion NPM is designed for daily use by staff that also have other responsibilities. The Orion NPM interface provides what you need where you expect to find it and offers advanced capabilities with minimal configuration overhead.

Affordable Value

While Orion NPM provides functionality that is comparable, if not superior, to most other solutions, the cost and maintenance of your Orion NPM installation is less than the initial cost of most other solutions.

Scalability

By adding individual polling engines, you can scale your Orion NPM installation to any environment size. By sharing the same database, you can also share a unified user interface, making the addition of polling engines transparent to your staff.

thwack.com Online Community

thwack.com is a community site that SolarWinds developed to provide SolarWinds users and the broader networking community with useful information, tools and valuable resources related to SolarWinds network management solutions. Resources that allow you both to see recent posts and to search all posts are available from the Orion Web Console, providing direct access to the thwack.com community.

Key Features of Orion Network Performance Monitor

Considering the previously listed benefits of Orion NPM and the following features, Orion NPM is a simple choice to make.

Customizable and Flexible Orion Web Console

You can easily customize the web console to meet your individual needs. If you want to segregate use, you can custom design views of your data and assign them to individual users. You can also create web console accounts for departments, geographic areas, or any other user-defined criteria.

Automatic and Scheduled Device Discovery

Wizard-driven device discovery further simplifies the addition of devices and interfaces to Orion NPM. Answer a few general questions about your devices, and the discovery application takes over, populating Orion NPM and immediately beginning network analysis. You can also create network discovery schedules to independently and automatically run Network Sonar Discovery jobs whenever you need them.

Intuitive Orion NPM Administration

Using the award-winning, intuitive Orion NPM web interface, you can now conduct administrative tasks, such as adding new devices, both individually and in groups, establish unique user accounts, and customize web console displays from anywhere on your network. These administration features allow you to save time by administering Orion NPM tasks remotely without having to RDP directly into the Orion NPM host server.

Open Integration

Enterprise-tested standards, including a Microsoft® SQL Server database and industry-standard MIBs and protocols, are the backbone of the Orion NPM network monitoring solution.

Integrated Wireless Poller

An integrated wireless device poller enables you to leverage proven Orion NPM alerts, reports, and web console resources as you monitor and manage wireless thin and autonomous access points in the same views in which you are already monitoring your wired network devices.

Cisco EnergyWise Monitoring

Cisco EnergyWise technology allows you to responsibly manage energy usage across the enterprise. With Orion NPM, you can view EnergyWise device management data to measure, report, and reduce the energy consumption of any devices connected to EnergyWise-enabled switches.

Network Atlas with ConnectNow

Network Atlas, the Orion network mapping application, gives you the ability to create multi-layered, fully customizable, web-based maps of your network to visually track the performance of any device in any location across your network in real time. The ConnectNow feature automatically draws links between directly-connected physical nodes discovered on your network.

Unpluggable Port Mode

Orion NPM enables you to designate selected ports as unpluggable, so you don't receive unnecessary alerts when users undock or shutdown connected devices. This feature is particularly useful for distinguishing low priority ports

connected to laptops and PCs from more critically important infrastructure ports. For more information, see “Editing Device Properties” on page 83.

Universal Device Pollers

The Universal Device Poller allows you to easily add any SNMP-enabled device into the local monitoring database and collect any statistics or information that are referenced in device MIB tables. Using poller transforms available in the Universal Device Poller Wizard, you can also manipulate data collected from multiple Universal Device Pollers to create your own custom statistics and then choose your own customized data display.

VMware ESX Server Monitoring

Orion NPM enables you to monitor VMware ESX servers, including VMware ESXi servers, and any virtual machines (VMs) hosted by ESX servers on your network. Available resources include lists of VMs on selected ESXi and ESX servers, performance details for ESXi and ESX servers and hosted VMs, and relevant charts and reports.

Incident Alerting

You can configure custom alerts to respond to hundreds of possible network scenarios, including multiple condition checks. Orion NPM alerts help you recognize issues before your network users experience productivity hits. Alert delivery methods and responses include email, paging, SNMP traps, text-to-speech, Syslog messaging, and external application execution.

Integrated Trap and Syslog Servers

Orion NPM allows you to save time when investigating network issues by giving you the ability to use traps and Syslog messages to access network information from a single interface instead of requiring that you poll multiple machines. You can use Orion NPM to easily set up alerts and then receive, process, forward, and send syslog and trap messages.

Detailed Historical Reports

Easily configure reports of data from the Orion database over custom time periods. Data is presented in an easily reviewed format in the web console or in the Orion Report Writer application. With over 40 built-in reports available, you can project future trends and capacity needs, and immediately access availability, performance, and utilization statistics. You can also download new reports for import into Report Writer from www.thwack.com.

Extensible Orion NPM Modules

With additional modules, including Application Performance Monitor, NetFlow Traffic Analyzer, IP SLA Manager (formerly VoIP Monitor), IP Address Manager, and the Network Configuration Manager integration, Orion NPM

can monitor network applications, analyze network traffic, monitor VoIP and WAN traffic using Cisco IP SLA, manage IP address and subnet allocations, and monitor EnergyWise devices, respectively. Orion modules save time by leveraging the existing Orion NPM deployment to add feature functionality without requiring additional standalone software.

Product Update Notifications

Receive regular, automatic notification of updates to your installed Orion monitoring and management applications in the Orion Web Console as soon as they are available from SolarWinds. Product updates can include upgrade opportunities, service packs, and hotfixes.

Orion Product Team Blog

Stay in touch with the people who bring you the products in the Orion family by following the Orion Product Team Blog on [thwack](#), the SolarWinds online user community. Read posts from Orion product managers and developers to learn how to extend and optimize your Orion installation to best meet the needs of your network.

Networking Concepts and Terminology

The following sections define the networking concepts and terminology that are used within Orion NPM.

- Internet Control Message Protocol (ICMP)
- Simple Network Management Protocol (SNMP)
- SNMP Credentials
- Management Information Base (MIB)

Internet Control Message Protocol (ICMP)

Orion NPM uses the Internet Control Message Protocol (ICMP) to poll for status using `ping` and `echo` requests of managed devices. When Orion NPM polls a managed device using ICMP, if the device is operationally up, it returns a response time and record of any dropped packets. This information is used by Orion NPM to monitor status and measure average response time and packet loss percentage for managed devices.

Note: Orion NPM only uses ICMP to poll devices for status, average response time, and packet loss percentage. Other information displayed in the Orion Web Console is obtained using SNMP requests.

Simple Network Management Protocol (SNMP)

For most network monitoring and management tasks, Orion NPM uses the Simple Network Management Protocol (SNMP). SNMP-enabled network devices, including routers, switches, and PCs, host SNMP agents that maintain a virtual database of system status and performance information that is tied to specific Object Identifiers (OIDs). This virtual database is referred to as a Management Information Base (MIB), and Orion NPM uses MIB OIDs as references to retrieve specific data about a selected, SNMP-enabled, managed device. Access to MIB data may be secured either with SNMP Community Strings, as provided with SNMPv1 and SNMPv2c, or with optional SNMP credentials, as provided with SNMPv3.

For more information about MIBs, see “Management Information Base (MIB)” on page 7.

For more information about SNMP credentials, see “SNMP Credentials” on page 6.

Notes:

- To properly monitor devices on your network, you must enable SNMP on all devices that are capable of SNMP communications. The steps to enable SNMP differ by device, so you may need to consult the documentation provided by your device vendor.
- If SNMPv2c is enabled on a device you want Orion NPM to monitor, by default, Orion NPM will attempt to use SNMPv2c to poll the device for performance information. If you only want Orion NPM to poll using SNMPv1, you must disable SNMPv2c on the device to be polled.

SNMP Credentials

SNMP credentials secure access to SNMP-enabled managed devices. SNMPv1 and SNMPv2c credentials serve as a type of password that is authenticated by confirming a match between a cleartext SNMP Community String provided by an SNMP request and the SNMP Community String stored as a MIB object on an SNMP-enabled, managed device. SNMPv3 provides a more secure interaction by employing the following fields:

- The **User Name** is a required cleartext string that identifies the agent or poll request that is attempting to access an SNMP-enabled device. User Name functions similarly to the SNMP Community String of SNMP v1 and v2c.
- The **Context** is an optional identifying field that can provide an additional layer of organization and security to the information available in the MIB of an SNMP-enabled device. Typically, the context is an empty string unless it is specifically configured on an SNMP-enabled device.

- SNMPv3 provides two optional **Authentication Methods**: Message Digest 5 (MD5) and Secure Hash Algorithm 1 (SHA1). Both methods, MD5 and SHA1, include the **Authentication Key** with the SNMPv3 packet and then generate a digest of an entire SNMPv3 packet that is then sent. MD5 digests are 20 bytes long, and SHA1 digests are 16 bytes long. When the packet is received, the User Name is used to recreate a packet digest using the appropriate method. Both digests are then compared to authenticate.
- SNMPv3 also provides two optional **Privacy/Encryption Methods**: Data Encryption Standard (DES56) and Advanced Encryption Standard (AES128) using a 128 bit key. DES56 uses a 56 bit key with a 56 bit salt, and AES128 uses a 128 bit key with a 128 bit salt to encrypt the full SNMP v3 packet.

Management Information Base (MIB)

A Management Information Base (MIB) is the formal description of a set of objects that can be managed using SNMP. MIB-I refers to the initial MIB definition, and MIB-II refers to the current definition. Each MIB object stores a value such as `sysUpTime`, `bandwidth utilization`, or `sysContact`. During polling, Orion NPM sends a `SNMP GET` request to each network device to poll the specified MIB objects. Received responses are then recorded in the Orion NPM database for use in Orion NPM, including within Orion Web Console resources.

Most network devices can support several different types of MIBs. While most devices support the standard MIB-II MIBs, they may also support any of a number of additional MIBs that you may want to monitor. Using a fully customizable Orion Universal Device Poller, you can gather information from virtually any MIB on any network device to which you have access.

How Orion Network Performance Monitor Works

Through ICMP, SNMP, and Syslog communication and data collection, Orion NPM continuously monitors the health and performance of your network. Orion NPM does this without interfering with the critical functions of your network devices. Unlike many other network monitoring products, Orion NPM helps you maintain the overall performance of your network in the following ways:

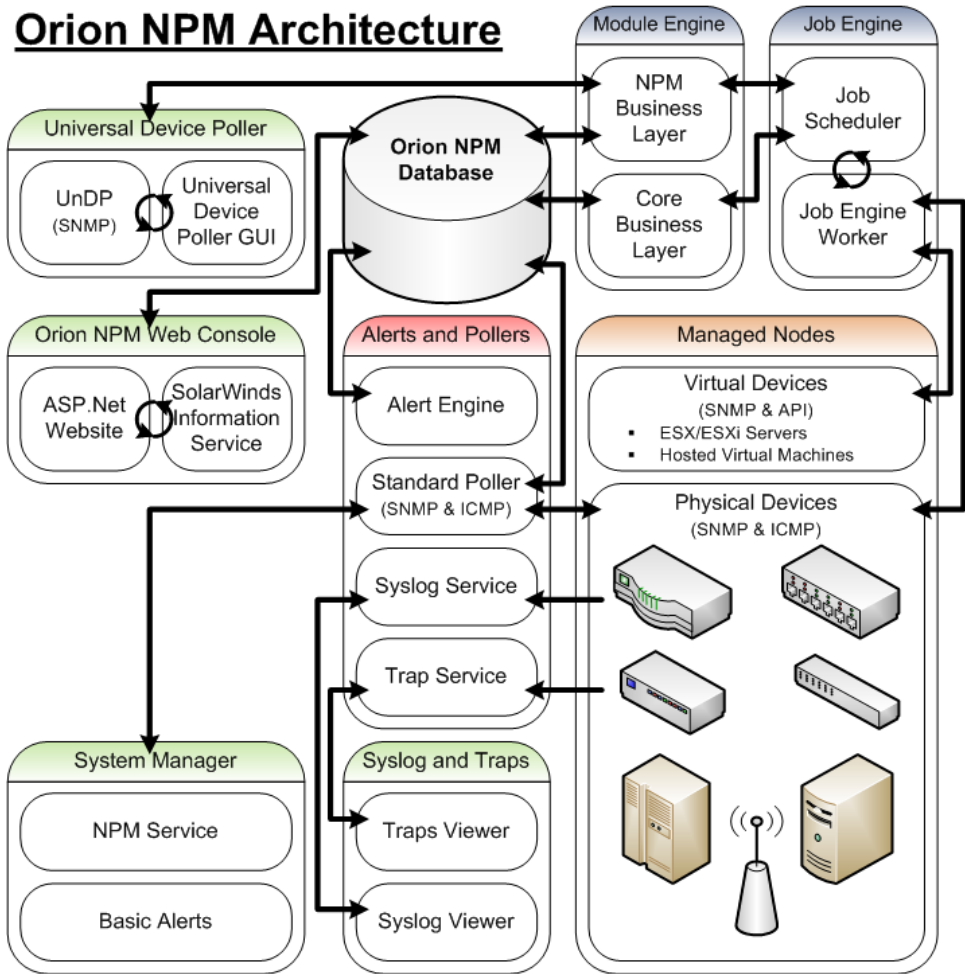
- Orion NPM does not install outside agents on your mission-critical servers
- Orion NPM does not employ services that take vital resources from critical applications
- Orion NPM does not install any code on monitored network devices. Unmanaged or outdated code can open security holes in your network.

After installing Orion NPM, you can automate the initial discovery of your network, and then simply add new devices to Orion NPM as you add them to your network. Orion NPM stores gathered information in a SQL database and

provides a user-friendly, highly customizable web console in which to view current and historical network status.

The following diagram provides an overview of the current Orion NPM architecture, including interactions among Orion NPM components, the Orion NPM database, and the managed nodes on your network.

Orion NPM Architecture



Chapter 2

Installing SolarWinds Orion Network Performance Monitor

Orion Network Performance Monitor (Orion NPM) provides a simple, wizard-driven installation process. For an enterprise-class product, licensing, hardware and software requirements are nominal.

Licensing Orion Network Performance Monitor

Orion NPM can collect data and detailed information from any of your version 3 or earlier SNMP-enabled devices, including routers, switches, firewalls, and servers. Orion NPM is licensed in accordance with the largest number of the following three types of monitored network elements:

Nodes

Nodes include entire devices, for example, routers, switches, virtual and physical servers, access points, and modems.

Interfaces

Interfaces include switch ports, physical interfaces, virtual interfaces, sub-interfaces, VLANs, and any other single point of network traffic.

Volumes

Volumes are equivalent to the logical disks you are monitoring.

The following list provides the different types of Orion Network Performance Monitor licenses that are available:

- Up to 100 elements (SL100)
- Up to 250 elements (SL250)
- Up to 500 elements (SL500)
- Up to 2000 elements (SL2000)
- Unlimited elements (SLX)

Database size increases with the addition of monitored elements. Depending on the number of elements and the amount of traffic flowing through the elements on your network, the successful monitoring of more than 8,000 objects can require the addition of more polling engines. For more information about adding polling engines, see “Using Additional Polling Engines” on page 295.

Orion NPM Requirements

SolarWinds recommends installing Orion NPM on its own server, with the Orion database hosted separately, on its own SQL Server. Installations of multiple Orion NPM servers using the same database are not supported.

Orion NPM Server

The following tables list minimum requirements for your Orion server.

Software	Requirements
Operating System	Windows 2008 Server R2 (32-bit or 64-bit, with IIS in 32-bit mode) Windows 2003 Server R2 (32-bit or 64-bit, with IIS in 32-bit mode) IIS must be installed. SolarWinds recommends that Orion NPM administrators have local administrator privileges to ensure full functionality of local Orion NPM tools. Accounts limited to use of the web console do not require administrator privileges. Note: SolarWinds does not support production installations of Orion NPM in Windows XP, Windows Vista, or Windows 7 environments.
Web Server	Microsoft IIS, version 6.0 and higher, in 32-bit mode. DNS specifications require that hostnames be composed of alphanumeric characters (A-Z, 0-9), the minus sign (-), and periods (.). Underscore characters (_) are not allowed. For more information, see <i>RFC 952</i> . Note: SolarWinds neither recommends nor supports the installation of Orion NPM on the same server or using the same database server as a Research in Motion (RIM) Blackberry server.
.NET Framework	Version 3.5 or higher. .NET Framework 3.5 SP1 is recommended.
SNMP Trap Services	Windows operating system management and monitoring tools component
Web Console Browser	Microsoft Internet Explorer version 6 or higher with Active scripting Firefox 3.0 or higher (Toolset Integration is not supported on Firefox)

Hardware	SL100, SL250, or SL500	SL2000	SLX
CPU Speed	2.0 GHz	2.4 GHz	3.0 GHz
	Note: Dual processor, dual core is recommended.		
Hard Drive Space	2 GB	5 GB	20 GB
	Note: A RAID 1 drive for server operating system, Orion NPM installation, and tempdb files is recommended. The Orion installer needs 1GB on the drive where temporary Windows system or user variables are stored. Per Windows standards, some common files may need to be installed on the same drive as your server operating system. For more information, see "Working with Temporary Directories" on page 352.		
Memory	2 GB	3 GB	3 GB
Application Ports	161/SNMP and 443/SNMP. VMware ESX/ESXi Servers are polled on 443. 17777/TCP open for Orion module traffic 17778/ HTTPS open to access the SolarWinds Information Service API		

Orion Database Server (SQL Server)

The following table lists software and hardware requirements, by license level, for your Orion database server.

Requirements	SL100, SL250, or SL500	SL2000	SLX
SQL Server	SQL Server 2005 SP1 Express, Standard, or Enterprise SQL Server 2008 Express, Standard, or Enterprise Notes: <ul style="list-style-type: none"> • Either mixed-mode or SQL authentication must be supported. • If you are managing your Orion database, SolarWinds recommends you install the SQL Server Management Studio component. • Use the following database select statement to check your SQL Server version, service pack or release level, and edition: <pre>select SERVERPROPERTY ('productversion'), SERVERPROPERTY ('productlevel'), SERVERPROPERTY ('edition')</pre> 		
CPU Speed	2.0 GHz	2.4 GHz	3.0 GHz
Hard Drive Space	2 GB	5 GB	20 GB
	Note: Due to intense I/O requirements, a RAID 1+0 drive is strongly recommended for the SQL Server database and Orion NPM data and log files. RAID 5 is not recommended for the SQL Server hard drive. The Orion installer needs at least 1GB on the drive where temporary Windows system or user variables are stored. Per Windows standards, some common files may need to be installed on drive as your server operating system. For more information, see “Working with Temporary Directories” on page 352.		
Memory	2 GB	3 GB	4 GB

The Configuration Wizard installs the following required x86 components if they are not found on your Orion database server:

- SQL Server System Common Language Runtime (CLR) Types. Orion NPM uses secure SQL CLR stored procedures for selected, non-business data operations to improve overall performance.
- Microsoft SQL Server Native Client
- Microsoft SQL Server Management Objects

Notes:

- If you are using SQL Server 2005 SP1 Express Edition on a Windows XP operating system, enable Shared Memory, TCP/IP, and Named Pipes.
- If Orion NPM installs SQL Server System CLR Types, a manual restart of the SQL Server service for your Orion database is required.

Requirements for Virtual Machines and Servers

Orion NPM installations on VMware Virtual Machines and Microsoft Virtual Servers are fully supported if the following minimum configuration requirements are met for each virtual machine.

Note: SolarWinds strongly recommends that you maintain your SQL Server database on a separate physical server.

Virtual Machine Configuration	Orion NPM Requirements by License Level		
	SL100, SL250, or SL500	SL2000	SLX
CPU Speed	2.0 GHz	2.4 GHz	3.0 GHz
Allocated Hard Drive Space	2GB	5GB	20GB
	Note: Due to intense I/O requirements, SQL Server should be hosted on a separate physical server configured as RAID 1+0. RAID 5 is not recommended for the SQL Server hard drive.		
Memory	2GB	3 GB	3 GB
Network Interface	Each installation of Orion NPM should have its own, dedicated network interface card. Note: Since Orion NPM uses SNMP to monitor your network, if you are unable to dedicate a network interface card to your Orion NPM installation, you may experience gaps in monitoring data due to the low priority generally assigned to SNMP traffic.		

SNMP Requirements for Monitored Devices

Orion NPM can monitor the performance of any SNMPv1-, SNMPv2c-, or SNMPv3-enabled device on your network. Consult your device documentation or a technical representative of your device manufacturer to acquire specific instructions for configuring SNMP on your device.

Notes:

- To properly monitor devices on your network, you must enable SNMP on all devices that are capable of SNMP communications.
- Unix-based devices should use the configuration of Net-SNMP version 5.5 or higher that is specific to the type of Unix-based operating system in use.
- Orion NPM is capable of monitoring VMware ESX and ESXi Servers versions 3.5 and higher with VMware Tools installed. For more information about enabling SNMP and VMware Tools on your VMware device, consult your VMware documentation or technical representative.
- If SNMPv2c is enabled on a device you want Orion NPM to monitor, by default, Orion NPM will attempt to use SNMPv2c to poll the device for performance information. If you only want Orion NPM to poll using SNMPv1, you must disable SNMPv2c on the device to be polled.

Server Sizing

Orion NPM is capable of monitoring networks of any size, ranging from small corporate LANs to large enterprise and service provider networks. Most Orion NPM systems perform well on 3.0 GHz systems with 3 GB of RAM, using default polling engine settings. However, when monitoring larger networks, you should give additional consideration to the hardware used and the system configuration.

There are three primary variables that affect scalability. The most important consideration is the number of monitored elements, where an element is defined as a single, identifiable node, interface, or volume. Systems monitoring more than 1,000 elements may require tuning for optimal performance. The second variable to consider is polling frequency. For instance, if you are collecting statistics every five minutes instead of the default nine, the system will have to work harder and system requirements will increase. Finally, the number of simultaneous users accessing Orion NPM directly impacts system performance.

When planning an Orion NPM installation, there are four main factors to keep in mind with respect to polling capacity: CPU, memory, number of polling engines, and polling engine settings. For minimum hardware recommendations, see “Orion NPM Requirements” on page 10. For more information about polling engines, see “Managing Orion NPM Polling Engines” on page 99.

In most situations, installing Orion NPM and SQL Server on different servers is highly recommended, particularly if you are planning to monitor 2000 elements or more. If you experience performance problems or you plan to monitor a very large network, you should certainly consider this option. This scenario offers several performance advantages, as the Orion NPM server does not perform any database processing, and it does not have to share resources with SQL Server.

If you plan to monitor 8000 or more elements, SolarWinds recommends that you install additional polling engines on separate servers to help distribute the work load. For more information about sizing Orion NPM to your network, contact the SolarWinds sales team or visit www.solarwinds.com. For more information about additional polling engines, see “Using Additional Polling Engines” on page 295.

Enabling Microsoft Internet Information Services (IIS)

To host the Orion Web Console, Microsoft Internet Information Services (IIS) must be installed and enabled on your Orion NPM server. Windows Server 2003 and Windows XP require IIS version 6; Windows Server 2008 and Windows Vista require IIS version 7, as detailed in the following sections:

- Enabling IIS on Windows Server 2003 and Windows XP
- Enabling IIS on Windows Vista and Windows Server 2008
- Enabling IIS on Windows 7

Enabling IIS on Windows Server 2003 and Windows XP

The following procedure enables IIS on Windows Server 2003.

To enable IIS on Windows Server 2003 and Windows XP:

1. Click **Start > Control Panel > Add or Remove Programs**.
2. Click **Add/Remove Windows Components**.
3. Select **Application Server** and confirm that it is checked.
4. Click **Details**.
5. Select **Internet Information Services (IIS)** and confirm that it is checked.
6. Click **Details**.
7. Select **World Wide Web Service** and confirm that it is checked.
8. Click **Details**.
9. Select **World Wide Web Service** and confirm that it is checked.
10. Click **OK**.
11. Click **OK** on the **Internet Information Services (IIS)** window.
12. Click **OK** on the **Application Server** window.
13. Select **Management and Monitoring Tools** and confirm that it is checked.
14. Click **Details**.
15. Select both **Simple Network Management Protocol** and **WMI SNMP Provider** and confirm that they are checked, and then click **OK**.
16. Click **Next** on the Windows Components window, and then click **Finish** after completing the Windows Components Wizard.
Note: You may be prompted to install additional components, to provide your Windows Operating System media, or to restart your computer.
17. *If you are currently enabling IIS as part of an Orion NPM installation, restart the Orion NPM installer. For more information, see "Completing an Orion NPM Installation" on page 16.*

Enabling IIS on Windows Vista and Windows Server 2008

The following procedure enables IIS on Windows Server 2008.

To enable IIS on Windows Vista and Windows Server 2008:

1. Click **Start > All Programs > Administrative Tools > Server Manager**.
2. Click **Roles** in the left pane.

3. Click **Add Roles** on the right, in the main pane.
4. Click **Next** to start the Add Roles Wizard.
5. Check **Web Server (IIS)**.
6. *If you are prompted to add features required for Web Server (IIS), click **Add Required Features**.*
7. Click **Next** on the Select Server Roles window.
8. Click **Next** on the Web Server (IIS) window.
9. Confirm that **Common HTTP Features > Static Content** is installed.
10. Check **Application Development > ASP.NET**.
11. Click **Add Required Role Services**.
12. Check both **Security > Windows Authentication** and **Security > Basic Authentication**.
13. Check **Management Tools > IIS 6 Management Compatibility**.
14. Click **Next** on the Select Role Services window.
15. Click **Install** on the Confirm Installation Selections window.
16. Click **Close** on the Installation Results window.
17. *If you are currently enabling IIS as part of an Orion NPM installation, restart the Orion NPM installer as detailed in “Completing an Orion NPM Installation” on page 16.*

Enabling IIS on Windows 7

SolarWinds only supports evaluations of Orion NPM version 10 and higher on Windows 7. In these version of Orion NPM, IIS is enabled automatically after installation and prior to the start of the Configuration Wizard.

Installing Orion Network Performance Monitor

Any installation or upgrade of Orion NPM requires completion of both the installer and the Configuration Wizard, as detailed in the following sections:

- Completing an Orion NPM Installation
- Completing the Orion Configuration Wizard

Completing an Orion NPM Installation

Before completing the Orion configuration Wizard, ensure that the computer on which you install Orion NPM currently meets or exceeds the stated requirements. For more information, see “Orion NPM Requirements” on page 10.

Notes:

- If you are using Internet Explorer, SolarWinds recommends that you add both the URL of your Orion website (`http://FullOrionServerName/`) and `about:blank` to the list of trusted sites. For more information about adding sites to your trusted sites list, see the Microsoft article, “Working with Internet Explorer 6 Security Settings”.
- For evaluation purposes only, Orion NPM may be installed on Windows 7, Windows XP, or Windows Vista. SolarWinds does not, however, support or recommend installing Orion NPM on these operating systems in production environments.
- When installing Orion NPM on Windows XP, you must confirm that Shared Memory, Named Pipes, and TCP/IP are enabled on remote databases.
- When installing Orion NPM on Windows Server 2008, Windows Vista, or Windows 7, you must disable IPv6 support in Internet Information Services (IIS). For more information, see <http://support.microsoft.com/kb/929852/>.
- If you are upgrading from a previous version of Orion Network Performance Monitor, see “Upgrading Orion Network Performance Monitor” on page 20.

The following procedure installs Orion NPM.

To install Orion Network Performance Monitor:

1. As an administrator, log on to your Orion NPM server.

Notes:

- To avoid permissions issues, do not log on using a domain account and do not install Orion NPM on a domain controller.
 - SolarWinds generally recommends that you back up your database before performing any upgrade.
2. ***If you are using more than one polling engine to collect network information***, shut down each of these polling engines before continuing.
 3. ***If you downloaded the product from the SolarWinds website***, navigate to your download location, and then launch the executable file.
 4. ***If you received physical media***, browse to the executable and launch it.

5. **If you are prompted to install requirements**, click **Install**, and then complete the installation, including a reboot, if required.

Notes:

- Downloading and installing Microsoft .NET Framework 3.5 may take up to 20 minutes or more, depending on your existing system configuration.
- If a reboot is required, after restart, click **Install** to resume installation, and then click **Next** on the Welcome window.

6. Review the Welcome text, and then click **Next**.

7. **If the InstallShield Wizard detects that Microsoft Internet Information Services (IIS) is not installed**, select **Suspend installation to manually install IIS**, click **Next**, quit setup, and then install IIS as shown in any of the following sections:

Note: The Orion Web Console requires that Microsoft IIS is installed on the Orion NPM Server. If you do not install IIS at this point, you must install IIS later, and then configure a website for the Orion Web Console to use.

- Enabling IIS on Windows Server 2003 and Windows XP
- Enabling IIS on Windows Vista and Windows Server 2008
- Enabling IIS on Windows 7

8. **If the InstallShield Wizard detects that Microsoft SQL Server CLR Types, Native Client, or Management Objects are not already installed**, click **Install**:

9. Accept the terms of the license agreement, and then click **Next**.

10. **If you want to install Orion NPM in a destination folder other than the default given**, click **Browse**, select an installation folder, and then click **OK**.

11. Click **Next** on the Choose Destination Location window.

12. Confirm the current installation settings, and then click **Next** on the Start Copying Files window.

13. Provide the appropriate information on the Install Software License Key window, and then click **Continue**.

Note: You need your customer ID and password to successfully install the key. For more information, see “Software License Key” on page 303.

14. Click **Continue** when the license is successfully installed.

15. Click **Finish** on the InstallShield Wizard Complete window.

The Orion Configuration Wizard should load automatically. For more information about completing the Orion Configuration Wizard, see “Completing the Orion Configuration Wizard” on page 18.

Completing the Orion Configuration Wizard

The following procedure using the Orion Configuration Wizard completes and configures your Orion NPM installation.

Notes:

- Confirm that you have designated a SQL Server database instance for Orion NPM. For more information, see “Orion NPM Requirements” on page 10.
- Confirm that the Internet Information Services (IIS) Manager is not open while the Configuration Wizard is running.
- During configuration, the Orion polling engine will shutdown temporarily with the result that, if you are actively polling, you may lose some polling data. SolarWinds recommends that you perform upgrades during off-peak hours of network usage to minimize the impact of this temporary polling stoppage.

To configure Orion Network Performance Monitor:

1. **If the Configuration Wizard has not loaded automatically**, click **Start > All Programs > SolarWinds Orion > Configuration and Auto-Discovery > Configuration Wizard**.
2. Click **Next** on the Welcome window of the Configuration Wizard.
3. **If you are prompted to stop services**, click **Yes**.

Note: To ensure that all updates and changes are installed correctly, it is imperative that you stop all services.

4. Specify the SQL Server instance you want to use to store network data.
5. Provide the credentials, if necessary, that are required to log into the selected instance.

Notes:

- **If you are using an existing database**, the user account needs only to be in the `db_owner` database role for the existing database.
- **If you are using an existing SQL account**, the user account needs only to be in the `db_owner` database role for the Orion NPM database.
- The selected instance must support mixed-mode or SQL authentication with strong passwords. A strong password must meet at least three of the following four criteria:
 - Contains at least one uppercase letter.
 - Contains at least one lowercase letter.

- Contains at least one number.
- Contains at least one non-alphanumeric character, e.g., #, %, or ^.

For more information about authentication with strong passwords, see <http://msdn.microsoft.com/ms143705.aspx>.

- ***If you are using SQL Express***, specify your instance as `(local)` and use a strong password. For more information about authentication with strong passwords, see <http://msdn.microsoft.com/ms143705.aspx>. Due to its inherent limitations, SolarWinds recommends against the use of SQL Express in production environments.
- ***If you are creating a new database***, the user account must be a member of the `dbcreator` server role. The `sysadmin` role and the `sa` user account are always members of `dbcreator`.
- ***If you are creating a new SQL account for use with Orion NPM***, the user account must be a member of the `securityadmin` server role.

Note: The `sysadmin` role and the `sa` user account are always members of `securityadmin`.

6. Click **Next**.

7. ***If you are creating a new database***, select **Create a new database**, provide a name for the new database, and then click **Next**.

Note: SolarWinds recommends against using non-alphanumeric characters in database names.

8. ***If you are using an existing database***, select **Use an existing database**, type the database name or select it from the list, and then click **Next**.

9. ***If you want to create a new SQL account for the Orion NPM polling engine and web console to use for accessing the database***, select **Create a new account**, provide an account name and password, confirm the account password, and then click **Next**.

10. ***If you want to use an existing SQL account for the Orion NPM polling engine and web console to use for accessing the database***, select the existing account, provide the appropriate password, and then click **Next**.

11. ***If you need to specify a particular IP Address for the Orion NPM Web Console***, provide the IP address of the host web server.

Note: SolarWinds recommends the default **All Unassigned** unless your environment requires a specific IP address for your Orion Web Console.

12. Specify both the port through which you want to access the web console and the volume and folder in which you want to install the web console files.

Note: If you specify any port other than 80, you must include that port in the URL used to access the web console. For example, if you specify an IP address of 192.168.0.3 and port 8080, the URL used to access the web console is `http://192.168.0.3:8080`.

13. Click **Next**.

14. **If you are prompted to create a new directory**, click **Yes**.

15. **If you are prompted to create a new website**, click **Yes**.

Note: Choosing to overwrite the existing website will not result in the deletion of any custom Orion NPM website settings you may have previously applied.

16. Confirm that all services you want to install are checked, and then click **Next**.

17. Review the final configuration items, and then click **Next**.

18. Click **Next** on the Completing the Orion Configuration Wizard dialog.

19. Click **Finish** when the Orion Configuration Wizard completes.

20. Log in to the Orion Web Console as an administrator.

Note: By default, you can log in with User Name `Admin` and no password.

21. **If you have not discovered your network devices and added them to the Orion database**, the Network Discovery Wizard starts. For more information, see “Discovering and Adding Network Devices” on page 25.

Upgrading Orion Network Performance Monitor

Complete the following procedure when you are upgrading Orion NPM from a previous version or upgrading the licensed number of elements you can monitor.

Notes:

- SolarWinds recommends that you backup your database before any upgrade. For more information about creating database backups, see the “Moving Your Orion NPM Database” technical reference.
- SolarWinds recommends that you backup your web console configuration after creating a backup of your database. For more information about web console configuration backups, see “Creating a Web Console Configuration Backup” on page 75.
- Discovery profiles from older Orion NPM versions are not retained through upgrades to this Orion NPM version. If you want to retain a discovery profile, prior to starting your upgrade, externally record the configuration of the profiles you want to retain.

- While it is being upgraded, your Orion polling engine will shutdown temporarily with the result that you may lose some polling data. SolarWinds recommends that you perform upgrades during off-peak hours of network usage to minimize the impact of this temporary polling stoppage.
- If you currently have Orion NPM 7.X installed, you must first upgrade to Orion NPM 7.8.5. After upgrading from Orion NPM 7.8.5 to Orion NPM 8.5.1, you can then upgrade to Orion NPM 9.1 SP5 before upgrading to any newer Orion NPM versions.
- For more information about upgrading Orion NPM, particularly if you are upgrading an Orion NPM installation that includes Orion modules, log in to your SolarWinds Customer Portal at www.solarwinds.com/customerportal/, click **License Management**, and then click **Upgrade Instructions** under the license listing of any Orion product.

To upgrade Orion Network Performance Monitor:

1. ***If you are using more than one polling engine to collect network information***, shut down all polling engines before continuing.
2. Using the local administrator account, log on to the computer on which you want to upgrade Orion Network Performance Monitor.
3. ***If you downloaded the product from the SolarWinds website***, navigate to your download location and then launch the executable.
4. Review the Welcome text, and then click **Next**.
5. Orion Network Performance Monitor automatically detects the previous installation. When prompted to upgrade the current installation, click **Next**.
Note: All customizations, including web console settings, are preserved.
6. Accept the terms of the license agreement, and then click **Next**.
7. Confirm the current installation settings.
8. Click **Next** on the Start Copying Files window.
9. Provide required information on the Install Software License Key window.
Note: You need your customer ID and password to successfully install the key. For more information, see “Software License Key” on page 303.
10. Click **Continue**, and then click **Continue** again when the license is successfully installed.
11. Review the Upgrade Reminder, and then click **Next**.
12. Click **Finish** on the InstallShield Wizard Complete window.
13. Complete the Configuration Wizard. For more information, see “Completing the Orion Configuration Wizard” on page 18.

Maintaining Licenses with License Manager

SolarWinds License Manager is an easily installed, free utility that gives you the ability to migrate Orion licenses from one computer to another without contacting SolarWinds Customer Service. The following sections provide procedures for installing and using License Manager.

Installing License Manager

Install License Manager on the computer from which you are migrating currently licensed products.

Note: You must install License Manager on a computer with the correct time. If the time on the computer is even slightly off, in either direction, from Greenwich Mean Time (GMT), you cannot reset licenses without contacting SolarWinds Customer Service. Time zone settings neither affect nor cause this issue.

To install License Manager:

1. Click **Start > All Programs > SolarWinds > SolarWinds License Manager Setup**.
2. Click **I Accept** to accept the SolarWinds EULA.
3. ***If you are prompted to install the SolarWinds License Manager application, click Install.***

Using License Manager

You must run License Manager on the computer where the currently licensed SolarWinds product is installed before you can migrate licenses to a new installation. The following procedure deactivates currently installed licenses that can then be transferred to a new installation.

To deactivate currently installed licenses:

1. Click **Start > All Programs > SolarWinds > SolarWinds License Manager**.
2. Check the products you want to deactivate on this computer.
3. Click **Deactivate**.
4. Specify your SolarWinds Customer ID and password when prompted, and then click **Deactivate**.

Note: Deactivated licenses are now available to activate on a new computer.

When you have successfully deactivated your products, log on to the computer on which you want to install your products, and then begin installation. When asked to specify your licenses, provide the appropriate information. The license you deactivated earlier is then assigned to the new installation.

Enabling Secure Channels with SSL

Orion NPM supports the use of Secure Sockets Layer certificates to enable secure communications with the Orion Web Console. The following procedure enables SSL connections to the Orion Web Console.

Notes:

- Secure SSL communications are conducted over port 443.
- The following procedure does not detail the process of either obtaining a required certificate or generating a certificate signing request for a third-party certificate authority. It is assumed that the required SSL certificate has already been installed on your Orion NPM server. For more information about acquiring and installing a required server certificate for SSL communications, see <http://support.microsoft.com/kb/298805>, from which the following procedure was adapted.

To enforce SSL connections to the Orion Web Console:

1. Log on as an administrator to your Orion NPM server.
2. Click **Start > Control Panel > Administrative Tools > Computer Management**.
3. Expand **Services and Applications > Internet Information Services (IIS) Manager > Web Sites**.
4. Click **SolarWinds NetPerfMon**.
5. Click **Action > Properties**.
6. Click the Web Site tab.
7. Confirm that **SSL port** is set to 443.
8. Click **Apply**.
9. Click **Advanced**.
10. **If the Multiple SSL identities for this Web site field does not list the IP address for the Orion Web Console with SSL port 443**, complete the following steps.
 - a. Click **Add**, and then select the **IP address** of the Orion Web Console.

Note: As it was set initially in the Configuration Wizard, this option is usually set to **(All Unassigned)**. If the IP address of the Orion Web Console was not initially set to (All Unassigned), select the actual, configured IP address of the Orion Web Console.
 - b. Type 443 as the **TCP port**, and then click **OK**.

11. Click the Directory Security tab.
12. Click **Edit** in the Secure communications section.
13. Check **Require secure channel (SSL)**.
14. Select **Accept client certificates** in the Client certificates area.
15. Click **OK** on the Secure Communications window.
16. Click **Apply**, and then click **OK** to exit.

Chapter 3

Discovering and Adding Network Devices

This chapter details the process of discovering network devices and then adding them to the Orion database. There are two ways—Web Node Management and network discovery using the Network Sonar Wizard—to add nodes in Orion NPM. The method recommended largely depends on the number of devices added. To discover and add a larger number of devices across your enterprise, the Network Sonar and Network Sonar Results Wizards are available. This chapter provides instructions for quickly populating your Orion database with the network devices, interfaces, and volumes that you want to monitor with Orion NPM. The Orion Web Console also provides an easy-to-use Web Node Management wizard suited to discovering and adding individual nodes, interfaces, and volumes. For more information, see “Managing Devices in the Web Console” on page 77.

Network Discovery Using the Network Sonar Wizard

Orion NPM provides the easy-to-use Network Sonar Wizard to direct you in the discovery of devices on your network. Before using the Network Sonar Wizard, consider the following points about network discovery in Orion NPM:

- The Network Sonar Wizard recognizes network devices that are already in your Orion database and prevents you from importing duplicate devices.
- CPU and Memory Utilization charts are automatically enabled for your Windows, Cisco Systems, VMware, and Foundry Networks devices.
- The community strings you provide in the Network Sonar Wizard are only used for SNMP `GET` requests, so read-only strings are sufficient.

The following procedure steps you through the discovery of devices on your network using the Network Sonar Wizard.

To discover devices on your network:

1. If the Network Sonar Wizard is not already open, click **Start > All Programs > SolarWinds Orion > Configuration and Auto-Discovery > Network Discovery**.
2. ***If you have already defined a network discovery***, a number of options are available on the Network Sonar Discovery tab. Select one of the following:
 - ***If you want to create a new discovery***, click **Add New Discovery**.
 - ***If you want to use an existing discovery to rediscover your network***, select the discovery you want to use, click **Discover Now**, and then

complete the Network Sonar Results Wizard after discovery completes. For more information about network discovery results, see “Using the Network Sonar Results Wizard” on page 30.

- ***If you want to edit an existing discovery before using it***, select the discovery you want to edit, and then click **Edit**.
 - ***If you want to import some or all devices found in a defined discovery that you may not have already imported for monitoring***, select a currently defined discovery, and then click **Import All Results**. For more information about network discovery results, see “Using the Network Sonar Results Wizard” on page 30.
 - ***If you want to import any newly enabled devices matching a defined discovery profile***, select a currently defined discovery, and then click **Import New Results**. For more information about network discovery results, see “Using the Network Sonar Results Wizard” on page 30.
 - ***If you want to delete an existing discovery profile***, select a currently defined discovery and then click **Delete**.
3. ***If the devices on your network do not require community strings other than the default strings `public` and `private` provided by Orion NPM***, click **Next** on the SNMP Credentials view.
 4. ***If any of your network devices require community strings other than `public` and `private` or if you want to use an SNMPv3 credential***, complete the following steps to add the required SNMP credential.

Note: Repeat the following procedure for each new community string. To speed up discovery, highlight the most commonly used community strings on your network, and then use the arrows to move them to the top of the list.

 - a. Click **Add New Credential**, and then select the **SNMP Version** of your new credential.
 - b. ***If you are adding an SNMPv1 or SNMPv2c credential***, provide the new **SNMP Community String**.
 - c. ***If you are adding an SNMPv3 credential***, provide the following information for the new credential:
 - **User Name, Context, and Authentication Method**
 - **Authentication Password/Key**, if required.
 - **Privacy/Encryption Method and Password/Key**, if required.
 - d. Click **Add**.
 5. Click **Next** on the SNMP Credentials view.

6. **If you want to discover any VMware ESX or ESXi Servers on your network**, confirm that **Poll for ESX** is checked, and then complete the following steps to add or edit required local ESX Server credentials.

Note: Repeat the following procedure for each new credential. To speed up discovery, use the arrows to move the most commonly used credentials on your network to the top of the list.

- a. Click **Add ESX Credential**.
- b. **If you are using an existing ESX credential**, select the appropriate credential from the **Choose Credential** dropdown menu.
- c. **If you are adding a new ESX credential**, select **<New Credential>** in the **Choose Credential** dropdown menu, and then provide a new credential name in the **Credential Name** field.

Note: SolarWinds recommends against using non-alphanumeric characters in VMware credential names.

- d. Add or edit the credential **User Name** and **Password**, as necessary.
 - e. Confirm the password, and then click **Add**.
7. Click **Next** on the Local ESX Credentials for VMware view.

8. **If you want to discover devices located on your network within a specific range of IP addresses**, complete the following procedure.

Note: Only one selection method may be used per defined discovery.

- a. Click **IP Ranges** in the Selection Method menu, and then, for each IP range, provide both a **Start address** and an **End address**.

Note: Scheduled discovery profiles should not use IP address ranges that include nodes with dynamically assigned IP addresses (DHCP).

- b. **If you want to add another range**, click **Add More**, and then repeat the previous step.

Note: If you have multiple ranges, click **X** to delete an incorrect range.

- c. **If you have added all the IP ranges you want to poll**, click **Next**.

9. **If you want to discover devices connected to a specific router or on a specific subnet of your network**, complete the following procedure:

Note: Only one selection method may be used per defined discovery.

- a. Click **Subnets** in the Selection Method menu.
- b. **If you want to discover on a specific subnet**, click **Add a New Subnet**, provide both a **Subnet Address** and a **Subnet Mask** for the desired subnet, and then click **Add**.

Note: Repeat this step for each additional subnet you want to poll.

- c. **If you want to discover devices using a seed router**, click **Add a Seed Router**, provide the IP address of the **Router**, and then click **Add**.

Notes:

- Repeat this step for each additional seed router you want to use.
 - Orion NPM reads the routing table of the designated router and offers to discover devices on the Class A network (255.0.0.0 mask) containing the seed router and the Class C networks (255.255.255.0 mask) containing all interfaces on the seed router, using the SNMP version chosen previously on the SNMP Credentials page.
 - Networks connected through the seed router are NOT automatically selected for discovery.
- d. Confirm that all networks on which you want to conduct your network discovery are checked, and then click **Next**.

10. **If you already know the IP addresses or hostnames of the devices you want to discover and include in the Orion database**, complete the following procedure:

- a. Click **Specific Nodes** in the Selection Method menu.
- b. Type the IPv4 addresses or hostnames of the devices you want Orion NPM to discover for monitoring into the provided field.

Note: Type only one IPv4 address or hostname per line.

- c. Click **Validate** to confirm that the provided IPv4 addresses and hostnames are assigned to SNMP-enabled devices.
- d. **If you have provided all the IPv4 addresses and hostnames you want to discover**, click **Next**.

11. Configure the options on the Discovery Settings view, as detailed in the following steps.

- a. Provide a **Name** and **Description** to distinguish the current discovery profile from other profiles you may use to discover other network areas.

Note: This Description displays next to the **Name** in the list of available network discovery configurations on the Network Sonar view.

- b. Position the slider or type a value, in ms, to set the **SNMP Timeout**.

Note: If you are encountering numerous SNMP timeouts during Network Discovery, increase the value for this setting. The SNMP Timeout should be at least a little more than double the time it takes a packet to travel the longest route between devices on your network.

- c. Position the slider or type a value, in ms, to set the **Search Timeout**.

Note: The Search Timeout is the amount of time Orion NPM waits to determine if a given IP address has a network device assigned to it.

- d. Position the slider or type a value to set the number of **SNMP Retries**.

Note: This value is the number of times Orion NPM will retry a failed SNMP request, defined as any SNMP request that does not receive a response within the SNMP Timeout defined above.

- e. Position the slider or type a value to set the **Hop Count**.

Note: If the Hop Count is greater than zero, Orion NPM searches for devices connected to any discovered device. Each connection to a discovered device counts as a hop.

- f. Position the slider or type a value to set the **Discovery Timeout**.

Note: The Discovery Timeout is the amount of time, in minutes, Orion NPM is allowed to complete a network discovery. If a discovery takes longer than the Discovery Timeout, the discovery is terminated.

- 12. If you only want to use SNMP to discover devices on your network, check Use SNMP only.**

Note: By default, Network Sonar uses ICMP ping requests to locate devices.

- 13. If multiple Orion polling engines are available in your environment, select the Polling Engine you want to use for this discovery.**

- 14. Click Next.**

- 15. If you want the discovery you are currently defining to run on a regular schedule, select either Custom or Daily as the discovery Frequency, as shown in the following steps:**

Notes:

- Scheduled discovery profiles should not use IP address ranges that include nodes with dynamically assigned IP addresses (DHCP).
 - Default Discovery Scheduling settings execute a single discovery of your network that starts immediately, once you click **Discover**.
 - Results of scheduled discoveries are maintained on the Scheduled Discovery Results tab of Network Discovery. For more information about managing scheduled discovery results, see “Managing Scheduled Discovery Results” on page 32.
- a. **If you want to define a Custom discovery schedule to perform the currently defined discovery repeatedly in the future, select Custom and then provide the period of time, in hours, between discoveries.**

- b. If you want your scheduled discovery to run once daily**, select **Daily**, and then provide the time at which you want your discovery to run every day, using the format `HH:MM AM/PM`.
- 16. If you do not want to run your network discovery at this time**, select **No, don't run now**, and then click **Save** or **Schedule**, depending on whether you have configured the discover to run once or on a schedule, respectively.
- 17. Click Discover** to start your network discovery.

Note: Because some devices may serve as both routers and switches, the total number of Nodes Discovered may be less than the sum of reported Routers Discovered plus reported Switches Discovered.

Using the Network Sonar Results Wizard

The Network Sonar Results Wizard directs you through the selection of network devices for monitoring, and it opens whenever discovery results are requested, either when the Network Sonar Wizard completes or when either **Import All Results** or **Import New Results** is clicked for a selected discovery. For more information, see “Network Discovery Using the Network Sonar Wizard” on page 25.

The following steps detail the process of selecting discovered devices, interfaces, and volumes for monitoring in Orion NPM.

To select the results of a network discovery for monitoring in Orion NPM:

- 1.** On the Device Types to Import page, check the device types you want Orion NPM to monitor, and then click **Next**.

Note: If you are not sure you want to monitor a specific device type, check the device type in question. If, later, you do not want to monitor a selected device, simply delete the device using Web Node Management. For more information, see “Managing Devices in the Web Console” on page 77.

- 2.** On the Interface Types to Import page, check the interface types you want Orion NPM to monitor, and then click **Next**.

Note: If you are not sure you want to monitor a specific interface type, check the interface type in question. If, later, you do not want to monitor a selected interface, delete it using Web Node Management. For more information, see “Managing Devices in the Web Console” on page 77.

- 3.** On the Volume Types to Import page, check the volume types you want Orion NPM to monitor, and then click **Next**.

Note: If you are not sure you want to monitor a specific volume type, check the volume type in question. If, later, you do not want to monitor any volume

of the selected type, delete the volume using Web Node Management. For more information, see “Managing Devices in the Web Console” on page 77.

4. ***If you want to import nodes, even when they are already known to be polled by another polling engine***, check the option in the **Allow Duplicate Nodes** section. For more information about working with multiple polling engines, see “Managing Orion NPM Polling Engines” on page 99.
5. Check valid states for imported interfaces on the Import Settings page, and then click **Next**.

Note: By default, Orion NPM imports interfaces that are discovered in an **Operationally Up** state. However, because interfaces may cycle off and on intermittently, the Import Settings page allows you to select interfaces found in **Operationally Down** or **Shutdown** states for import, as well.

6. Confirm that the devices, interfaces, and volumes you want to monitor are checked on the Import Preview page, and then click **Import**.
7. After the import completes, click **Finish**.

Note: Imported devices display in the All Nodes resource.

Importing a List of Nodes Using a Seed File

Orion NPM provides a Specific Nodes option in the Network Discovery Wizard that may be used to import devices from a seed file. The following procedure details how the Specific Nodes option is used with a seed file to import devices in the Orion database.

To import devices from a seed file:

1. Open your seed file.
2. Click **Start > All Programs > SolarWinds Orion > Configuration and Auto-Discovery > Network Discovery**.
3. Click **Add New Discovery**.
4. ***If you need to supply new SNMP credentials to discover the devices in your seed file***, click **Add New Credential**, provide the required information, and then click **Add**. For more information, see “Network Discovery Using the Network Sonar Wizard” on page 25.
5. ***If you intend to import known ESX servers and you need to supply new ESX credentials to discover these servers in your seed file***, complete the following steps on the Local ESX Credentials for VMware view:
 - a. Check **Poll for ESX**.
 - b. Click **Add ESX Credential**.

- c. Provide the required information, and then click **Add**.

Note: For more information, see “Network Discovery Using the Network Sonar Wizard” on page 25.

6. Click **Next**, and then click **Specific Nodes** in the Selection Method menu.
7. Copy and then paste the IP addresses or hostnames of the devices you want Orion NPM to discover from your seed file into the provided field.
Note: Type only one IPv4 address or hostname per line.
8. Click **Validate** to confirm that the provided IP addresses and hostnames are assigned to SNMP-enabled devices.
9. *If you have provided all the IP addresses and hostnames you want to discover*, click **Next**.
10. Complete the Network Discovery and Network Discovery Results Wizards. For more information, see “Network Discovery Using the Network Sonar Wizard” on page 25.

Managing Scheduled Discovery Results

The Scheduled Discovery Results tab of Network Discovery provides a list of all recently discovered, changed, or imported devices on your monitored network. Results are compared between discoveries, and results are listed on this tab. The following procedure provides guidelines for managing discovery results.

To manage scheduled discovery results:

1. Click **Start > All Programs > SolarWinds Orion > Configuration and Auto-Discovery > Network Discovery**.
2. Click **Scheduled Discovery Results**.
3. Select the type of devices you want to view from the Status menu in the left pane. The following options are available:
 - Select **Found** to view all devices discovered by a scheduled discovery.
 - Select **Changed** to view all devices that have changed between recent scheduled discoveries. Changes include the addition of interfaces and device configuration changes.
 - Select **Imported** to view all devices you have recently imported into Orion NPM. For more information about importing devices, see “Using the Network Sonar Results Wizard” on page 30.
 - Select **Ignored** to view all devices you have added to your Discovery Ignore List. For more information about the Discovery Ignore List, see “Using the Discovery Ignore List” on page 33.

- Select **Found and Changed** to view a combined list of all devices found or changed as described above.
 - Select **All except Ignored** to view all discovered, changed or imported devices you have not already designated as Ignored, as detailed above.
4. ***If you want to apply a grouping criterion to organize your listed results,*** select an appropriate criterion from the Group by menu in the left pane.
 5. ***If there are changed or discovered nodes in the results list that you want to update your Orion database to include,*** check all nodes to update or add, and then click **Import Nodes**.
 6. ***If there are devices you want Orion NPM to ignore in future discoveries, regardless of discovered updates or changes,*** check all nodes to ignore, and then click **Add to Ignore List**. For more information about the Discovery Ignore List, see “Using the Discovery Ignore List” on page 33.

Using the Discovery Ignore List

Often, devices are found during a network discovery that you never intend to monitor with Orion NPM. The Discovery Ignore List is a record of all such devices on your network. By placing a device on the Discovery Ignore List you can minimize the SNMP processing load associated with discovering devices that you never intend to monitor.

To manage devices on the Discovery Ignore List:

1. Click **Start > All Programs > SolarWinds Orion > Configuration and Auto-Discovery > Network Discovery**.
2. ***If you want to view the current Discovery Ignore List,*** click **Discovery Ignore List**.
3. ***If you want to add devices to the Discovery Ignore List,*** complete the following procedure:
 - a. Click **Scheduled Discovery Results**.
 - b. Check devices you want to ignore, and then click **Add to Ignore List**.
4. ***If you want to remove devices from the Discovery Ignore List,*** complete the following procedure:
 - a. Click **Scheduled Discovery Results**, and then
 - b. Check the devices you want to remove from the list.
 - c. Click **Remove from Ignore List**.
 - d. Confirm that you want to stop ignoring selected items by clicking **OK**.

Chapter 4

Managing the Orion Web Console

The Orion Web Console is an integral part of the Orion family of products that can be configured for viewing from virtually any computer connected to the Internet. You can also customize the web console interface for multiple users, and individually customized views may be stored as user profiles. Administrator functions are accessed by clicking **Settings** in the top right of all Orion Web Console views.

Logging in for the First Time as an Administrator

When you launch the Orion Web Console, you are presented with a login view requiring both a **User Name** and a **Password**. Log in to the Orion Web Console as shown in the following steps.

To log in to the Orion Web Console:

1. Launch the Orion Web Console using either of the following methods:
 - Click **Start > All Programs > SolarWinds Orion > Orion Web Console**.
 - Or launch a browser on your Orion NPM server and enter `http://ip_address` or `http://hostname`, where `ip_address` is the IP address of your Orion NPM host server, or where `hostname` is the domain name of the server hosting your Orion NPM installation.
2. Enter `Admin` as your **User Name**, and then click **Login**.

Note: Until you set a password, you can log in as `Admin` with no **Password**. After your first login, you may want to change the `Admin` password. For more information, see “Changing an Account Password” on page 38.

Using the Web Console Notification Bar

Below the web console menu bar, the Orion notification bar provides informational messages related to the following Orion NPM features:

- If you have configured the Orion Web Console to store blog posts, new and unread posts to the Orion Product Team Blog are announced in the notification bar. For more information about the Orion Product Team Blog, see “Product Updates” on page 40.
- If you have configured the Orion Web Console to check for product updates, an announcement displays in the notification bar when an update, including any upgrade, service pack, or hotfix, to Orion NPM or any other Orion

modules you currently have installed becomes available. For more information about Orion Product Updates, see “Product Updates” on page 40.

- If you have currently configured a scheduled discovery, results display in the notification bar when the discovery completes. For more information about Scheduled Discovery, see “Discovering and Adding Network Devices” on page 25.
- If you are currently using Orion NPM to monitor any VMware ESX or ESXi Servers, the notification bar can display messages communicating the number of ESX nodes found during any discovery, and, if any discovered ESX nodes require credentials, the notification bar tells you. For more information about managing ESX Servers, see “Monitoring VMware ESX Servers” on page 119.

For more information about any displayed notification bar message, click **More Details** and a web console view relevant to the displayed message opens.

To delete a posted message, either click **Dismiss Message** next to the displayed message, or properly address the situation mentioned in the posted notification.

To remove the notification bar from your web console, click Close (**X**) at the right end of the notification bar.

Navigating the Orion Web Console

The Orion Web Console offers two primary methods of navigation: top-level web console tabs and view-level breadcrumbs. The following sections describe how these navigation methods are used:

- Using Web Console Tabs
- Using Web Console Breadcrumbs

Using Web Console Tabs

In the case of a basic Orion NPM installation, the Orion Web Console displays the following tabs:

Home

The **Home** tab provides a menu bar of links to views aiding you in general network management and monitoring. Information, like events and Top 10 lists, and technologies, like alerts, used to generate the views linked from the Home menu are generally available to all Orion modules. By default, the **Network Summary Home** view displays when you click **Home** from any view in the web console.

Network

The **Network** tab opens a menu bar of links to views and technologies, like wireless network monitoring, that are specific to the features provided by Orion NPM. By default, the **NPM Summary Home** view displays when you click **Home** from any view in the web console.

For each additional Orion module installed in your environment, an additional tab is provided, offering access to views and tools specific to the Orion module added. For more information about additional Orion modules, see “Orion NPM Modules” at www.solarwinds.com. For more information about customizing menu bars, see “Customizing Web Console Menu Bars” on page 59.

Using Web Console Breadcrumbs

As you navigate the views of the Orion Web Console, your location is recorded as a series of links, or breadcrumbs, to the web console views through which you have linked to arrive at your current location. Each breadcrumb offers the following navigation options:

- Clicking a breadcrumb opens the corresponding view directly.
- Clicking **>** next to a breadcrumb opens a clickable list of all other views at the same navigation level in the web console. For example, if you are on a Node Details view, clicking **>** displays a list of other monitored nodes.

Note: Only the first 50 monitored nodes, listed in alphanumeric order by IP address, are displayed.

Dropdown breadcrumb lists are customizable, as shown in the following procedure.

To customize the items in a breadcrumb dropdown:

1. Click **>** at an appropriate level in a breadcrumb to open the dropdown.
2. Click **Customize this list**.
3. Select a criterion from the menu, and then click **Submit**.

Note: All items in the customized breadcrumb list will be identical for the selected criterion.

Administrative Functions of the Orion Web Console

The following sections describe the primary administrative functions performed by an Orion Web Console administrator.

- Changing an Account Password
- Orion Website Administration

- Viewing Secure Data on the Web
- Handling Counter Rollovers

Changing an Account Password

Orion NPM Administrators may change user account passwords at any time, as shown in the following procedure.

To change an account password:

1. Log in to the web console as an administrator.
2. Click **Settings** in the top right corner of the web console.
3. Click **Account Manager** in the Accounts grouping of the Orion Website Administration page.
4. Select the user account with the password you want to change, and then click **Change Password**.
5. Complete the New Password and Confirm Password fields, and then click **Change Password**.
6. Click **Continue** when the password is successfully changed.

Orion Website Administration

If you are logged in to the web console as an administrator, clicking **Settings** in the top right corner of the web console displays the Orion Website Administration page, presenting a variety of tools to control the appearance and delivery of information to Orion Web Console users. The following options are available on the Orion Website Administration page.

Node Management

The Node Management grouping of the Orion Website Administration page gives you access to the following web console node management interfaces:

- Clicking **Manage Nodes** displays the Node Management page, where an Orion NPM administrator can immediately add, view, and manage all network nodes, interfaces, and volumes currently monitored by Orion NPM. For more information, see “Managing Devices in the Web Console” on page 77.
- Clicking **Add a Node** opens the Add Node Wizard directly. For more information about adding nodes individually, see “Adding Devices for Monitoring in the Web Console” on page 78.
- Clicking **VMware Settings** opens the VMware Settings view, where you can view both a list of currently monitored VMware ESX Servers and a library of

the VMware credentials Orion NPM uses to monitor your ESX Servers. For more information, see “Managing VMware Credentials” on page 126.

- Clicking **Network Sonar Discovery** opens the Network Sonar Discovery Wizard. Network Discovery enables you to quickly discover nodes, interfaces and volumes across your entire network for monitoring. For more information about using Network Sonar Discovery, see “Network Discovery Using the Network Sonar Wizard” on page 25.

Accounts

The Accounts grouping of the Orion Website Administration page gives an Orion NPM administrator access to the following web console configuration pages:

- The **Account Manager** allows an Orion NPM administrator to set and change passwords, set user rights and access, and configure the user interface for all Orion Web Console users. For more information about using Account Manager, see “Managing Web Accounts” on page 91.
- The **Account Views** page is a quick-reference view of the states and settings of existing web console user accounts. You can immediately enable or disable an account by clicking its **Account Enabled** icon. Clicking an **Account** user name opens the Account Manager for the selected account. For more information about using Account Manager, see “Managing Web Accounts” on page 91.

Note: All changes made to any account on the Account Views view are effective immediately upon selection.

- Clicking **Account List** opens the Orion Website Accounts view, providing an immediate overview of web console user account settings. You may use this view to make changes to multiple accounts simultaneously and immediately by clicking to check or clear options. Clicking an **Account** user name opens the Account Manager for the selected account. For more information about using Account Manager, see “Managing Web Accounts” on page 91.

Customize

The Customize grouping of the Orion Website Administration page offers options to customize the navigation and appearance of your Orion Web Console on the following pages:

- The **Customize Menu Bars** page allows an Orion Web Console administrator to configure the menu bars seen by individual users. For more information, see “Customizing Web Console Menu Bars” on page 59.
- The **Color Scheme** page gives a web console administrator the ability to select a default color scheme for resource title bars. The color scheme selection takes effect immediately throughout the web console. For more information, see “Changing the Web Console Color Scheme” on page 61.

- The **External Websites** page enables an Orion Web Console administrator to designate any external website as an Orion Web Console view, appearing in the Views toolbar. For more information, see “Creating and Editing External Website Views” on page 59.

Product Updates

The Product Updates grouping provides links to web console views offering up-to-date information about using and upgrading Orion NPM.

- The **Available Product Updates** view allows you to configure regular checks for Orion NPM updates that can include version upgrades and service packs.
- The **Orion Product Team Blog** offers regular posts from members of the Orion product team to help you take full advantage of features provided by Orion NPM and its modules.

Views

The Views grouping of the Orion Website Administration page gives an Orion Web Console administrator access to the following view configuration pages:

- The **Manage Views** page enables a web console administrator to add, edit, copy, or remove individual web console views. For more information about managing Orion Web Console views, see “Customizing Views” on page 46.
- The **Views by Device Type** page gives an Orion Web Console administrator the ability to designate default views for network nodes and interfaces. For more information, see “Views by Device Type” on page 49.

Settings

The Settings grouping of the Orion Website Administration page gives an Orion NPM administrator access to the following settings configuration pages:

- **Web Console Settings** allow an Orion Web Console administrator to customize the function and appearance of both the Orion Web Console and the charts that are displayed as resources in Orion Web Console views. For more information about configuring Orion Web Console and Chart Settings, see “Orion Web Console and Chart Settings” on page 63.
- **Polling Settings** define the configuration of polling intervals, timeouts, statistics calculations, and database retention settings for your Orion NPM polling engine. For more information about configuring Orion Polling Settings, see “Orion Polling Settings” on page 101.
- The **Orion** and **NPM Thresholds** pages open the Orion General Thresholds and Network Performance Monitor Thresholds pages, respectively, where Orion NPM threshold settings are configured. For more information, see “Orion Network Performance Monitor Thresholds” on page 43.

If you currently have any Orion modules installed, links to the respective module settings pages display in the Settings grouping. For more information about configuring Orion modules, see the Administrator Guide for your Orion module.

Details

The Details grouping of the Orion Website Administration page provides links to the following pages containing information about your Orion NPM installation:

Database Details

This is an information-only page that displays details about the SQL Server database currently used by your Orion NPM installation. In addition to current version information and configuration settings for both your Orion NPM server and your database server, this page displays the total number of monitored elements, nodes, interfaces, and volumes in the Orion database.

Polling Engines

Orion NPM supports the implementation of multiple distributed polling engines. Each engine can monitor and collect data from different parts of your network. This page shows the status and selected configuration information for each currently operational polling engine.

License Details

This is an information-only page that displays details about both your Orion NPM license and your monitored network. This page also shows the version of the Orion Network Performance Monitor applications that you are running and the versions of associated DLLs. For more information about managing your license, see “Maintaining Licenses with License Manager” on page 22.

Modules Details

This information-only page provides version and service pack level information for all Orion modules you currently have installed. For more information about Orion modules, see the Administrator Guide for your module. Online versions of Orion module administrator guides are available on the SolarWinds website, as follows:

- Orion Network Performance Monitor documentation
- Orion Modules documentation

Viewing Secure Data on the Web

In the interest of security, sensitive network information, such as community strings, logins, and passwords, is not viewable in the web console. However, if you have secured your network, you may check **Allow Secure Data On Web**

(advanced) in the Calculations & Thresholds area of the Orion Polling Settings page to allow the passage of community strings through the web console.

Note: This setting does not affect the display of custom reports that you export to the web. For more information see “Creating Reports” on page 185.

Handling Counter Rollovers

The Counter Rollover setting configures Orion NPM to properly handle counter rollovers. Orion NPM is capable of handling either 32-bit or 64-bit counters, but, by default, Orion NPM assumes counters are 32-bit. 32-bit counters have a maximum value of 2^{32} , or 4,294,967,296, and 64-bit counters, if they are supported by your network devices, have a maximum value of 2^{64} , or 18,446,744,073,709,551,616.

Note: The 32-bit counters option is designated as Method 1 in the Counter Rollover field on the Orion Polling Settings page.

The following procedure designates the type of counter-handling used by Orion NPM.

To designate the type of counter-handling used by Orion NPM:

1. Log in to the web console as an administrator.
2. Click **Settings** in the top right of the web console.
3. Click **Polling Settings** in the Settings grouping of the Orion Website Administration page.
4. **If you are using 64-bit counters**, select **Method 2** in the Counter Rollover field in the Calculations & Thresholds area.

Notes:

- If **Method 2** is selected, Orion NPM will intentionally skip a poll if a polled value is less than the previous polled value to permit counting to 2^{64} .
 - Orion NPM fully supports the use of 64-bit counters; however, these 64-bit counters can exhibit erratic behavior in some implementations. If you notice peculiar results when using these counters, disable the use of 64-bit counters for the problem device and contact the device manufacturer.
5. **If you are using of 32-bit counters**, select **Method 1** in the Counter Rollover field in the Calculations & Thresholds area.

Note: If Method 1 is selected, when a rollover is detected, the time between polls is calculated as $(2^{32} - \text{Last Polled Value}) + \text{Current Polled Value}$.

Orion Network Performance Monitor Thresholds

Many of the resources available in the Orion Web Console are capable of displaying error and warning conditions for the devices on your network. Errors and warnings display in the Orion Web Console Orion NPM uses the values provided on the thresholds pages to determine when and how to display errors and warnings in the Orion Web Console. The following sections provide more information about threshold types and configuration:

- Orion General Threshold Types
- Network Performance Monitor Threshold Types
- Setting Orion NPM Thresholds

Orion General Threshold Types

The following device condition thresholds are available for configuration as Orion General Thresholds:

CPU Load

Monitored network devices experiencing CPU loads higher than the value set for the **High Level** display in High CPU Load reports and resources. Gauges for these devices also display as bold red. Monitored network devices experiencing a CPU load higher than the value set for the **Warning Level**, but lower than the value set for the **High Level**, display as red in High CPU Load reports and resources. Gauges for these devices also display as red.

Disk Usage

Monitored network devices experiencing a disk usage higher than the value set for the **High Level** display as bold red in Disk Usage reports and resources. Monitored network devices experiencing a disk usage higher than the value set for the **Warning Level**, but lower than the value set for the **High Level**, display as red in High Disk Usage reports and resources.

Percent Memory Used

Monitored network devices experiencing a percent memory usage higher than the value set for the **Error Level** display in High Percent Utilization reports and resources. Gauges for these devices also display as bold red. Monitored network devices experiencing a percent memory usage higher than the value set for the **Warning Level**, but lower than the value set for the **Error Level**, display in High Percent Utilization reports and resources. Gauges for these devices also display as red.

Percent Packet Loss

Monitored network devices experiencing a percent packet loss higher than the value set for the **Error Level** display in High Percent Loss reports and resources. Gauges for these devices also display as bold red. Monitored network devices experiencing a percent packet loss higher than the value set for the **Warning Level**, but lower than the value set for the **Error Level**, display in High Percent Loss reports and resources. Gauges for these devices also display as red.

Orion NPM calculates percent packet loss using ICMP ping requests made on the Default Poll Interval. Orion NPM pings monitored devices and records the results of the ten most recent ping attempts. Percent packet loss is expressed as the number of failed ping requests, X, divided by the number of ping requests, 10. For more information about the Default Poll Interval, see “Orion Polling Settings” on page 101.

For example, if, at a given point in time, the last ten ping requests made of a selected device resulted in 2 failures and 8 successes, the percent packet loss for the selected device at the given time is reported as 2/10, or 20%.

Response Time

Monitored devices experiencing response times longer than the value set for the **Error Level** display in High Response Time reports and resources. Gauges for these devices also display as bold red. Devices experiencing response times longer than the value set for the **Warning Level**, but shorter than the value set for the **Error Level**, also display in High Response Time reports and resources. Gauges for these devices also display as red.

Orion NPM calculates response time using ICMP ping requests made on the Default Node Poll Interval. Orion NPM pings monitored devices and records the results of the ten most recent ping attempts. Average Response Time is expressed as the average response time of these last 10 ping requests. If Orion NPM does not receive a ping response within the Default Poll Interval, Orion NPM will attempt to ping the nonresponsive device once every 10 seconds for the period designated as the Warning Interval. For more information, see “Orion Polling Settings” on page 101.

Network Performance Monitor Threshold Types

The following device condition thresholds are available for configuration as Network Performance Monitor thresholds:

Cisco Buffer Misses

Many Cisco devices can report buffer misses. Monitored network devices with more buffer misses than the value set for the **High Level** display as bold red in Cisco Buffer resources. Monitored network devices with more buffer

misses than the value set for the **Warning Level**, but fewer than the value set for the **High Level**, display as red in Cisco Buffer resources.

Interface Errors and Discards

Monitored interfaces experiencing more errors and discards than the value set for the **Error Level** display as bold red in High Errors and Discards reports and resources. Monitored interfaces experiencing more errors and discards than the value set for the **Warning Level**, but fewer than the value set for the **Error Level**, display as red in High Errors and Discards reports and resources.

Interface Percent Utilization

Monitored interfaces experiencing current percent utilization higher than the value set for the **High Level** display in High Percent Utilization reports and resources. Gauges for these devices also display as bold red. Monitored interfaces experiencing current percent utilization higher than the value set for the **Warning Level**, but lower than the value set for the **High Level**, display in High Percent Utilization reports and resources. Gauges for these devices also display as red.

Setting Orion NPM Thresholds

The following procedure opens the Network Performance Monitor Thresholds page for configuration.

To set Orion NPM thresholds:

1. Log in to the Orion Web Console as an administrator.
2. Click **Settings** in the top right of the web console.
3. *If you want to edit Orion General thresholds*, click **Orion Thresholds** in the Settings grouping of the Orion Website Administration page.

Note: For more information about Orion General thresholds, see “Orion General Threshold Types” on page 43.

4. *If you want to edit Network Performance Monitor thresholds*, click **NPM Thresholds** in the Settings grouping of the Orion Website Administration page.

Note: For more information about Network Performance Monitor thresholds, see “Network Performance Monitor Threshold Types” on page 44.

5. Provide appropriate values for **Error Level**, **High Level**, or **Warning Level** for selected thresholds.

Customizing Views

Orion Web Console views are configurable presentations of network information that can include maps, charts, summary lists, reports, events, and links to other resources. Customized views can then be assigned to menu bars.

Creating New Views

You can customize the Orion Web Console for individual users by logging in as an administrator and creating new views as shown in the following procedure.

To create a new view:

1. Click **Settings** in the top right of the web console, and then click **Manage Views** in the Views grouping of the Orion Website Administration page.
2. Click **Add**.
3. Enter the **Name of New View**, and then select the **Type of View**.

Note: The **Type of View** selection affects how the view is made accessible to users, and your choice may not be changed later. For more information, see “Views by Device Type” on page 49.

4. Click **Submit**.

After you have created a new view, the *Customize YourView* page opens. For more information, see “Editing Views” on page 46.

Editing Views


The Orion Web Console allows administrators to configure views for individual users. The following steps are required to configure an existing view.

To edit an existing view:

1. Click **Settings** in the top right of the web console.
2. Click **Manage Views** in the Views grouping of the Orion Website Administration page.
3. Select the view you want to customize from the list, and then click **Edit**.
4. **If you want to change the column layout of your view**, click **Edit** to the right of the column widths, and then configure the column layout of your view as follows:
 - a. Select the number of columns under **Layout**.
 - b. Provide the width, in pixels, of each column in the appropriate fields..
 - c. Click **Submit**.

5. **If you want to add a resource**, repeat the following steps for each resource:

Notes:

- Resources already in your view will not be checked on this page, as it is a view of all web console resources. It is, therefore, possible to pick duplicates of resources you are already viewing.
 - Several options on the Add Resources page are added to the list of resources for a page, but the actual configuration of a given map, link, or code is not added until the page is previewed.
 - Some resources may require additional configuration. For more information, see “Resource Configuration Examples” on page 49.
- a. Click **+** next to the column in which you want to add a resource.
 - b. Click **+** next to a resource group on the Add Resources page to expand the resource group, displaying available resources.
 - c. Check all resources you want to add.
 - d. **If you have completed the addition of resources to the selected view**, click **Submit**.
6. **If you want to delete a resource from a column**, select the resource, and then click **X** next to the resource column to delete the selected resource.
7. **If you want to copy a resource in a column**, select the resource, and then click  next to the resource column to delete the selected resource.
8. **If you want to rearrange the order in which resources appear in your view**, select resources, and then use the arrow keys to rearrange them.
9. **If you have finished configuring your view**, click **Preview**.
- Note:** A preview of your custom web console displays in a new window. A message may display in the place of some resources if information for the resource has not been polled yet. For more information, see “Resource Configuration Examples” on page 49.
10. Close the preview window.
11. **If you are satisfied with the configuration of your view**, click **Done**.

Notes:

- For more information about adding a customized view to menu bars as a custom item, see “Customizing Web Console Menu Bars” on page 59.
- For more information about assigning your customized view as the default view for a user, see “Editing User Accounts” on page 92.

Configuring View Limitations

As a security feature, the web console gives administrators the ability to limit the types of devices displayed on any selected view. The following view limitations are defined by default:

Orion Web Console View Limitations		
Single Network Node	Group of Nodes	Single Machine Type
Node Name Pattern	System Name Pattern	IP Address Pattern
Machine Type Pattern	Group of Machine Types	Single Interface
Hardware Manufacturer	Device Status	Interface Status
System Location	System Location Pattern	Interface Type
System Contact	System Contact Pattern	Single Hardware Manufacturer
Group of Volumes	Group of Interfaces	Interface Name Pattern
Interface Alias Pattern		

The following procedure configures a view limitation.

To enable a view limitation:

1. Click **Settings** in the top right of the web console.
2. Click **Manage Views** in the Views grouping of the Orion Website Administration page.
3. Select the view to which you want to add a limitation, and then click **Edit**.
4. In the View Limitation area of the Customize *View* page, click **Edit**.
5. Select the type of view limitation you want to apply, and then click **Continue**.
6. Provide or check appropriate strings or options to define the device types to include or exclude from the selected view, and then click **Submit**.

Note: The asterisk (*) is a valid wildcard. Pattern limitations restrict views to devices for which the corresponding fields include the provided string.

Copying Views

When you want to create multiple views based on the same device type, copying views allows you to create one view, and then use that view as a template to create other new views. The following steps copy an existing view.

To copy a view:

1. Click **Settings** in the top right of the web console.
2. Click **Manage Views** in the Views grouping of the Orion Website Administration page.

3. Select the view you want to copy, and then click **Copy**.
4. *If you want to edit a copied view*, follow the procedure in the “Editing Views” section on page 46.

Deleting Views

The following steps delete an existing view.

To delete an existing view:

1. Click **Settings** in the top right of the web console, and then click **Manage Views** in the Views grouping of the Orion Website Administration page.
2. Select the view you want to delete, and then click **Delete**.

Views by Device Type

There are vast differences among network devices and the statistics they report, but the Orion Web Console can make it easier to view network data by displaying node and interface details by device type, giving you the ability to have a different view for each unique type of device you have on your network, including routers, firewalls, and servers. The following steps assign a view by either Nodes or Interfaces.

To assign a view by device type:

1. Click **Settings** in the top right of the web console, and then click **Views by Device Type** in the Views grouping of the Orion Website Administration page.
2. Select available Web Views for the different types of devices that Orion NPM is currently monitoring on your network.
3. Click **Submit**.

Resource Configuration Examples

Several resources that may be selected from the Add Resources page require additional configuration. Included in this section are examples of these resources and the steps that are required for their proper configuration.

Selecting a Network Map

Network maps created with Orion Network Atlas can give a quick overview of your network, right from the main web console view. For more information about creating maps, see “Creating Network Maps” on page 183.

Note: Clicking the resource title in the title bar menu displays the resource by itself in a browser window.

The following procedure adds a network map to the Orion Web Console.

To add a network map to the web console:

1. Create a new view or edit an existing view.
Note: For more information, see “Customizing Views” on page 46.
2. Select the view to which you want to add the map, and then click **Edit**.
3. Click **+** next to the view column in which you want to display the new map.
4. Click **+** next to **Network Maps**, check **Network Map**, and then click **Submit**.
5. Click **Preview** on the Customize *YourView* page.
6. Click **Edit** in the Network Map resource title bar.
7. **If you do not want to use the default title provided**, enter a new **Title** for the title bar of the added map.
8. **If you want a subtitle**, enter a new **Subtitle** for the added map.
Note: Titles and subtitles may be entered as either text or HTML.
9. Select from the list of available maps.
10. Select the **Scale** at which you want to display the map.
Note: If you leave the **Scale** field blank, the map will display at full scale, based on the size of the column in which the map displays.
11. Click **Submit**.

Displaying a List of Objects on a Network Map

When your web console view includes a network map, it can be helpful to maintain a list of network objects that appear on the map. The following procedure enables a resource listing network map objects.

Note: Clicking the resource title displays the resource in a new browser window.

To display a list of network map objects:

1. Create a new view or edit an existing view.
Note: For more information, see “Customizing Views” on page 46.
2. Select the view to display the list of network map objects, and then click **Edit**.
3. Click **+** next to the view column in which you want to display the new list of network map objects.
4. Click **+** next to **Network Maps**, check **List of Objects on Network Map**, and then click **Submit**.

5. Click **Preview** on the Customize *YourView* page.
6. Click **Edit** in the title bar of the List of Objects on Network Map resource.
7. **If you do not want to use the default title provided**, enter a new **Title** for the header of the objects list.
8. **If you want a subtitle**, enter a new **Subtitle** for the added objects list.
Note: Titles and subtitles may be entered as either text or HTML.
9. Select from the list of available maps for the objects that you want to populate your list, and then click **Submit**.

Displaying a Custom List of Maps

The web console allows you to populate a custom view with a list of available network maps. Each map in your custom list, when clicked, opens in a new window. The following procedure enables a custom network maps list resource.

Note: Clicking the resource title displays the resource in its own browser window.

To display a custom list of maps:

1. Create a new view or edit an existing view.
Note: For more information, see “Customizing Views” on page 46.
2. Select the view to which you want to add the custom list of network maps, and then click **Edit**.
3. Click **+** next to the view column in which you want to display the custom list of network maps.
4. Click **+** next to **Network Maps**.
5. Check **Custom List of Maps**, and then click **Submit**.
6. Click **Preview** on the Customize *YourView* page, and then click **Edit** in the title bar of the Custom List of Maps resource.
7. **If you do not want to use the default title provided**, enter a new **Title** for the header of the maps list.
8. **If you want a subtitle**, enter a new **Subtitle** for the custom list of maps.
Note: Titles and subtitles may be entered as either text or HTML.
9. Check the maps you want to include in your maps list.
10. Click **Submit**.

Displaying an Event Summary - Custom Period of Time

You may want your web console view to display an event summary for a specified period of time. The following procedure details the steps to include an event summary in your web console.

Note: Clicking the resource title in the title bar menu displays the resource by itself in a browser window.

To display an event summary:

1. Create a new view or edit an existing view.

Note: For more information about creating a new view or editing an existing view, see “Customizing Views” on page 46.

2. Select the view to include the event summary, and then click **Edit**.
3. Click **+** next to the view column that will display the event summary.
4. Click **+** next to **Events**.
5. Check **Event Summary – Custom Time Period**, and then click **Submit**.
6. Click **Preview** on the Customize *YourView* page.
7. Click **Edit** in the title bar of the Event Summary resource.
8. **If you do not want to use the default title provided**, enter a new **Title** for the header of the event summary.
Note: Titles may be entered as either text or HTML.
9. Select the time period for displaying events from **Display Events for the following Time Period**.
10. Click **Submit**.

Specifying User-Defined Links

The User-Defined Links option may be used to create quick access to external websites or customized views. URLs of your customized views can be copied from their preview pages and pasted in a User-Defined Links field. The following steps enable user-defined links from within your web console.

Note: Clicking the resource title in the title bar menu displays the resource by itself in a browser window.

To enable a user-defined links resource:

1. Create a new view or edit an existing view.
Note: For more information, see “Customizing Views” on page 46.
2. Select the view to which you want to add the user-defined links resource.

3. Click **Edit**.
4. Click **+** next to the view column to display the user-defined links resource.
5. Click **+** next to **Miscellaneous**
6. Check **User Defined Links**.
7. Click **Submit**.
8. Click **Preview** on the Customize *YourView* page.
9. Click **Edit** in the title bar of the User Defined Links resource.
10. **If you do not want to use the default title provided**, enter a new **Title** for the links list.
11. **If you want a subtitle**, enter a new **Subtitle** for the links list.
Note: Titles and subtitles may be entered as either text or HTML.
12. Enter the following information for each link you want to define:
 - a. A link **Name** and the **URL** of your link.
 - b. **If you want your links to open in a new browser window**, check **Open in New Window**.
13. Click **Submit**.

Specifying Custom HTML or Text

In situations where you have static information that you want to provide in the web console, use the **Custom HTML or Text** option. The **Custom HTML or Text** option may also be used to create quick access to your customized views. The following procedure will create a static content area within your web console for displaying text or HTML content.

Note: Clicking the resource title displays the resource in a new browser window.

To specify custom HTML or text:

1. Create a new view or edit an existing view.
Note: For more information, see “Customizing Views” on page 46.
2. Select the view to include the custom HTML or text.
3. Click **Edit**.
4. Click **+** next to the column to display the custom HTML or text.
5. Click **+** next to **Miscellaneous**, and then check **Custom HTML or Text**.
6. Click **Submit**.
7. Click **Preview** on the Customize *YourView* page.

8. Click **Edit** in the title bar of the Custom HTML or Text resource.
9. **If you do not want to use the default title provided**, enter a new **Title** for the specified content area.
10. **If you want a subtitle**, enter a new **Subtitle** for the specified content area.
Note: Titles and subtitles may be entered as either text or HTML.
11. Enter content as either text or HTML into the **Raw HTML** field.
12. Click **Submit**.

Specifying an Orion Network Performance Monitor Report

The web console is able to incorporate reports that you have created in Orion Report Writer into any view. The following procedure will take a report that you have created with Report Writer and include it within a web console view.

Note: Clicking the resource title in the title bar menu displays the resource by itself in a browser window.

To include an Orion NPM report:

1. Create a new view or edit an existing view.
Note: For more information, see “Customizing Views” on page 46.
2. Select the view to which you want to add the report.
3. Click **Edit**.
4. Click **+** next to the view column in which you want to display the report.
5. Click **+** next to **Report Writer**.
6. Check **Report from Orion Report Writer**.
7. Click **Submit**.
8. Click **Preview** on the Customize *YourView* page.
9. Click **Edit** in the title bar of the Report from Orion Report Writer resource.
10. **If you do not want to use the default title provided**, enter a new **Title** for the included report.
11. **If you want a subtitle**, enter a new **Subtitle** for the included report.
Note: Titles and subtitles may be entered as either text or HTML.
12. **Select a Report** to include.

13. **If you want to add a filter to the included report**, enter an appropriate query in the **Filter Nodes** field.

Note: **Filter Nodes** is an optional, advanced, web console feature that requires some knowledge of SQL queries. Click **+** next to **Show Filter Examples** to view a few example filters.

14. Click **Submit**.

Displaying a Custom List of Reports

The web console allows you to populate a custom view with a custom reports list. When clicked from the list, each report opens in a new window. The following procedure details the steps required to enable a custom list of network reports.

Note: Clicking the resource title displays the resource in a new browser window.

To display a custom list of reports:

1. Create a new view or edit an existing view. For more information, see “Customizing Views” on page 46.
2. Select the view to which you want to add the custom list of reports, and then click **Edit**.
3. Click **+** next to the column to display the custom list of reports.
4. Click **+** next to **Report Writer**.
5. Check **Custom List of Reports**, and then click **Submit**.
6. Click **Preview** on the **Customize *YourView*** page, and then click **Edit** in the title bar of the Report from Orion Report Writer resource.
7. **If you do not want to use the default title provided**, enter a new **Title** for the header of the reports list.
8. **If you want a subtitle**, enter a new **Subtitle** for the custom list of reports.
Note: Titles and subtitles may be entered as either text or HTML.
9. Check the reports that you want to include in your custom list of reports.
Note: To allow a user to view a report included in the custom list, you must set the report access for the account. For more information, see “Configuring an Account Report Folder” on page 96.
10. Click **Submit**.

Filtering Nodes

Your Orion Web Console can maintain a customizable node list for your network. Node lists may be configured for specific views using SQL query filters. The following steps set up node filtering for node lists included in web console views.

Note: Clicking the resource title displays the resource in a new browser window.

To enable filtering on a node list:

1. Create a new view or edit an existing view.

Note: For more information, see “Customizing Views” on page 46.

2. Select the view to which you want to add the node list
3. Click **Edit**.
4. Click **+** next to the view column in which you want to display the node list.
5. Click **+** next to **Node Lists**.
6. Check **All Nodes – Table**.
7. Click **Submit**.
8. Click **Preview** on the **Customize** *YourView* page, and then
9. Click **Edit** in the title bar of the All Nodes – Table resource.
10. **If you do not want to use the default title provided**, enter a new **Title** for the node list.
11. **If you want a subtitle**, enter a new **Subtitle** for the node list.

Note: Titles and subtitles may be entered as either text or HTML.

12. **If you want to filter your node list by text or IP address range**, provide the text or IP address range by which you want to filter your node list in the Filter Text field, as shown in the following examples:
 - Type `Home` in the Filter Text field to list all nodes with “Home” in the node name or as a location.
 - Type `192.168.1.*` in the Filter Text field to list all nodes in the 192.168.1.0-255 IP address range.
13. Select the property that is appropriate to the filter text provided above, as shown in the following examples:
 - **If you typed** `Home` **in the Filter Text area**, select **Node Name** or **Location** to list nodes with “Home” in the node name or as a location.
 - **If you typed** `192.168.1.*` **in the Filter Text area**, select **IP Address** to list only nodes in the 192.168.1.0-255 IP address range.

14. *If you want to apply a SQL filter to the node list*, enter an appropriate query in the **Filter Nodes (SQL)** field.

Notes:

- **Filter Nodes (SQL)** is an optional, advanced, web console feature that requires some knowledge of SQL queries. Click **+** next to **Show Filter Examples** to view a few example filters.
- By default, node list resources are designed to sort nodes alphabetically by node caption. This configuration can not be overwritten using a SQL filter, so `order by` clauses included in SQL filters are redundant and will result in Custom SQL filter formatting errors.

15. Click **Submit**.

Grouping Nodes

Your Orion Web Console can maintain a customizable node list for your network. Node lists may be configured for specific views with node grouping. The following steps set up node grouping for node lists included in web console views.

Note: Clicking the resource title in the title bar menu displays the resource by itself in a browser window.

To enable grouping on a node list:

1. Create a new view or edit an existing view.

Note: For more information, see “Customizing Views” on page 46.

2. Select the view to which you want to add the node list, and then click **Edit**.

3. Click **+** next to the view column in which you want to display the node list.

4. Click **+** next to **Node Lists**.

5. Check **All Nodes – Tree**, **All Nodes – Tree (AJAX)**, or **All Nodes – Tree (Non-AJAX)**, and then click **Submit**.

6. Click **Preview** on the **Customize *YourView*** page.

7. Click **Edit** in the title bar of the All Nodes – Tree (AJAX) resource.

8. *If you do not want to use the default title provided*, enter a new **Title** for the node list.

9. *If you want a subtitle*, enter a new **Subtitle** for the node list.

Note: Titles and subtitles may be entered as either text or HTML.

10. Select up to three criteria, in specified levels, for **Grouping Nodes** within your web console view.

11. **If you want to apply a SQL filter to the node list**, enter an appropriate query in the **Filter Nodes** field.

Notes:

- **Filter Nodes (SQL)** is an optional, advanced, web console feature that requires some knowledge of SQL queries. Click **+** next to **Show Filter Examples** to view a few example filters.
- By default, node list resources are designed to sort nodes alphabetically by node caption. This configuration can not be overwritten using a SQL filter, so `order by` clauses included in SQL filters are redundant and will result in Custom SQL filter formatting errors.

12. Click **Submit**.

Adding a Service Level Agreement Line to Charts

The Orion Web Console can display a service level agreement (SLA) line on any Min/Max/Average bps chart. When you add a customer property named “SLA” and populate the field with your device SLA values, the Orion Web Console will display the appropriate line on your charts.

Note: The SLA line may not appear immediately. It may take several minutes for the change to be detected by the Orion NPM web engine.

To add a Service Level Agreement line to Min/Max/Average bps charts:

1. Click **Start > All Programs > SolarWinds Orion > Grouping and Access Control > Custom Property Editor**.
2. Click **Add Custom Property**.
3. Confirm that **Add Predefined Properties** is selected.
4. Check **SLA** in the list of predefined properties, and then click **OK**.
5. Click **Properties > Edit Interfaces Properties**.
6. Enter the SLA value (in bps) in the **SLA** column for each interface you want to label with SLA values. For example, type `1544000` for a T1 interface (1.544 Mbps) or `225000` for a serial connection running at 225 Kbps.
7. Close the Custom Property Editor.
8. Click **Start > All Programs > SolarWinds Orion > Orion Web Console**.
9. Browse to the Interface Details view of one of the interfaces you edited. The SLA line displays on any chart showing Min/Max/Average bps.

Creating and Editing External Website Views

With the external website view feature, any Orion NPM administrator can select any external website and designate it as an Orion Web Console view, as shown in the following procedure.

To create or edit an external website view in the web console:

1. Click **Settings** in the top right of the web console.
2. Click **External Websites** in the Customize grouping of the Orion Website Administration page.
3. *If you want to delete an existing external website*, click **Delete** next to the website you want to delete, and then click **OK** to confirm the deletion.
4. *If you want to add a new external website*, click **Add**.
5. *If you want to edit an existing external website*, click **Edit** next to the name of the website you want to edit.
6. Provide a **Menu Title** for the external website to display in the Views toolbar.
7. *If you want to include a heading within the view*, provide an optional **Page Title** to display within the view.
8. Provide the **URL** of the external website, in `http://domain_name` format.
9. Select the **Menu Bar** to which you want to add the new external website link.
Note: For more information about customizing menu bars, see “Customizing Web Console Menu Bars” on page 59.
10. Click **OK**.
11. Click **Preview** to view the external website as the web console will display it.

Customizing the Orion Web Console

The following sections provide details for customizing your Orion Web Console:

- Customizing Web Console Menu Bars
- Changing the Web Console Color Scheme
- Changing the Web Console Site Logo

Customizing Web Console Menu Bars

The menu bars displayed at the top of every page may be configured to display various menu items. You can also define menu items and add them to custom menu bars. For more information about customizing menu bars for individual accounts, see “Editing User Accounts” on page 92.

The following procedure customizes a web console menu bar.

To customize web console menu bars:

1. Click **Settings** in the top right of the web console.
2. Click **Customize Menu Bars** in the Customize grouping of the Orion Website Administration page.
3. *If you want to modify an existing menu*, click **Edit** beneath the menu bar you want to modify, and then click and drag items between the Available items list on the left and the Selected items list on the right until the Selected items list includes all the items you want to include in your edited menu.

Note: Hover over any view title to read a description. Selected items display from left to right in the edited menu bar as they are listed from top to bottom.

4. *If you want to create a new menu bar*, complete the following steps:
 - a. Click **New Menu Bar**, and then provide a **Name for the New Menu Bar**.
 - b. Click and drag the buttons you want to include in your new menu bar from the Available items list on the left to their correct relative locations in the Selected items list on the right.

Note: Hover over any view title to read a view description. Selected items display from left to right in the new menu bar as they are listed from top to bottom.

5. *If you want to add menu items*, complete the following steps:
 - a. Click **Edit** under the menu bar to which you are adding the new item.
 - b. Click and drag the items you want to include in your new menu from the Available items list on the left to their correct relative locations in the Selected items list on the right.

Notes:

- Hover over any view title to read a view description. Selected items display from left to right in the new menu bar as they are listed from top to bottom.
- If you check **Reports** from the **Select Menu Items** page, you must also enable reports for the accounts that use the menu bar. For more information, see “Configuring an Account Report Folder” on page 96.

6. *If you want to add a custom menu item*, complete the following steps:
 - a. Click **Edit** under the menu bar to which you are adding the custom item.
 - b. Click **Add**.
 - c. Provide the **Name**, **URL**, and **Description** of your custom menu item.

- d. **If you want the menu option to open in a new window**, check **Open in a New Window**.
 - e. Click **OK**.
7. **If you want to delete a menu item**, click and drag the item to delete from the Selected items list on the right to the Available items list on the left.
Warning: Do not delete the **Admin** option from the Admin menu bar.
 8. **If you want to change the location of an item in your menu**, click and drag items to move them up and down in the Selected items list.
 9. **If you have finished editing your menu bar**, click **Submit**.

Changing the Web Console Color Scheme

The overall color scheme of the Orion Web Console may be changed to any of several color schemes that are viewable by all users, as shown in the following procedure.

To change the web console color scheme:

1. Click **Settings** in the top right of the web console.
2. Click **Color Scheme** in the Customize grouping.
3. Select the desired color scheme, and then click **Submit**.

Changing the Web Console Site Logo

The Orion Web Console can be configured to display your logo instead of the default SolarWinds banner across the top of every web console page. The following steps change the default SolarWinds web console banner.

To change the web console banner:

1. Create an appropriately sized graphic to replace the SolarWinds logo.

Notes:

- The SolarWinds banner file is 271x48 pixels at 200 pixels/inch.
- The SolarWinds.com **End User License Agreement** prohibits the modification, elimination, or replacement of either the SolarWinds.com logo and link on the menu bar or the SolarWinds copyright line at the bottom of the page.

2. Place your graphic in the `images` directory.

Note: By default, it is in `C:\Inetpub\SolarWinds\NetPerfMon\`.

3. Log in to the web console as an administrator.

4. Click **Settings** in the top right of the web console.
5. Click **Web Console Settings** in the Settings grouping of the Orion Website Administration page.
6. Type the new logo image name as a replacement for `SolarWinds.Logo.jpg` in the **Site Logo URL** field.

Configuring the Available Product Updates View

The Orion Web Console can automatically check for the availability of any updates to your currently installed Orion products. By default, the web console regularly checks for product updates automatically, as indicated by the dates and times reported as **Last Check** and **Next Check**, but you can click **Check Now** at any time to see an up-to-the-minute update. If updates are available, a note is posted in the web console notification bar and updates are listed in this view, where you can then select and download them as needed.

Note: For more information about downloading listed product updates, see “Updating your Orion Installation” on page 62.

To configure product updates:

1. Log in to the web console as an administrator, and then click **Settings** in the top right corner of the web console.
2. Click **Available Product Updates** in the Product Updates grouping.
3. *If you want to disable the automatic check for product updates*, clear **Check for product updates**, and then click **Save Settings**.
4. *If you want to ensure that updates are listed for all currently installed Orion products, including Orion NPM and all Orion modules*, check **Show all updates**.
5. Click **Save Settings**.

Updating your Orion Installation

If your Product Updates view is configured to list Orion updates, you can download them directly from the Product Updates view.

To update your Orion installation:

1. Log in to the web console as an administrator, and then click **Settings** in the top right corner of the web console.
2. Click **Available Product Updates** in the Product Updates grouping.
3. Click **Check Now** to refresh the updates list.

4. **If there are any updates you want to ignore**, check the updates to ignore, and then click **Ignore Selected**.
5. Check the updates you want to apply, and then click **Download Selected**.
6. Save and then execute downloaded installers. For more information, see either the `readme.txt` file packaged with the downloaded update or review related documentation available at www.solarwinds.com.

Orion Web Console and Chart Settings

The Orion Website Settings page allows an Orion Web Console administrator to set a number of options that apply to the web console user environment. The following settings are configured on this page:

- Web Console Settings
- Chart Settings
- Discovery Settings

The following procedure configures web console settings.

To configure Orion Website and Chart Settings:

1. Click **Settings** in the top right of the web console.
2. Click **Web Console Settings** in the Settings grouping of the Orion Website Administration page.
3. When you finish configuring web console and chart settings, click **Submit**.

Web Console Settings

The following options are configured on the Orion Web Console Settings page:

- **Session Timeout** is the amount of time (in minutes) the Orion Web Console waits through user inactivity before the user is logged out.
- **Page Refresh** specifies the amount of time that passes before a web console page, or view, reloads automatically.
- **Site Logo URL** is the local path to the banner graphic that appears at the top of every web console page. For more information about changing the banner to display your logo, see “Changing the Web Console Site Logo” on page 61.
- **Site Login Text** is optional text displayed on the Orion Web Console login page. The text entered here is seen by all web console users when they log in. HTML tags are allowed.

- **Help Server** is the URL of the server where online help for Orion NPM is stored. The default location is <http://www.solarwinds.com>. If you are in an Internet-restricted network environment but require access to online help, download the entire online help, copy it to a web server, and then change the Help Server URL to that of the web server. You can download the online help from <http://www.solarwinds.com/support/Orion/docs/OrionLocalHelp.zip>.
- **Status Rollup Mode** establishes the way the availability status of a collection of nodes on the node tree or on a map is displayed in the web console. For more information about the types of information communicated using status icons, see “Status Icons and Identifiers” on page 305. For more information about Status Rollup Modes, including examples, see “Status Rollup Mode” on page 306.

There are two options for the case when there are nodes of differing statuses in a selected group:

- **Mixed Status shows Warning**, the default status, ensures the status of a node group displays the worst warning-type state in the group. If none of the group members have a warning-typed state but the group contains both up and down nodes, a Mixed Availability warning state is displayed for the whole group. For example, `Critical + Down = Critical`, `Critical + Warning = Critical`, and `Up + Down = Mixed Availability`.
- **Show Worst Status** ensures the worst state in a node group is displayed for the whole group. For example, `Up + Down = Down` and `Unreachable + Shutdown = Shutdown`.

Chart Settings

The following chart settings may be configured in the Chart Settings section of the Web Console Settings page:

- **Chart Aspect Ratio** is the height/width ratio for web console charts. This ratio should be set between 0.25 and 3.0 to avoid erratic display problems, though the performance of individual systems may differ.
- **Thumbnail Aspect Ratio** is the height/width ratio for chart thumbnails.
- **95th Percentile Calculations** is a setting that adds annotation lines to charts at the entered percentile. This value is normally set to 95. For more information about 95th percentile calculations, see “95th Percentile Calculations” on page 339.
- **Font Size** sets the default relative size, **Small**, **Medium**, or **Large**, of the text that is displayed within charts in the Orion Web Console. This setting is independent of your browser settings. The font settings in your browser will affect resource headers and some resource contents.

Discovery Settings

The Discovery Settings section provides the **Notify about new removable volumes** option. This option allows you to indicate whether or not you want to be notified when removable volumes are added to your network and discovered during network discovery. For more information about network discovery in Orion NPM, see “Discovering and Adding Network Devices” on page 25.

Using Node Filters

When managing large numbers of network devices with Orion NPM, node list resources can easily become very large and difficult to navigate. Filters are optional SQL queries that are used to limit node list displays for easier resource navigation. SQL queries can be made on any predefined or custom properties. For more information about defining custom properties, see “Creating Custom Properties” on page 251.

To apply a node filter:

1. Click **Edit** in any node list resource.
2. Provide an appropriate SQL query in the **Filter Nodes (SQL)** field.
3. Click **Submit**.

The following are a few example filters with associated SQL queries.

Note: By default, node list resources are designed to sort nodes alphabetically by node caption. This configuration can not be overwritten using a SQL filter, so `order by` clauses included in SQL filters are redundant and will result in Custom SQL filter formatting errors.

- Filter the results to only show nodes that are not **Up**:

```
Status<>1
```

The following are valid status levels:

- 0 = **Unknown** (current up/down status of the node is unknown)
 - 1 = **Up** (The node is responding to PINGs)
 - 2 = **Down** (The node is not responding)
 - 3 = **Warning** (The node may be responding, but the connection from the server to the Node is dropping packets)
- Only show Cisco devices:

```
Vendor = 'Cisco'
```

- Only show devices in Atlanta. (using a custom property named City)
`City = 'Atlanta'`
- Only show devices beginning with "AX3-":
`Caption Like 'AX3-*`
- Only show Nortel devices that are Down:
`Vendor Like 'Nortel*' AND Status=2`
- Only show devices ending in '-TX':
`Vendor Like '*-TX'`

Custom Charts in the Orion Web Console

The Orion Web Console provides charts for monitored interfaces, nodes, and volumes that you can customize for your own use, as detailed in the following sections.

Customizing Charts in the Orion Web Console

Clicking any chart opens the Custom Chart view in a new window, displaying the selected chart with additional chart customization options. For more information about the Custom Chart view, see “Custom Chart View” on page 71.

You can also configure any custom chart resource in the Orion Web Console directly from the resource title bar either by selecting from the dropdown menu of options or by clicking **Edit** to display the Edit *Chart Title* view, as described in the following sections.

Custom Chart Resource Title Bar Options

The title bar menu of the custom chart resource provides the following options for viewing chart data:

- View chart data over the **Last 7 Days**
- View chart data over the **Last 30 Days**
- Select **Edit Chart** to view and modify chart settings.
Note: This is the same as clicking **Edit** in the title bar.
- **View Chart Data** as an HTML format document
- **View Chart Data in Excel** to see chart data in an Excel™-compatible format

Edit Chart Title View

Click **Edit** in the title bar of a custom chart resource to display the *Edit Chart Title* view. This view provides the following options to configure your chart resource:

- **Select a Chart** allows you to change the chart type displayed in the current resource. Chart options are determined in accordance with the type of view displaying the resource you are currently editing. For more information about available interface charts, see “Custom Interface Charts” on page 68. For more information about available node charts, see “Custom Node Charts” on page 69. For more information about available volume charts, see “Custom Volume Charts” on page 70.
- The **Time Period** for the selected chart may be any of the following:

Last Hour	Last 2 Hours	Last 24 Hours	Today
Yesterday	Last 7 Days	This Month	Last Month
Last 30 Days	Last 3 Months	This Year	Last 12 Months

- The **Sample Interval** for the selected chart may be any of the following:

Every Minute	Every 5 Minutes	Every 10 Minutes	Every 15 Minutes
Every 30 Minutes	Every Hour	Every 2 Hours	Every 6 Hours
Every 12 Hours	One a Day	Every 7 Days	

Notes:

- Each sample interval is represented on a chart by a single point or bar. Data within a selected sample interval is summarized automatically.
- Due to limits of memory allocation, some combinations of time periods and sample intervals require too many system resources to display, due to the large number of polled data points. As a result, charts may not display if the time period is too long or if the sample interval is too small.
- The **Trend Line** option allows you to enable the trend line feature of Orion NPM charts. By enabling trend lines on Orion NPM charts, you can see potential future results as they are extrapolated from collected historical data.

Note: Due to the broad array of factors that can affect the performance of devices on your network, trend lines provided on Orion NPM charts are intended as approximate predictions of future data only.

For more information about customizing web console views to display custom charts, see “Customizing Views” on page 46. Some charts also provide a 95th Percentile marker for your reference. For more information about calculating 95th percentile values, see “95th Percentile Calculations” on page 339.

Custom Interface Charts

The following interface-related charts, grouped by type, are available as resources within the Orion Web Console. To add any of these charts to a web console view dealing with monitored interfaces, add the Custom Interface Chart resource to the Interface Details view. For more information about adding resources to Orion Web Console views, see “Customizing Views” on page 46. For more information about customizing any of the following charts, see “Orion Web Console and Chart Settings” on page 63.

Discards and Errors Charts

The following charts are available to display information about discards and errors on interfaces monitored by Orion NPM.

- In/Out Discards – Step Chart
- In/Out Errors – Step Chart
- In/Out Errors and Discards – Step Chart

Percent Utilization Charts

The following charts are available to display percent utilization information for monitored interfaces in Orion NPM.

- Min/Max/Average Percent Utilization
- Min/Max/Average Transmitted + Received Traffic Percent Utilization
- Percent Utilization – Line Chart
- Percent Utilization – Step Chart

Traffic Charts

The following charts are available to display information about interface traffic, including multicast traffic, on devices monitored by Orion NPM.

- Average bps – Line Chart
- Average bps – Step Chart
- Average Packets per Second
- Min/Max/Average bps In/Out
- Min/Max/Average bps Received
- Min/Max/Average bps Transmitted
- Min/Max/Average bps Transmit+Receive
- Min/Max/Average bps Transmit+Receive Percent Utilization

- Min/Max/Average Packets In/Out
- Multicast Traffic
- Total Bytes Transferred
- Total Packets Transmitted/Received

Custom Node Charts

The following node-related charts, grouped by type, are available as resources within the Orion Web Console. To add any of these charts to a web console view dealing with monitored nodes, add the Custom Node Chart resource to the Node Details view. For more information about adding resources to Orion Web Console views, see “Customizing Views” on page 46. For more information about customizing any of the following charts, see “Orion Web Console and Chart Settings” on page 63.

Availability

The following charts are available to display node availability information over custom time periods for nodes monitored by Orion NPM.

- Availability
- Availability – Autoscale
- Availability and Response Time

CPU Load

The following charts display CPU loading information over specified periods of time for nodes monitored by Orion NPM.

- Average CPU Load
- Min/Max/Average CPU Load

Memory Usage

The following charts present memory usage information over custom time periods for nodes monitored by Orion NPM.

- Average Memory Usage
- Memory/Buffer Failures
- Min/Max/Average Memory Usage
- Percent Memory Used

Packet Loss and Response Time

The following charts are available to display historical statistics about packet loss and response time for nodes monitored by Orion NPM.

- Availability and Response Time
- Average Response Time
- Average Response Time and Packet Loss
- Min/Max/Average Response Time
- Min/Max/Average Response Time and Packet Loss
- Percent Loss – Bar Chart
- Percent Loss – Line Chart

Custom Volume Charts

The following volume-related charts, grouped by type, are available as resources within the Orion Web Console. To add any of these charts to a web console view dealing with monitored volumes, add the Custom Volume Chart resource to the Volume Details view. For more information about adding resources to Orion Web Console views, see “Customizing Views” on page 46. For more information about customizing the following charts, see “Orion Web Console and Chart Settings” on page 63.

Allocation Failures

Shows the number of disk allocation failures that have occurred on the selected volume.

Min/Max/Average Disk Usage

Shows both the total disk space available and the average amount of disk space used on the selected volume. Bars are also included to show minimum and maximum levels of disk usage.

Percent Disk Usage

Shows the total available disk space and the average amount of disk space used, as a percentage of the total available, on the selected volume.

Volume Size

Shows the total disk space available on the selected volume.

Custom Chart View

Charts in the Orion Web Console are easily customizable. Clicking a chart opens the Custom Chart view in a new window. The following sections describe options that are available on the Custom Chart page to modify the presentation of a selected chart.

Note: Click **Refresh** at any time to review changes you have made.

Printing Options

To print your customized chart, click **Printable Version** and a printable version of your customized chart displays in the browser.

Chart Titles

Chart Titles are displayed at the top center of a generated chart. The Chart Titles area allows you to modify the **Title** and **Subtitles** of your generated chart.

Note: Orion NPM may provide default chart titles and subtitles. If you edit any of the Chart Titles fields on the Custom Chart page, you can restore the default titles and subtitles by clearing the respective fields, and then clicking **Submit**.

Time Period

Predefined and custom time periods are available for generated charts. You may designate the time period for a chart by either of the following methods:

- Select a predefined period from the **Select a Time Period:** menu.
- Provide custom **Beginning** and **Ending Dates/Times** in the appropriate fields in the Time Period area.

Sample Interval

The sample interval dictates the precision of a given chart. A single point or bar is plotted for each sample interval. If a sample interval spans multiple polls, data is automatically summarized and plotted as a single point or bar on the chart.

Note: Due to limits of memory allocation and the large number of polled data points, some combinations of time periods and sample intervals may require too many system resources to display. As a result, charts may not display if the time period is too long or if the sample interval is too small.

Chart Size

Chart Size options configure the width and height, in pixels, of the chart. You can maintain the same width/height aspect ratio, or scale the chart in size, by entering a width in the **Width** field and then entering 0 for the **Height**.

Font Size

Font sizes for generated charts are variable. The **Font Size** option allows you to select a **Small**, **Medium**, or **Large** size font for your chart labels and text.

Note: **Font Size** selections are maintained in the printable version of your chart.

Data Export Options

The Display Data from Chart area provides the following options to export chart data as either Excel-compatible **Raw Data** or as HTML-formatted **Chart Data**:

- To view chart data in an Excel-compatible format, click **Raw Data**, and then follow the prompts, if provided, to open or save the resulting raw data file.
- To view HTML-formatted chart data in a new browser, click **Chart Data**.

Integrating SolarWinds Engineer's Toolset

When you are browsing the Orion Web Console from a computer that already has a SolarWinds Toolset installed, Orion NPM allows you to launch Toolset tools directly from your web browser. Right-clicking any node, interface, or volume listed in an Orion Web Console running the Toolset Integration displays a menu of available Toolset tools and functions. The following sections detail the configuration of the available Toolset integration.

Note: For more information about the SolarWinds Engineer's Toolset tools, see www.solarwinds.com.

Configuring a Toolset Integration

The following procedure configures SolarWinds Toolset for integration within the Orion Web Console.

Note: The first time the Toolset tools are accessed, a security warning may be displayed. Click **Yes** to allow the toolset integration.

To configure SolarWinds Toolset integration settings:

1. Right-click any node, interface, or volume displayed within the Orion Web Console.
2. Click **Settings**.
3. Click **SNMP Community String**.

Note: The first time you launch a tool requiring an SNMP community string from the right-click menu, the SNMP Community String window displays.

4. **If you want to delete any or all saved community strings**, select the strings that you want to delete, and then click **Remove**, or click **Remove All**.

5. Click **Menu Options**, and then configure the right-click menu as follows:
 - a. *If you want either to add menu items to the right-click menu or to remove menu items from the right-click menu*, move menu items between the list of **Available Menu Options** on the left and **Selected Menu Options** on the right by selecting items in either column and clicking the right and left arrows, as appropriate.
 - b. *If you want to change the order of menu items*, select items and then click the up and down arrows next to the **Selected Menu Options** list.
 - c. *If you want to add a separator between items*, move the ----- menu option from the **Available** list to the **Selected** list, and then move it to your preferred location within the **Selected Menu Options** list.
6. Click **Automatic Menu Items**.
7. Check either or both of the following options:
 - **Automatically add sub-menu items to the “MIB Browser (Query MIB)” menu option from the MIB Browser’s Bookmarks.**
 - **Automatically add sub-menu items to the “Real Time Interface Monitor” menu option from the Real-Time Interface Monitor saved report types.**

Note: These options expand the list of available menu items by incorporating menu links to MIB browser bookmarks and Real-Time Interface Monitor saved reports, respectively.

Adding Programs to a Toolset Integration Menu

The following procedure provides the steps required to add any external scripts or applications to the SolarWinds Toolset integration menu.

To add a program to the SolarWinds Toolset integration menu:

1. *If you want to add an external script to the Toolset Integration menu*, save the script in an appropriate location on the install volume of your Orion NPM server (e.g. `<InstallVolume>:\Scripts\`).
2. *If you want to add an external application to the Toolset Integration menu*, install the application in an appropriate location on the install volume of your Orion NPM server (e.g. `<InstallVolume>:\Application\`).
3. Open `SWToolset.MenuOptions`, the Toolset Integration menu configuration file, in a text editor.

Note: By default, `SWToolset.MenuOptions` is located in the following folder:
`<InstallVolume>:\Program Files\SolarWinds\Common\`.

4. Save a copy of `SWToolset.MenuOptions` as `SWToolset_Old.MenuOptions`.

5. Add the following line between the `<MenuOptions>``</MenuOptions>` tags of the `SWToolset.MenuOptions` file:




```
<MenuOption Visible="TRUE" Title="ApplicationName"
BeginGroup="FALSE" HasSubMenu="FALSE"
ExecString="<InstallVolume>:\Application\ExecutableFile"
Icon="" Extra="" Parent="" Required="4"/>
```

Note: The string supplied for `Title` is the name for the added script or application that will display in the menu. The string supplied for the `ExecString` is the path to the script or application executable file.

6. Save the new `SWToolset.MenuOptions` to automatically update the Toolset Integration menu.

Accessing Nodes Using HTTP, SSH, and Telnet

The Orion Web Console supports the use of HTTP, SSH, and Telnet protocols for remote device access if associated applications like PuTTY and FiSSH on your Orion NPM server are properly registered. For more information, see the MSDN article, “Registering an Application to a URL Protocol”. Launch remote access applications from any Details view as follows:

- To browse directly to the viewed device using a web browser, click .
- To open a secure shell (SSH) to a monitored device, click .
- To open a Telnet session with a monitored device, click .

Using Integrated Remote Desktop


Sometimes it is necessary to console into a remote server to troubleshoot an issue. This can be accomplished within the Orion Web Console as follows.

Note: Press `Ctrl+Alt+Break` to enter/exit full screen mode.

To launch Integrated Remote Desktop:

1. Open the Node Details view for the server you want to view remotely.

Note: The easiest way to open the Node Details view is to click the remote server you want to view in any All Nodes resource.

2. Click , located at the of the Node Details view.

Note: Depending on the security settings of your browser, you may be asked to install an ActiveX control for remote desktop viewing. Follow all prompts to install this required control.

3. Verify the **Server** IP address or hostname.

4. Select an appropriate **Screen Size**.
5. Click **Connect**.

Managing Orion Web Console Configurations

Orion Web Console configurations store all account, menu bar, and view settings. The Orion Web Configuration Backup/Restore utility allows you to complete each of the following related tasks:

- Back up your Orion Web Console configuration. For more information, see “Creating a Web Console Configuration Backup” on page 75.
- Restore a web console configuration backup. For more information, see “Restoring a Web Console Configuration Backup” on page 76.
- Clear your current Orion Web Console configuration. For more information, see “Clearing a Web Console Configuration” on page 76.

Creating a Web Console Configuration Backup

The following procedure uses the Orion Web Configuration Backup/Restore utility to create a backup of your Orion Web Console configuration.

Note: The Orion Web Configuration Backup/Restore utility does not create a backup of the Orion database. As a result, configuration backups do not retain any of the network device data or monitoring statistics for any nodes, interfaces, or volumes on your network. For more information about creating a backup of your Orion database, see “Managing the Orion NPM Database” on page 269.

To create an Orion Web Console configuration backup:

1. Log in to the Orion Web Console as an administrator.
2. Click **Start > All Programs > SolarWinds Orion > Advanced Features > Web Configuration Backup**.
3. Click **Create Backup**.
4. Confirm that the Orion folder is open or browse to it, located, by default within `<Volume:>\Program Files\Solarwinds\`.
5. Provide an appropriate file name and location, and then click **Save**.
6. Click **OK** when the web console configuration backup is completed.

Restoring a Web Console Configuration Backup

The following procedure uses the Orion Web Configuration Backup/Restore utility to restore a saved backup of your Orion Web Console configuration.

Warning: Do not restore web console configurations from any version of Orion NPM prior to the version currently installed.

To restore an Orion Web Console configuration backup:

1. Log in to the Orion Web Console as an administrator.
2. Click **Start > All Programs > SolarWinds Orion > Advanced Features > Web Configuration Backup**.
3. In the Restore Web Site Configuration area, select the configuration backup file you want to restore.
4. *If you want the restored Orion Web Console configuration to overwrite your current web console configuration*, select **Overwrite**, and then click **Restore Backup**.
5. *If you want the restored Orion Web Console configuration to merge with your current web console configuration*, select **Merge**, and then click **Restore Backup**.
6. Click **Yes** to confirm the restoration of the selected configuration backup.

Clearing a Web Console Configuration

The following procedure clears an existing Orion Web Console configuration.

Warning: Clearing a web console configuration deletes all existing user accounts, account and view settings, and menu bar customizations. SolarWinds recommends you create a backup of your current Orion Web Console configuration before you clear it to confirm that no issues arise as a result of the deletion of your web console customizations.

To clear your Orion Web Console configuration:

1. Log in to the Orion Web Console as an administrator.
2. Click **Start > All Programs > SolarWinds Orion > Advanced Features > Web Configuration Backup**.
3. Click **File > Clear Web Configuration**.
4. Click **Yes** to confirm the deletion of your current web console configuration.
5. Click **OK** after the web console configuration is cleared.

Chapter 5

Managing Devices in the Web Console

Managing all the monitored devices on your network is greatly simplified with the Node Management feature of the Orion Web Console. Using this tool, you can easily add and remove nodes, interfaces, and virtual servers and quickly view and edit device properties. Any user that has been granted node management rights can directly access the Node Management tool either from any All Nodes resource or through the Orion Website Administration page. For more information about granting node management rights, see “Editing User Accounts” on page 92. The following sections describe the various functions that allow you to view and manage all your network devices from the Orion Web Console.

Note: The Node Management feature is accessible by clicking **Manage Nodes** either in the header of any All Nodes resource or in the Node Management group of the Orion Website Administration page. The All Nodes resource is included on the Network Summary Home view by default, but you can include it on any other web console view as well. Confirm that the All Nodes resource is available on an appropriate Web Console view before continuing. For more information about adding resources to Orion NPM views, see “Editing Views” on page 46.

Network Overview

By default, the Orion Web Console provides a Network Overview that shows, at a glance, a wide array of information about all the nodes and interfaces on your network that Orion NPM is currently monitoring. The Network Overview lists a node property status icon to the left of each monitored node on your network. To the right of each node is a row of status icons, where each icon represents the status of a selected interface property on the listed node. The following table lists the types of information for monitored nodes and interfaces that is communicated in the form of colored icons on the Network Overview.

Node Property	Interface Property
Response Time	Percent Utilization
Average Response Time	Type
Maximum Response Time	Errors and Discards Today
CPU Load	Errors and Discards This Hour
Percent of Memory Used	Status
Percent Packet Loss	Traffic
Machine Type	
Node Status	

A legend at the bottom of the Network Overview provides translations between icon colors and measured values for each network device property. Hovering over any icon, IP address, or node name opens a tooltip providing current status information about the associated node or interface.

To view the Network Overview:

1. Click **Start > All Programs > SolarWinds Orion > Orion Web Console**.
2. Log in to the Orion Web Console, and then click **Network > Overview**.
3. Select the node property you want to view in the **Nodes** field, and then select the interface property you want to view in the **Interfaces** field.
4. Click **Refresh** to show the updated overview.

Adding Devices for Monitoring in the Web Console

The following procedure details the steps required to add a device and its interfaces and volumes for monitoring in the Orion Web Console.

To add a device for monitoring in the Orion Web Console:

1. Log in to the Orion Web Console as an administrator.
2. Click **Settings** in the top right of the web console.
3. Click **Manage Nodes** in the Node Management grouping of the Orion Website Administration page.
4. Click **Add Node** on the Node Management toolbar.
5. Provide the hostname or IP Address of the node you want to add in the **Hostname or IP Address** field.
6. *If you only want to use ICMP to monitor node status, response time, or packet loss for the added node, check **ICMP (Ping only)**.*
7. *If you are adding a VMware ESX Server, check **Poll for ESX** to ensure that Orion NPM acquires any data the ESX Server provides to SNMP polling requests, and then complete the following steps to provide required ESX Server credentials. For more information about monitoring VMware ESX Servers, see “Monitoring VMware ESX Servers” on page 119.*
 - a. Provide an appropriate **VMware credential name**.

Notes:

- If you are editing an existing credential, select the credential you are editing from the **Choose Credential** field.
- SolarWinds recommends against using non-alphanumeric characters in VMware credential names.

- b. Provide an appropriate **User name** and a **Password**.
 - c. Provide the password again in the **Confirm password** field.
 - d. Click **Validate VMware** to confirm the ESX credentials you provided.
8. ***If you want to add an External node to monitor a hosted application with Orion Application Performance Monitor, check External.***

Note: Orion NPM does not collect or monitor any network performance data from nodes designated as External. The External status is reserved for nodes hosting application that you want to monitor with Orion Application Performance Monitor.

9. ***If you want to use SNMP to monitor the added node, confirm that ICMP (Ping only) is cleared, and then complete the following steps:***
- a. Select the **SNMP Version** for the added node.

Notes:

- Orion NPM uses **SNMPv2c** by default. If the device you are adding supports or requires the enhanced security features of SNMPv3, select **SNMPv3**.
 - If SNMPv2c is enabled on a device you want Orion NPM to monitor, by default, Orion NPM will attempt to use SNMPv2c to poll for performance information. If you only want Orion NPM to poll using SNMPv1, you must disable SNMPv2c on the device to be polled.
- b. ***If you have installed multiple polling engines, select the Polling Engine you want to use to collect statistics from the added node.***
- Note:** This option may not be available if you are only using one polling engine to collect information from your network.
- c. ***If the SNMP port on the added node is not the Orion NPM default of 161, provide the actual port number in the SNMP Port field.***
 - d. ***If the added node supports 64 bit counters and you want to use them, check Allow 64 bit counters.***

Note: Orion NPM fully supports the use of 64-bit counters; however, these high capacity counters can exhibit erratic behavior depending on manufacturer implementation. If you notice peculiar results when using these counters, use the Node Details view to disable the use of 64-bit counters for the device and contact the hardware manufacturer.

10. ***If you want Orion NPM to use SNMPv2c to monitor the added node, provide valid community strings for the added node.***

Note: The **Read/Write Community String** is optional, but Orion NPM does require the `public` **Community String**, at minimum, for node monitoring.

11. *If you want Orion NPM to use SNMPv3 to monitor the added node*, provide the following **SNMP Credentials, Authentication, and Privacy/Encryption** settings:
 - **SNMPv3 Username and Context**
 - **SNMPv3 Authentication Method and Password/Key**
 - **SNMPv3 Privacy/Encryption Method and Password/Key**
12. *If you are using SNMP to communicate with your added node*, click **Validate SNMP** after entering all credentials to confirm your SNMP settings.
13. Click **Next**.
14. Check the interfaces, volumes, and interface charts for the added node that you want Orion NPM to monitor. The following options are available in the selection toolbar:
 - Clicking **All** selects all listed devices and charts for monitoring.
 - Clicking **None** clears any checked interfaces, volumes, or interface charts that have been selected for monitoring.
 - Clicking **All Active Interfaces** selects only currently active interfaces and the associated interface charts for monitoring.
 - Clicking **All Volumes** selects all listed volumes for monitoring.
 - Clicking **All Interfaces** selects all listed interfaces for monitoring.
15. After you have selected interfaces, volumes, or interface charts for monitoring, click **Next**.
16. *If you want to apply pollers to the added node*, click **+** to expand poller groups, as necessary, check the appropriate pollers, and then click **Next**.

Note: For more information about using predefined pollers or about defining your own universal device pollers, see “Monitoring MIBs with Universal Device Pollers” on page 235.
17. *If you want to edit the SNMP settings you provided earlier*, change the appropriate values in the SNMP area of the Change Properties page, and then click **Validate SNMP** to confirm your new settings.
18. *If you want to edit the default polling settings for your added node*, change the **Node Status Polling** or **Collect Statistics Every** values in the Polling area of the Change Properties page, as appropriate.

Note: The **Node Status Polling** value refers to the number of seconds, between the node status checks Orion NPM performs on the added node. The **Collect Statistics Every** value refers to the period of time between the updates Orion NPM makes to displayed statistics for the added node.

19. **If you have defined any custom properties for monitored nodes**, provide appropriate values for the added node in the Custom Properties area of the Change Properties page.

Note: The Custom Properties area is empty if you have not defined any custom properties for monitored nodes in Orion NPM.

20. Click **OK, Add Node** when you have completed properties configuration.

21. **If you have successfully added the node**, click **OK** on the dialog.

Deleting Devices from Monitoring

The following procedure deletes devices from monitoring in the web console.

Warning: Deleting nodes from monitoring in the web console automatically terminates monitoring of all interfaces and volumes on deleted nodes.

Note: You can select multiple devices to delete at the same time. Additionally, using the search tool above the node list, you can select multiple interfaces on different nodes for simultaneous deletion.

To delete devices from monitoring in the Orion Web Console:

1. Log in to the Orion Web Console as an administrator.
2. Click **Settings** in the top right of the web console, and then click **Manage Nodes** in the Node Management grouping of the Orion Website Administration page.
3. **If you want to delete a node with all its monitored interfaces**, complete the following steps.
 - a. Locate the node to delete using either of the following methods:
 - Use the search tool above the node list to search your Orion database for the node you want to delete.
 - Select an appropriate **Group by:** criterion, and then click the appropriate group including the node to delete.
 - b. Check the node to delete in the list, and then click **Delete** on the toolbar.
4. **If you want to delete an interface or a volume**, use the following steps.
 - a. Locate the element to delete using either of the following methods:
 - Use the search tool above the node list to search your Orion database either for the interface or for the parent node of the interface or volume to delete.
 - Select a **Group by:** criteria, and then click the appropriate group including the parent node of the interface or volume to delete.

- b. **If you have a list of node results**, click **+** to expand the parent node of the interface or volume you want to delete.
 - c. Check the interface or volume to delete, and then click **Delete** on the Node Management toolbar.
5. Click **OK** to confirm deletion.

Viewing Node and Interface Data in Tooltips

Node and interface tooltips in Orion NPM provide immediate status overviews of monitored nodes and interfaces. To view a quick overview of any monitored node or interface in the web console, hover over the device name. Depending on the selected device, the information in the following tables is displayed immediately.

Interface Data	
Interface Name	The name of the interface as discovered from its parent node
Operational Status	Operational status of the interface
Administrative Status	Administrative status of the interface (enabled or disabled)
Interface Type	Numerical type of the interface, as determined by Orion NPM when the parent node is discovered.
Transmitted Current Traffic	The amount of traffic the interface was transmitting as of the last interface poll
Transmitted Percent Utilization	The percent of available bandwidth used for traffic transmitted from the interface as of the last interface poll
Received Current Traffic	The amount of traffic the interface was receiving as of the last interface poll
Received Percent Utilization	The percent of available bandwidth used for traffic received by the interface as of the last interface poll

Node Data	
Node Status	Current status of the node. (up, down, warning, unplugged, or unmanaged)
IP Address	The IP address currently assigned to the selected node
Machine Type	The vendor icon and vendor description of the selected node
Average Response Time	The measured average response time of the selected node as of the last node poll
Packet Loss	The percent of all transmitted packets that are lost by the selected node as of the last node poll
CPU Load	The percent of available processing capacity on the selected node that is currently used as of the last node poll
Memory Used	The percent of available memory on the selected node that is currently used as of the last node poll

Editing Device Properties

The following procedure provides the steps required to edit node, interface, or volume properties using the Node Management utility of the Orion Web Console.

To edit device properties in the Orion Web Console:

1. Log in to the Orion Web Console as an administrator.
2. Click **Settings** in the top right of the web console.
3. Click **Manage Nodes** in the Node Management grouping.
4. Locate the device to edit using either of the following methods:
 - Use the search tool above the node list to search your Orion database for either the node or interface you want to edit or the parent node of the volume you want to edit.
 - Select an appropriate **Group by** criteria, and then click the appropriate group including either the node to edit or the parent node of the interface or volume to edit.
5. *If you want to edit the properties of a monitored node*, check the node you want to edit, and then click **Edit Properties**.
6. *If you want to edit the properties of a monitored interface*, click **+** next to the parent node of the interface you want to edit, check the interface you want to edit, and then click **Edit Properties**.
7. *If you are editing the SNMP properties of a node*, click **Validate SNMP** after providing new settings to confirm they are valid for the edited node.
8. *If the selected node is a VMware ESX Server and you want to poll it for data using the VMware API*, Confirm that **Poll for ESX** is checked.
9. *If you want to poll for ESX data using an existing ESX credential*, select the appropriate credential from the **VMware credentials** dropdown menu.
10. *If you want to poll for ESX data using a new ESX credential*, complete the following steps:
 - a. Select **<New Credential>** in the **Choose Credential** dropdown menu, and then provide a new credential name in the **Credential Name** field.

Note: SolarWinds recommends against using non-alphanumeric characters in VMware credential names.
 - b. Add the credential **User name** and **Password**, as necessary.
 - c. Confirm the password, and then click **Validate VMware** to confirm the credentials you have provided are valid for the edited node.
11. Edit additional device properties as needed, and then click **Submit**.

Promoting a Node from ICMP to SNMP Monitoring

After adding a node to the Orion database as an ICMP only node, you may need to promote the node to SNMP to start collecting additional statistics. The Node Management utility of the Orion Web Console can easily promote your node to SNMP without any loss of historical data.

To promote an ICMP only node to SNMP:

1. Log in to the Orion Web Console as an administrator.
2. Click **Settings** in the top right of the web console, and then click **Manage Nodes** in the Node Management grouping of the Orion Website Administration page.
3. Locate the device to promote using either of the following methods:
 - Use the search tool above the node list to search your Orion database for the node you want to promote.
 - Select an appropriate **Group by** criteria, and then click the appropriate group including the node to promote.
4. Click **Edit Properties**, and then clear **ICMP (Ping only)**.
5. In the SNMP area, select the **SNMP Version** for the promoted node.

Note: Orion NPM uses **SNMPv2c** by default. If the promoted device supports or requires the enhanced security features of SNMPv3, select **SNMPv3**.
6. **If you have installed multiple polling engines**, select the **Polling Engine** you want to use to collect statistics from the added node.

Note: This option may not be available if you are only using one polling engine to collect information from your network.
7. **If the SNMP port on the added node is not the Orion NPM default of 161**, provide the actual port number in the **SNMP Port** field.
8. **If the added node supports 64 bit counters and you want to use them**, check **Allow 64 bit counters**.

Note: Orion NPM fully supports the use of 64-bit counters; however, these high capacity counters can exhibit erratic behavior depending how they are used. If you notice peculiar results when using these counters, use the Edit Properties view to disable the use of 64-bit counters on the device in question, and then contact the hardware manufacturer.
9. **If you want to use SNMPv2c to monitor the promoted node**, provide valid community strings for the added node.

Note: The **Read/Write Community String** is optional, but Orion NPM does require the `public` **Community String**, at minimum, for node monitoring.

10. **If you want to use SNMPv3 to monitor the promoted node**, provide the following SNMPv3 credential settings:
 - **SNMPv3 Username** and **Context**
 - **SNMPv3 Authentication Method** and **Password/Key**
 - **SNMPv3 Privacy/Encryption Method** and **Password/Key**

Note: Read/Write SNMPv3 Credentials are optional, but the `public` Community String is required, at a minimum, for node monitoring.
11. **If you want to edit an existing SNMPv3 credential set**, select the name of your set from the **Saved Credential Sets** list, and then edit the stored settings..
12. **If you want save the provided SNMPv3 credentials as a credential set**, provide a **Name** for your new credential set, and then click **Save**.
13. Click **Validate SNMP** after entering all required credentials to confirm your SNMP settings.
14. **If you want to change the default polling settings for your promoted node**, edit the **Node Status Polling** or **Collect Statistics Every** values in the Polling area, as appropriate.

Note: The **Node Status Polling** value refers to the period of time, in seconds, between the node status checks performed by Orion NPM on the promoted node. The **Collect Statistics Every** value refers to the period of time between updates Orion NPM makes to displayed statistics for the promoted node.
15. **If you have defined any custom properties for monitored nodes**, provide appropriate values for the promoted node in the Custom Properties.
16. Click **Submit** when you have completed properties configuration for your promoted node.
17. **If you have successfully added the node**, click **OK** on the dialog.

Viewing Node Resources

The List Resources feature of the Orion Web Console Node Management utility allows you to immediately see all monitored interfaces, volumes, and interface charts on a selected node, as shown in the following procedure.

To view a list of all resources present on a node:

1. Log in to the Orion Web Console as an administrator.
2. Click **Settings** in the top right of the web console.

3. Click **Manage Nodes** in the Node Management grouping of the Orion Website Administration page.
4. Locate the node to view using either of the following methods:
 - Use the search tool above the node list to search your Orion database for the node you want to view.
 - Select an appropriate **Group by** criteria, and then click the appropriate group including the node to view.
5. Check the node you want to view from the list, and then click **List Resources** on the Node Management toolbar.

Setting Device Management States

Monitored devices are regularly polled for operational status. Collected statistics are displayed in the Orion Web Console. Using the Node Management feature of the Orion Web Console, the management status of monitored nodes, is easily set or changed, allowing you to either temporarily suspend data collection or resume polling and statistics collection, as necessary. The following procedure sets or changes management states for monitored nodes in the Orion Web Console.

Note: Setting a node to an unmanaged state automatically suspends the management of all interfaces and volumes on the selected node.

To set or change the management state of a node:

1. Log in to the Orion Web Console as an administrator.
2. Click **Settings** in the top right of the web console.
3. Click **Manage Nodes** in the Node Management grouping of the Orion Website Administration page.
4. Locate the node to manage using either of the following methods:
 - Use the search tool above the node list to search your Orion database for the device you want to manage.
 - Select an appropriate **Group by** criteria, and then click the appropriate group including the node to manage.
5. Check the node to change, and then click **Unmanage** or **Remanage**, as appropriate, for the selected node.
6. ***If you have selected Unmanage***, provide start and end times and dates for your management suspension, and then click **OK**.

Assigning Pollers to Monitored Devices

Orion NPM provides both a selection of predefined pollers and the Universal Device Poller utility for defining your own pollers to monitor specific aspects of your network devices. In the Orion Web Console, the assignment of pollers to monitored devices is a straightforward process, as shown in the following steps.

Note: If you do not see a poller that meets your specific monitoring needs, use the Universal Device Poller to create your own poller. For more information, see “Monitoring MIBs with Universal Device Pollers” on page 235.

To assign a poller to a monitored device:

1. Log in to the Orion Web Console as an administrator.
2. Click **Settings** in the top right of the web console.
3. Click **Manage Nodes** in the Node Management grouping of the Orion Website Administration page.
4. Locate the node to poll, the interface to poll, or the parent node of the interface or volume to poll using either of the following methods:
 - Use the search tool above the node list to search your Orion database.
 - Select an appropriate **Group by** criteria, and then click the appropriate group including either the node to poll or the parent node of the interface or volume to poll.
5. *If you want to assign a poller to a node*, complete the following steps:
 - a. Check the monitored node to which you want to assign the poller.
 - b. Click **Assign Pollers** in the Node Management toolbar.
 - c. Check the pollers you want to assign to the selected node, and then click **Submit**.
 - d. Click **OK** to confirm the assignment.
6. *If you want to assign a poller to an interface or volume*, complete the following steps:
 - a. Click **+** next to the parent node of the interface or volume to which you want to assign the poller.
 - b. Check the interface or volume to which you want to assign the poller.
 - c. Click **Assign Pollers** in the Node Management toolbar.
 - d. Check the pollers you want to assign to the selected interface or volume, and then click **Submit**.
 - e. Click **OK** to confirm the assignment.

Unscheduled Device Polling and Rediscovery

Orion NPM polls devices for statistics and status regularly, according to the polling settings available for configuration in System Manager. For more information, see “Network Performance Monitor Settings” on page 260. Sometimes, however, it may be necessary to conduct an unscheduled poll or rediscovery of a monitored device. The Node Management utility gives you this ability, as shown in the following procedure.

To perform an unscheduled poll or rediscovery:

1. Log in to the Orion Web Console as an administrator.
2. Click **Settings** in the top right of the web console.
3. Click **Manage Nodes** in the Node Management grouping of the Orion Website Administration page.
4. Locate and check the node or interface you want to poll or locate and check the node to rediscover, using either of the following methods:
 - Use the search tool above the node list to search your Orion database.
 - Select an appropriate **Group by** criteria, and then click the appropriate group including either the node or interface you want to poll or the node you want to rediscover.
5. *If you want to poll the selected node or interface*, click **More Actions > Poll Now**.
6. *If you want to rediscover the selected node*, click **More Actions > Rediscover**.

Remotely Managing Monitored Interfaces

Using the Orion NPM Node Management utility, you have the ability to shut down and enable interfaces remotely, as shown in the following procedures.

To remotely shut down or enable an interface:

1. Log in to the Orion Web Console as an administrator.
2. Click **Settings** in the top right of the web console, and then click **Manage Nodes** in the Node Management grouping.
3. Locate and check the interface you want to shut down or locate and check the interface you want to enable, using either of the following methods:
 - Use the search tool above the node list to search your Orion database.
 - Select an appropriate **Group by** criteria, and then click the appropriate group including the interface you want to shut down or enable.

4. **If you want to shut down the selected interface**, click **More Actions > Shut Down**, and then click **OK** to confirm.
5. **If you want to enable the selected shutdown interface**, click **More Actions > Enable**.

Monitoring Windows Server Memory

When Orion NPM polls a Windows server for CPU load and memory utilization, it pulls the amount of physical memory (this is the 100% number) and then it totals the amount of memory in use by each allocation to compute what percentage of the physical memory is in use. This can result in memory utilization readings over 100%, as many applications pre-allocate memory and swap before it is actually needed. To work around this, you can also add physical memory as a volume for these servers within Orion NPM. When monitored as a volume, the values will be more in line with your expectations.

Scheduling a Node Maintenance Mode Time Period

When you need to perform maintenance on a node or its components, such as upgrading firmware, installing new software, or updating security, you may want to discontinue polling while the device is down for maintenance. Disabling polling, or setting a node status as Unmanaged, while performing node maintenance, maintains the accuracy of your data and prevents unnecessary alert messages. For more information about disabling node polling to perform node maintenance, see “Setting Device Management States” on page 86.

Chapter 6

Managing Web Accounts

Orion Web Console user accounts, permissions, and views are established and maintained with the Orion Account Manager. When Advanced Customization is enabled on the Orion Website Settings page, you can use Account Manager to customize menu bars and views for different users. For more information about Orion Website Settings and Advanced Customization, see “Orion Web Console and Chart Settings” on page 63.

Notes:

- This guide assumes that Advanced Customization has been enabled. If it has not been enabled, the range of options available on the pages referenced in the following sections is much more limited. For more information, see “Orion Website Administration” on page 38.
- To prevent issues with web console accounts, your SQL Server should not be configured with the `no count` connection option enabled. The `no count` option is set in the **Default connection options** area of the **Server Properties > Connections** window of SQL Server Management Studio

Creating New Accounts

New Orion Web Console user accounts may be created by any web console administrator. The following procedure creates a new web console user account.

To create a new user account:

1. Log in to the Orion Web Console as an administrator.
2. Click **Settings** in the top right of the web console, and then click **Account Manager** in the Accounts grouping of the Orion Website Administration page.
3. Click **Add**.
4. Type a new **User Name** and **Password**.
5. Confirm the password, and then click **Submit**.

When the new account is created, the *Edit User Account* view displays, showing all configurable account options. For more information about editing account settings, see “Editing User Accounts” on page 92.

Note: For more information about using Windows Pass-through security and DirectLink accounts for automatic login to the Orion Web Console, see “Configuring Automatic Login” on page 341.

Editing User Accounts

The Edit *User Account* page provides options for configuring web console user accounts. On the Edit *User Account* page, administrators can disable an account, set an account expiration date, grant administrator and node management rights, set user view limitations, define a default menu bar, and set several other defaults defining how a user account views and uses the Orion Web Console. The following sections and procedures detail the configuration of user accounts.

Note: To reset a password, click **Change Password** at the bottom of the page.

User Account Access Settings

The following procedure is a guide to setting user account access.

To edit a user account:

1. Log in to the Orion Web Console as an administrator.
2. Click **Settings** in the top right of the web console.
3. Click **Account Manager** in the Accounts grouping of the Orion Website Administration page.
4. Select the account that you want to edit, and then click **Edit**.
5. Set **Account Enabled** to **Yes** or **No**, as appropriate.

Note: Accounts are enabled by default, and disabling an account does not delete it. Account definitions and details are stored in the Orion database in the event that the account is enabled at a later time.

6. *If you want the account to expire on a certain date*, click **Browse (...)** next to the **Account Expires** field, and then select the account expiration date using the calendar tool.

Note: By default, accounts are set to **Never** expire. Dates may be entered in any format, and they will conform to the local settings on your computer.

7. *If you want to allow the user to remain logged-in indefinitely*, select **Yes** for the **Disable Session Timeout** option.

Note: By default, for added security, new user accounts are configured to timeout automatically.

8. *If you want to grant administrator rights to the selected account*, set **Allow Administrator Rights** to **Yes**.

Notes:

- Granting administrator rights does not also assign the Admin menu bar to a user. If the user requires access to Admin options, they must be

assigned the Admin view. For more information, see “Setting Default Account Menu Bars and Views” on page 95.

- Administrator rights are not granted by default, but they are required to create, delete, and edit accounts. User accounts without administrator rights cannot access Admin page information.

9. If you want to allow the user to manage nodes directly from the Orion Web Console, set **Allow Node Management Rights to **Yes**.**

Note: By default, node management rights are not granted. For more information about node management in the Orion Web Console, see “Managing Devices in the Web Console” on page 77.

10. If you want to allow the user to customize views, set **Allow Account to Customize Views to **Yes**.**

Note: By default, customized view creation is not allowed. Changes made to a view are seen by all other users that have been assigned the same view.

11. Designate whether or not to **Allow Account to Clear Events and Acknowledge Alerts.**

12. Select whether or not to **Allow Browser Integration.**

Note: Browser integration can provide additional functionality, including access to right-click menu options, depending on client browser capabilities.

13. If you want to enable audible alerts through the client browser, select a sound from the **Alert Sound list.**

Note: By default, sounds are stored in the `Sounds` directory, located at `C:\Inetpub\SolarWinds\NetPerfMon\Sounds`. Sounds in `.wav` format that are added to this directory become available as soon as the `Edit User Account` page refreshes.

14. Provide the maximum **Number of items in the breadcrumb list.**

Note: If this value is set to 0, all available items are shown in breadcrumb dropdown lists.

Setting Account Limitations

Account limitations may be used to restrict user access to designated network areas or to withhold certain types of information from designated users. The following procedure sets user account limitations.

To set user account limitations:

1. Log in to the Orion Web Console as an administrator.
2. Click **Settings** in the top right of the web console.

3. Click **Account Manager** in the Accounts grouping of the Orion Website Administration page.
4. Select the account that you want to limit, and then click **Edit**.
5. Click **Add Limitation** in the Account Limitations section.
6. Select the type of limitation to apply from the list, and then click **Continue**.

Notes:

- Account limitations defined using the Account Limitation Builder display as options on the Select Limitation page. Account limitations can be defined and set using almost any custom properties. For more information, see "Creating Account Limitations" on page 257.
 - Because Orion NetFlow Traffic Analyzer initially caches account limitations, it may take up to a minute for account limitations related to Orion NetFlow Traffic Analyzer to take effect in Orion NetFlow Traffic Analyzer.
7. Define the limitation as directed on the Configure Limitation page that follows. For more information about defining pattern-type limitations, see "Defining Pattern Limitations" on page 94.

Defining Pattern Limitations

Pattern limitations may be defined using **OR**, **AND**, **EXCEPT**, and **NOT** operators with **_** and ***** as wildcard characters. The following examples show how to use available operators and wildcard characters:

Note: Patterns are not case sensitive.

- `foo` matches only objects named "foo".
- `foo_` matches all objects with names consisting of the string "foo" followed by only one additional character, like `foot` or `food`, but not `seafood` or `football`.
- `foo*` matches all objects with names starting with the string "foo", like `football` or `food`, but not `seafood`.
- `*foo*` matches all objects with names containing the string "foo", like `seafood` or `Bigfoot`.
- `*foo*` OR `*soc*` matches all objects containing either the string "foo" or the string "soc", including `football`, `socks`, `soccer`, and `food`.
- `*foo*` AND `*ball*` matches all objects containing both the string "foo" and the string "ball", including `football` but excluding `food`.

- `*foo* NOT ball` matches all objects containing the string "foo" that do not also contain the string "ball", including `food` but excluding `football`.
- `*foo* EXCEPT *ball*` matches all objects containing the string "foo" that do not also contain the string "ball", including `food` but excluding `football`.

You may also group operators using parentheses, as in the following example.

`(*foo* EXCEPT b) AND (all OR sea)` matches `seafood` and `footfall`, but not `football` or `Bigfoot`.

Setting Default Account Menu Bars and Views

The Default Menu Bar and Views section provides several options for configuring the default menu bar and views for your user account. The following procedure is a guide to setting these options.

To set default menu bar and view options:

1. Log in to the Orion Web Console as an administrator.
2. Click **Settings** in the top right of the web console.
3. Click **Account Manager** in the Accounts grouping of the Orion Website Administration page.
4. Select the account that you want to configure, and then click **Edit**.
5. Scroll down to **Default Menu Bar and Views**.
6. Select a **Home Tab Menu Bar** from the available list.

Note: This is the default menu bar displayed when you click **Home** in the Orion Web Console. If you are editing a user account that must have administrator privileges, set the **Home Tab Menu Bar** to **Admin**.

7. Select a **Network Tab Menu Bar** from the available list.

Note: This is the default menu bar displayed when you click **Network** in the Orion Web Console. If you are editing a user account that must have administrator privileges, select **Network_Admin**.

8. Select a **Home Page View**.

Note: If no **Home Page View** is specified, the default is designated to be the same as the page that is specified in the **Default Summary View** field below.

9. *If the Home Page View you have selected refers to a specific network device*, select a **Default Network Device** by clicking **Edit** and selecting from the list of available devices on the next page.

Note: If the **Home Page View** you have selected does not require a specific network device, Orion NPM will select a device to display, automatically.

10. Select a **Default Summary View** for the account.

Note: This is typically the same as the **Home Page View**.

11. *If you want all reports to be available for the account*, select **\Reports** from the Report folder list in the Default Menu Bars and Views area.

Note: If you are creating a new user, you must designate the **Report Folder** the new account is to use to access Orion reports. By default, no report folder is configured for new users. The Reports directory is located in the Orion NPM installation directory: `C:\Program Files\SolarWinds\Orion\`.

12. *If you want to designate default Node and Volume Details Views for this account*, expand **Account's Orion General Settings**, and then select both an appropriate **Node Detail View** and an appropriate **Volume Details View**.

13. *If you want to designate a default Interface Details View for this account*, expand **Account's Network Performance Monitor Settings**, and then select an appropriate **Interface Details View**.

14. Click **Submit**.

Configuring an Account Report Folder

Reports may be assigned to an account by creating sub-directories within the Reports directory. Desired reports are included within the sub-directory, and the sub-directories are then made available for assignment to an account. This provides a level of security when reports are included in a view or added as custom menu items. For more information, see "Creating and Editing External Website Views" on page 59.

To configure an account report folder:

1. Log in to the Orion Web Console as an administrator.
2. Click **Settings** in the top right of the web console.
3. Click **Account Manager** in the Accounts grouping of the Orion Website Administration page.
4. Select the account you want to configure, and then click **Edit**.
5. *If you want all reports to be available for the account*, select **\Reports** from the Report folder list in the Default Menu Bars and Views area.

Note: If you are creating a new user, you must designate the **Report Folder** the new account is to use to access Orion reports. By default, no report folder is configured for new users. The Reports directory is located in the Orion NPM installation directory: `C:\Program Files\SolarWinds\Orion\`.

6. Click **Submit**.

Configuring Audible Web Alerts

When browsing the Orion Web Console, audible alerts can be sounded whenever new alerts are generated. When enabled, you will receive an audible alert the first time, after login, that an alert is displayed on the page. This alert may come from either an alert resource or the Alerts view. You will not receive audible alerts if the Alerts view or the alert resource you are viewing is empty.

Following the initial alert sound, you will receive an audible alert every time an alert is encountered that was triggered later than the latest alert that has already been viewed.

For example, a user logs in and sees a group of alerts with trigger times ranging from 9:01AM to 9:25AM, and the user receives an audible alert. If the user browses to a new page or allows the current page to auto-refresh, a new alert sounds if and only if an alert triggered later than 9:25AM is then displayed.

To enable audible web alerts:

1. Log in to the Orion Web Console as an administrator.
2. Click **Settings** in the top right of the web console.
3. Click **Account Manager** in the Accounts grouping of the Orion Website Administration page.
4. Select the account you want to configure.
5. Click **Edit**.
6. Select the sound file you want to play when new alerts arrive from the **Alert Sound** list.

Note: By default, sounds are stored in the `Sounds` directory, located at `C:\Inetpub\SolarWinds\NetPerfMon\Sounds`. Sounds in `.wav` format that are added to this directory become available as soon as the Edit *User* Account page refreshes.

7. Click **Submit**.

Chapter 7

Managing Orion NPM Polling Engines

To ensure that your polling engines are optimized to run at peak performance, you will need to occasionally tune them. If you use more than one polling engine, you will need to balance the load so that each engine can perform optimally.

Viewing Polling Engine Status

Orion System Manager provides the NPM Engine Status window that gives an immediate report of the performance of your Orion NPM polling engine.

To view the polling engine status report:

1. Click **Start > All Programs > SolarWinds Orion > System Manager**.
2. Click **File > Polling Status**.
3. *If you want to view the NPM Engine Status report in a text editor*, click **Copy to Clipboard**, and then paste (**Ctrl+V**) the report into the text editor.

The following sections detail the information provided in each of the four groups listed in the NPM Engine Status window.

NetPerfMon Engine

The NetPerfMon Engine group provides up-to-the-second information about polling the full inventory of network nodes, interfaces, and volumes monitored by Orion NPM, as detailed in the following table:

Statistic	Description
Network Node Elements	The number of nodes currently monitored by Orion NPM.
Interface Elements	The number of interfaces currently monitored by Orion NPM.
Volume Elements	The number of volumes currently monitored by the Orion NPM.
Date Time	The current Date and Time, as reported by the Orion NPM server.
Paused	If, for any reason, the polling engine stops or pauses, <code>True</code> is returned. Otherwise, if the polling engine is operating normally, <code>False</code> is returned.
Max Outstanding Polls	The maximum number of poll requests that the Orion NPM polling engine is allowed to maintain in queue. Additional poll requests made after the polling engine queues this number of polls will be ignored.

Status Pollers

The Status Pollers group provides information about the number and rate of SNMP and ICMP device status polls the Orion NPM polling engine is currently completing, as detailed in the following table:

Statistic	Description
ICMP Status Polling index	The number of monitored objects (<i>i.e.</i> nodes, interfaces, and volumes) the Orion NPM polling engine has successfully used ICMP to poll for status.
SNMP Status Polling index	The number of monitored objects (<i>i.e.</i> nodes, interfaces, and volumes) the Orion NPM polling engine has successfully used SNMP to poll for status.
ICMP Polls per second	The number of ICMP polls for device status that the Orion NPM polling engine is currently completing, per second.
SNMP Polls per second	The number of SNMP polls for device status that the Orion NPM polling engine is currently completing, per second.
Max Status Polls Per Second	The maximum number of poll requests for device status that the Orion NPM polling engine is allowed to attempt per second.

Packet Queues

The Packet Queues group reports the number of DNS, ICMP, and SNMP polls the Orion NPM polling engine is currently completing, as detailed in the following table:

Statistic	Description
DNS Outstanding	The number of DNS polls the Orion NPM polling engine currently has queued to complete.
ICMP Outstanding	The number of ICMP polls the Orion NPM polling engine currently has queued to complete.
SNMP Outstanding	The number of SNMP polls the Orion NPM polling engine currently has queued to complete.

Statistics Pollers

The Statistics Pollers group provides information about the number and rate of SNMP and ICMP device statistics polls the Orion NPM polling engine is currently completing, as detailed in the following table:

Statistic	Description
ICMP Statistics Polling index	The number of monitored objects (<i>i.e.</i> nodes, interfaces, and volumes) the Orion NPM polling engine has successfully used ICMP to poll for statistics.
SNMP Status Polling index	The number of monitored objects (<i>i.e.</i> nodes, interfaces, and volumes) the Orion NPM polling engine has successfully used SNMP to poll for statistics.
ICMP Polls per second	The number of ICMP polls for device statistics the Orion NPM polling engine is currently completing, per second.

Statistic	Description
SNMP Polls per second	The number of SNMP polls for device statistics the Orion NPM polling engine is currently completing, per second.
Max Statistics Polls Per Second	The maximum number of poll requests for device statistics the Orion NPM polling engine is allowed to attempt per second.

Configuring Polling Engine Settings

Settings for your Orion NPM polling engine are configured on the Orion Polling Settings view within the Orion Web Console.

To open the Orion Polling Settings view:

1. Log in to the Orion Web Console as an administrator.
2. Click **Settings** in the top right of the web console.
3. Click **Polling Settings** in the Settings group.

The following section provides descriptions of the settings configurable on the Orion Polling Settings view.

Orion Polling Settings

The following poller settings are configurable on the Orion Polling Settings view.

Polling Intervals

The following settings configure default polling intervals. To apply poller settings, click **Re-Apply Polling Intervals to all Nodes, Interface, and Volumes**.

Default Node Poll Interval

Devices are regularly polled to determine status and response time on this designated interval. By default, this interval is 120 seconds.

Default Interface Poll Interval

Interfaces are regularly polled to determine status and response time on this designated interval for Interfaces. By default, this interval is 120 seconds.

Default Volume Poll Interval

Volumes are regularly polled to determine status and response time on this designated interval. By default, this interval is 120 seconds.

Default Rediscovery Interval

Your entire network is polled on this interval to detect any re-indexed interfaces. Monitored network devices are also checked for IOS upgrades permitting EnergyWise support. By default, this interval is 30 minutes.

Lock custom values

This option is enabled by default. Enabling this option automatically saves any polling customizations made on the Orion Polling Settings view.

Polling Statistics Intervals

The following settings configure default polling intervals for device statistics. To apply poller settings, click **Re-Apply Polling Statistic Intervals to all Nodes, Interface, and Volumes**.

Default Node Statistics Poll Interval

Device performance statistics are regularly polled on this interval. By default, this interval is 10 minutes.

Default Interface Statistics Poll Interval

Interface performance statistics are regularly polled on this interval. By default, this interval is 9 minutes.

Default Volume Statistics Poll Interval

Volume performance statistics are regularly polled on this interval. By default, this interval is 15 minutes.

Database Settings

The following options configure Orion database maintenance and retention settings.

Note: Changes to database maintenance and retention settings do not take effect until the SolarWinds Network Performance Monitor service is restarted.

Archive Time

The Archive Time is the time of day when Orion database maintenance occurs. For more information, see “Database Maintenance” on page 278.

Detailed Statistics Retention

All statistics collected on any basis shorter than 1 hour are summarized into hourly statistics after the period of time designated as the Detailed Statistics Retention period. By default, this period is 7 days.

Hourly Statistics Retention

All statistics collected on any basis shorter than 1 day but longer than 1 hour are summarized into daily statistics after the period of time designated as the Hourly Statistics Retention period. By default, this period is 30 days.

Daily Statistics Retention

All statistics in the Orion database that are collected on a daily basis are kept for this designated period of time. By default, this period is 365 days.

Events Retention

All network events data is deleted from the Orion database after the period of time designated by the Events Retention has passed after the event ending time. By default, this period is 30 days.

Syslog Messages Retention

All received Syslog messages are kept for the period of time designated. By default, this period is 7 days.

Trap Messages Retention

All received trap messages are kept for the period of time designated. By default, this period is 30 days.

Discovery Retention

All configured discovery profiles are kept for the period of time designated. By default, this period is 60 days. For more information about discovery profiles, see “Discovering and Adding Network Devices” on page 25.

Network

The following settings configure ICMP and SNMP requests.

ICMP Timeout

All ICMP (ping) requests made by the Orion poller time out if a response is not received within the period designated. By default, this period is 2500ms.

ICMP Data

This string is included within all ICMP packets sent by Orion NPM.

SNMP Timeout

All SNMP requests made by the Orion poller time out if a response is not received within the period designated. By default, this period is 2500ms.

SNMP Retries

If a response to an SNMP poll request made by the Orion poller is not received within the configured SNMP Timeout, the Orion poller will conduct as many retries as designated by this value. By default, this value is 2.

ESX API Timeout

All VMware ESX API requests made by the Orion poller time out if a response is not received within the period designated. By default, this period is 30000ms. For more information about VMware ESX polling, see “Monitoring VMware ESX Servers” on page 119.

Perform reverse DNS lookup

If you want Orion NPM to perform reverse DNS lookups on monitored DHCP nodes, confirm that this option is checked. By default, reverse DNS lookup for DHCP nodes is enabled.

Calculations & Thresholds

The following settings designate methods for calculating availability and transmission rate baselines, select the Orion NPM node warning level and counter type, and indicate security preferences for community strings and other potentially sensitive information in the web console.

Availability Calculation (advanced)

This setting designates the type of calculation Orion NPM performs to determine device availability. For more information, see “Calculating Node Availability” on page 105.

Baseline Calculation (advanced)

Upon startup, Orion NPM can calculate a baseline for the transmission rates of the various elements of your network. This baseline is used as a starting point for any comparison statistics. For more information, see “Calculating a Baseline” on page 105.

Allow Secure Data on Web (advanced)

In the interest of security, sensitive information about your network is not viewable in the Orion Web Console. However, if your network is properly secured, you may check this option to allow the viewing of community strings and other potentially sensitive information within the web console.

Note: This setting does not affect the display of custom reports that you export to the web. For more information see “Creating Reports” on page 185.

Node Warning Level

Devices that do not respond to polling within this designated period of time display as Down in the web console. By default, this value is 120 seconds.

Counter Rollover

This option sets the type of counter Orion NPM is to use. For more information, see “Handling Counter Rollovers” on page 42.

Calculating Node Availability

The Availability Calculation setting on the Orion Polling Settings view provides a choice between the following two methods for determining device availability.

Node Status:

The default method is based upon the historical up or down status of the selected node. The selected node is polled for status on the Default Node Poll Interval defined on the Orion Polling Settings view. For more information, see “Orion Polling Settings” on page 101.

If the selected node responds to a ping within the default interval, the node is considered up, and a value of 100 is recorded in the Response Time table of the Orion database. If the node does not respond to a ping within the default interval, the node is considered down and a value of 0 is recorded in the Response Time table of the Orion database. To calculate node availability over a selected time period, the sum of all Response Time table records for the selected node over the selected time period is divided by the selected time period, providing an average availability over the selected time period.

Percent Packet Loss:

The second method is a more complicated calculation that effectively bases the availability of a selected node on its packet loss percentage. As in the Node Status method, the selected node is polled for status. If it responds within the Default Node Poll Interval defined on the Orion Polling Settings view, a value of 100 is averaged with the previous 10 availability records. For more information, see “Orion Polling Settings” on page 101.

The result of the Percent Packet Loss calculation is a sliding-window average. To calculate node availability over a selected time period, the sum of all results in the Response Time table for the selected node over the selected time period is divided by the selected time period, providing an average availability over time.

Note: The Percent Packet Loss method introduces a historical dependency into each availability node record. In general, it is best to leave calculations based on Node Status unless you specifically need node availability based on packet loss.

Calculating a Baseline

On a new install or after a shutdown, when the SolarWinds Network Performance Monitor service starts, there is no current network data in your Orion database. In this situation, by default, Orion NPM calculates a baseline for the transmission rates of the various elements of your network. To calculate this baseline, all network resources are polled immediately upon startup, and then, as soon as the initial poll is complete, the network is polled again. The resulting two sets of data are used to calculate a nearly instant baseline view of your network performance.

If you do not need statistics immediately, or if you do not want Orion NPM to calculate a baseline at startup, disable baseline calculation at startup by setting the Baseline Calculation option on the Orion Polling Settings view to **False**. For more information, see “Configuring Polling Engine Settings” on page 101.

Note: Baseline calculation requires significant data gathering and processing. Until baseline calculation is completed, both Orion NPM server performance and the CPU performance of some of network routers may be adversely affected.

Setting the Node Warning Interval

A device may drop packets or fail to respond to a poll for many reasons. Should the device fail to respond, the device status is changed from Up to Warning. On the Node Warning Interval tab, you specify how long it will remain in the Warning status before it is marked as Down. During the interval specified, the service performs “fast polling” to continually check the node status.

Notes:

- To reduce the amount of packet loss reported by Orion NPM, configure the polling engine to retry ICMP pings a specific number of times before reporting packet loss. To do this, add the string value: “Response Time Retry Count” to the Windows Registry in the `Settings` folder of: `HKEY_LOCAL_MACHINE\SOFTWARE\SolarWinds.Net\SWNetPerfMon\`. Set the value data to the number of retries you prefer.
- You may see events or receive alerts for down nodes that are not actually down. This can be caused by intermittent packet loss on the network. Set the Node Warning Interval to a higher value to avoid these false notifications.

Polling Engine Tuning

By default, Orion NPM conducts a maximum of 30 status and 30 statistical polls per second. This default setting is adequate for most networks and ensures that the traffic load on the network is both small and evenly distributed across the polling cycle. In some cases, like when monitoring a very large network or when polling devices very frequently, it is necessary to increase these settings so Orion NPM can complete polling within the specified period. SolarWinds provides the Polling Engine Tuning tool to suggest and set values for maximum status polls per second and maximum statistics polls per second.

To tune your polling engine using the Polls Per Second Tuning tool, click **Start > All Programs > SolarWinds Orion > Advanced Features > Polls Per Second Tuning**, and then adjust each slider to set the maximum polls per second and click **OK**.

Note: Setting these values too high can cause excessive CPU load.

Estimating a Good Value

If you do not have access to the Polling Engine Tuner, you can estimate the appropriate values for these settings with the following formula:

$$\text{Maximum Polls per Second} = 2 \left(\frac{\text{Interfaces} \times \text{PPI}}{60 \times \text{PRI}} + \frac{\text{Nodes}}{60 \times \text{PRN}} + \frac{\text{Volumes}}{60 \times \text{PRV}} \right)$$

where:

PPI = Polls per Interface (normally two)

Interfaces = Number of Interfaces being monitored

PRI = Polling Rate for Interfaces (in minutes)

Nodes = Number of Nodes being monitored

PRN = Polling Rate for Nodes (in minutes)

Volumes = Number of Volumes being monitored

PRV = Polling Rate for Volumes (in minutes)

60 = seconds per minute

Note: Values for polling rates can be found within the Statistics tab of the System Manager Settings window. Numbers of nodes, interfaces, and volumes can be found in the Orion Web Console by clicking **Admin** in the Orion Web Console toolbar menu and then clicking either the **License Details** or **Database Details** in the Details grouping of the Orion Website Administration page.

Each interface may have multiple pollers assigned to it. For example, if you are collecting Interface Traffic and Interface Errors, then each interface has two pollers. Interface Traffic and Interface Errors Pollers each count as one poller. CPU collection on a node consumes only one poller, and collecting volume statistics on a volume also consumes only one poller. The following example shows how the MaximumPollsPerSecond formula works in a real-world situation.

Example

An Orion NPM system monitors a total of 250 nodes, 6000 total interfaces, and 100 volumes. It collects interface traffic and interface error statistics on each interface every five minutes. CPU utilization statistics are collected every 10 minutes, and volume usage is measured every 60 minutes.

Note: This calculated value can be rounded up to higher values to accommodate growth, but do not merely enter an arbitrarily large number into the **Maximum Polls per Second** registry settings. Too large a number will cause thrashing within the polling engine, resulting in lower performance.

Setting the Maximum Polls per Second

The Maximum Polls per Second can also be set using the Polls Per Second Tuning tool that is installed with Orion NPM. The following procedure opens the Polls Per Second Tuning tool and configures the Maximum Polls per Second for your Orion NPM polling engine.

Note: Maximum Polls per Second is the sum of **Maximum Node and Interface Status Polls** and **Maximum Statistics Collections**.

To set the Maximum Polls per Second:

1. Click **Start > All Programs > SolarWinds Orion > Advanced Features > Polls Per Second Tuning**.
2. Set the sliders for both **Maximum Node and Interface Status Polls** and **Maximum Statistics Collections**, as appropriate, and then click **OK**.

Note: Recommended values for both settings are provided. For simplicity, both **Maximum Node and Interface Status Polls** and **Maximum Statistics Collections** are given an estimated value. For more information about the formula used for this estimate, see “Estimating a Good Value” on page 107.

Using the Polling Engine Load Balancer

The Polling Engine Load Balancer is a useful tool for reassigning nodes to a new polling engine, deleting an unused polling engine, and performing load balancing between multiple polling engines. The tool is available within the Monitor Polling Engines application, which is an advanced feature of Orion NPM. Reassigning nodes to new polling engines may be required in the following situations:

- Moving or renaming your Orion NPM server
- Merging two or more Orion Network Performance Monitor servers

If these or any other conditions present the need for reassignment, complete the following procedure to reassign nodes to a new polling engine.

To reassign nodes to a different polling engine:

1. Click **Start > All Programs > SolarWinds Orion > Advanced Features > Orion Service Manager**.
2. Click **Shutdown Everything**.
Note: Confirm that you stop the SolarWinds Network Performance Monitor Service on all polling engines.
3. Click **Start > All Programs > SolarWinds Orion > Advanced Features > Monitor Poling Engines**.

4. Click **Servers > Poller Load Balancing**.
5. Select the nodes you want to reassign.
Note: Use `Shift + click` to highlight multiple consecutive rows, and use `Ctrl + click` to highlight multiple non-consecutive rows.
6. Click **Polling Engines > Move Selected Nodes to ***, substituting the target polling engine for *. The node is reassigned, and it reflects the name of the polling engine in the polling engine column.
7. Click **Start > All Programs > SolarWinds Orion > Advanced Features > Orion Service Manager** to restart Orion NPM services.

Chapter 8

Monitoring EnergyWise Devices

SolarWinds has partnered with Cisco to present EnergyWise to optimize energy usage on your network. The EnergyWise technology enables you to configure energy usage policies for EnergyWise-enabled and power-over-Ethernet (PoE) devices on your network.

What is EnergyWise?

EnergyWise is a Cisco technology developed to help you cut enterprise energy costs, address environmental concerns, and adhere to government directives around *green* technologies. By deploying EnergyWise capable devices and by enabling their energy-saving features, you can run business-critical systems in a fully powered state while allowing less critical devices on Power over Ethernet (PoE) ports to power down or drop into standby during off-peak hours.

EnergyWise Terminology

The following terms and concepts are provided in the EnergyWise MIB and used within EnergyWise resources in the Orion Web Console.

Domain

The EnergyWise MIB includes a field for labeling groups of EnergyWise capable devices, or entities, as members of a designated domain. With respect to Orion NPM, a single domain consists of all monitored EnergyWise entities defined as neighbors

Entity

Any network device, including switches, IP phones, and other components connected to Power over Ethernet (PoE) ports on EnergyWise capable devices, that either draws power from another network device or supplies power to another network device.

Importance Level

The Importance Level, or, simply, the Importance, is a priority value ranging from 1 to 100 that is assigned to both EnergyWise entities and EnergyWise policies. The higher the value, the more important the device and the less likely it is to be changed by energy policy modifications. When a policy application is attempted, the importance levels of the policy and the selected entity are compared to determine whether or not the policy is actually applied to the selected entity. If the policy importance level is greater than or equal to

the entity importance level, the policy is applied to the entity and the entity power level is changed. Likewise, as long as the importance level of an entity to which policy applications are attempted is greater than the importance levels of the policies applied, the entity power level will remain unchanged.

For example, an IP phone assigned an importance level of 80 is operating at a power level of 8. Policy A5, to change entity power levels to 5, has an importance of 50, and Policy B10, to change entity power levels to 10, has an importance of 95. If Policy A5 is applied to the phone, the phone will continue to operate at power level 8. However, if Policy B10 is applied to the phone, the phone power level changes to 10 in keeping with applied Policy B.

The importance value may be used to exempt specific entities from policy changes. For example, if all your emergency phones are on a single switch, the switch should never go into standby mode. To ensure that the switch hosting your emergency phones never goes into standby mode, set the switch importance to 100 so all policies with an importance of 99 and lower will have no effect on the emergency phone switch.

Keywords

The EnergyWise MIB provides for the identification of individual entities with unique labels. When an entity is initially configured, keywords may be added in series, as a string of words separated by commas without spaces, as shown in the following example:

```
Keyword1 , Keyword2 , Keyword3
```

Name

A user-friendly identifier for an EnergyWise entity or domain that may be assigned in the EnergyWise MIB when the entity or domain is configured. The default name for a switch is the hostname, and the default name for a Power over Ethernet (PoE) port is a shortened version of the port name. EnergyWise name values cannot include spaces. Modifying the EnergyWise name does not change the hostname of the device or the port name on the device. Omit spaces and refrain from using asterisks (*) in your name designations. Valid characters include alphanumeric characters and symbols, including #, (, %, !, or &.

Neighbor

Any two EnergyWise entities defined within the same domain are neighbors. Neighbors are capable of communicating EnergyWise events including the issuance of energy management directives.

Policy Level

The Policy Level is the power level of the policy that is currently applied to the selected entity.

Power Level

The Power Level is a designation of the amount of power an EnergyWise entity is allowed to draw, based on the policies currently acting upon it. The following table details available levels with category labels and icon colors.

Note: In some web console resources, the Power Level may be designated as either the EnergyWise Level or the EW Level.

Level	Label	Category	Color	Color Code			
10	Full	Operational (1)	Red	FF0000			
9	High		Operational (1)	Yellow	FFFF00		
8	Reduced						
7	Medium						
6	Frugal					Green	00FF00
5	Low						
4	Ready	Standby (0)				Blue	0000FF
3	Standby		Standby (0)	Brown	A52A2A		
2	Sleep						
1	Hibernate						
0	Shut	Nonoperational (-1)				Black	000000

Monitoring EnergyWise Devices with Orion NPM

Orion NPM provides the EnergyWise Summary view and related EnergyWise resources to help you monitor the energy expended on your network and the energy savings provided by EnergyWise-enabled devices. The following sections describe the EnergyWise Summary view and related EnergyWise resources.

Notes:

- Confirm that you have fully upgraded the IOS of all EnergyWise-enabled devices. For more information, consult your device documentation or www.cisco.com.
- The EnergyWise Summary view may not display by default in the Orion Web Console menu bar. For more information, see “Adding the EnergyWise Summary View” on page 117.

EnergyWise Summary View and Resources

By default, the EnergyWise Summary view provides the following resources:

All Nodes

The All Nodes resource included on the EnergyWise Summary view is configured to display your entire network in terms of EnergyWise capability. All nodes on your network are included in one of the following groups:

- The **EnergyWise Capable** group includes all monitored devices on which the EnergyWise technology is available but not yet enabled.
- The **EnergyWise Enabled** group includes all monitored devices on which the EnergyWise technology is both available and enabled.
- The **Not EnergyWise Capable** group includes all monitored devices that do not feature the EnergyWise technology.

EnergyWise NCM Information

Network Configuration Manager (NCM) is the Orion module used for network configuration and change management. This resource provides some basic information about how Orion NCM can be used to manage EnergyWise settings and policies on your network. For more information about Orion NCM, including the option to download a free trial, click **Download NCM**.

EnergyWise Reports

The EnergyWise Reports resource provides a list of reports detailing current EnergyWise readiness and energy savings across your network. For more information, see “EnergyWise Reports” on page 188.

Overall EnergyWise Savings

The Overall EnergyWise Savings resource provides a chart displaying the difference between the maximum amount of power that can be consumed and the actual amount of power that is consumed by all EnergyWise-enabled devices on your network as a percentage of the maximum amount of power that can be consumed.

Notes:

- Graphed bars represent average savings over the designated interval.
- Maximum and actual power consumption may be equivalent if you have not yet enabled an EnergyWise management policy on your network.

Overall Historical Power Consumption

The Overall Historical Power Consumption resource displays a chart of both the actual and the maximum amount of power consumed by all EnergyWise entities on your network.

Note: Maximum and actual power consumption may be equivalent if you have not yet enabled an EnergyWise management policy on your network.

Additional EnergyWise Resources

In addition to the resources provided by default on the EnergyWise Summary view, Orion NPM provides the following EnergyWise resources for inclusion on other Orion Web Console views, as indicated.

Note: For more information about the EnergyWise Summary view and its resources, see “EnergyWise Summary View and Resources” on page 114.

Device Power Consumption

The Device Power Consumption resource displays a chart of both the actual and the maximum power consumed by a selected EnergyWise entity.

Note: Maximum and actual power consumption may be equivalent if you have not yet enabled an EnergyWise policy on the selected entity.

EnergyWise Interface Details

This resource provides both information about the selected interface entity and the ability to immediately set the current Power Level of the selected interface entity. For more information about setting the current Power Level, see “Managing EnergyWise Interface Entity Power Levels” on page 117.

The EnergyWise Interface Details resource provides the following information about the selected interface entity:

- The Name listing provides the user-friendly EnergyWise entity name that has been defined for the viewed interface entity.
- The Power Level listing provides the colored icon and label associated with the power level currently reported by the viewed interface entity.

Note: The Power Level may be temporarily reset by clicking **Set Power Level** in this resource. For more information, see “Managing EnergyWise Interface Entity Power Levels” on page 117.

- The Policy Level listing provides the colored icon and label indicating the power level of the policy currently applied to the viewed interface entity.

Notes:

- The Policy Level is the same Power Level that is reported in the EnergyWise Policy Overview Calendar for the currently viewed interface entity at the current local time of the viewed interface entity.
- Policies are set either on the monitored device or with a configuration management utility like Orion Network Configuration Manager. For more information about Orion NCM, see www.solarwinds.com.
- The Keywords listing provides any keywords that have been defined for the viewed interface entity.

EnergyWise Node Details

The EnergyWise Node Details resource provides the following information about the selected node entity:

- The Domain Name listing provides the user-friendly name of the EnergyWise domain that has been defined for the viewed node entity.
- The Maximum Importance field indicates the importance level assigned to the viewed node.
- The Number of Neighbors field indicates the number of other currently monitored EnergyWise entities that are capable of communicating EnergyWise directives to the viewed node entity.
- The Status field communicates whether or not EnergyWise power management is currently enabled on the viewed node entity.

EnergyWise Policy Overview Calendar

The EnergyWise Policy Overview Calendar resource provides a visual record of policy- or configuration-based power level assignments for the viewed entity. EnergyWise recurrence policies assign power levels on an hourly basis, and this resource reports the assigned power levels, by the hour, for the viewed entity over a selected week.

Notes:

- All time references are in terms of the viewed entity and are not necessarily the time of the Orion NPM server.
- Policies are configured either on the monitored device itself or with a configuration management utility like Orion Network Configuration Manager (Orion NCM). For more information about Orion NCM, see www.solarwinds.com.

Entity Power Consumption

The Entity Power Consumption resource provides a chart displaying both the maximum amount of power that can be consumed and the actual amount of power that is consumed by the viewed EnergyWise-enabled entity.

Note: Maximum and actual power consumption may be equivalent if you have not yet enabled an EnergyWise policy on the selected device.

Adding the EnergyWise Summary View

The following procedure adds the EnergyWise Summary View to the Orion Web Console Views menu bar.

To add the EnergyWise Summary view to the web console Views menu bar:

1. Log in to the Orion Web Console as an administrator.
2. Click **Settings** in the top right of the web console.
3. Click **Customize Menu Bars** in the Customize grouping of the Orion Website Administration page.
4. Click **Edit** beneath the web console menu bar to which you want to add a link to the EnergyWise Summary view.
5. Click and drag the **EnergyWise** button from the Available items list on the left to the correct relative location in the Selected items list on the right.

Note: Selected items display from left to right in the selected menu bar as they are listed from top to bottom.

6. Click **Submit**.

Managing EnergyWise Interface Entity Power Levels

Although entity power levels are typically set using recurrence policies enacted by a configuration management utility like Orion Network Configuration Manager (Orion NCM), Orion NPM provides the ability to temporarily change the currently active power level of a selected EnergyWise interface entity from either of the following locations:

- The Interface Details view for the selected EnergyWise interface entity.
- The Web Console Node Management utility.

In either case, the following procedure provides the steps required to temporarily change the currently active power level of an EnergyWise interface entity.

Note: Any change made to the power level of a monitored EnergyWise entity is only effective until the next scheduled application of a defined recurrence policy.

Policies are configured either manually on the monitored device itself or with a configuration management utility like Orion NCM. For more information about Orion NCM, see www.solarwinds.com.

To reset the current power level of a monitored EnergyWise entity:

1. Log in to the Orion Web Console using an account with node management or administrator privileges.
2. *If you want to set the entity power level from the Interface Details view*, click **Set Power Level** in the EnergyWise Interface Details resource.
3. *If you want to use the Web Console Node Management utility*, complete the following steps:
 - a. Click **Home** in the Views toolbar, and then click **Manage Nodes** in the All Nodes resource.
 - b. Locate the device to edit using either of the following methods:
 - Use the search tool above the node list to search your Orion database for the parent node of the EnergyWise interface entity you want to reset.
 - Select an appropriate **Group by** criteria, and then click the appropriate group including the parent node of the EnergyWise interface entity you want to reset.
 - c. Click **+** to expand the parent node of the EnergyWise interface entity you want to reset, and then check the interface entity.
 - d. Click **More Actions > Override Power Level**.
4. Select the appropriate power level, and then click **OK**.

Chapter 9

Monitoring VMware ESX Servers

Orion NPM is capable of monitoring VMware ESXi and ESX Servers versions 3.5 and higher with VMware Tools installed. The VMware Settings view in the Orion Web Console provides both an overview of all discovered and monitored ESX Servers on your network and a library of the credentials ESX Servers require for monitoring. The following sections provide procedures for configuring VMware ESX Servers, adding them to the Orion database, and then monitoring them in the Orion Web Console.

Monitoring VMware ESX Servers with Orion NPM

The following table provides a summary of the methods used by Orion NPM to monitor VMware ESX Servers.

	3.5	3i	4	4i
Detection as ESX Server	VMware API			
Volumes	SNMP	N/A	SNMP	N/A
Interfaces	SNMP	N/A	SNMP	SNMP (partial)
CPU	SNMP	N/A	SNMP	SNMP
Memory	SNMP	N/A	SNMP	SNMP
Total Memory	VMware API			
Guest VM List	VMware API			

Requirements for Monitoring ESXi and ESX Servers

The following table provides minimal requirements for effectively using Orion NPM to monitor your VMware ESXi and ESX Servers.

Requirement	Description
SNMP	Orion NPM uses SNMP to monitor all ESXi and ESX Servers. For more information about enabling SNMP, see "Enabling SNMP on VMware ESXi and ESX Servers" on page 120.
VMware API	Orion NPM uses the VMware API to poll most performance data from devices running ESXi and ESX Server versions 3.5 and 4.0. For more information about creating required credentials, see "Creating ESX Server Credentials for Orion NPM" on page 125.
VMware Tools	VMware Tools must be installed on all ESXi and ESX Servers you intend to monitor. VMware Tools is not required on virtual machines running on monitored ESXi and ESX servers, but additional information, including IP addresses, are made available when VMware Tools is installed on virtual machines hosted by monitored ESXi and ESX Servers.

Enabling SNMP on VMware ESXi and ESX Servers

Orion NPM uses SNMP to poll performance data from VMware ESXi and ESX Servers. In order to make this performance data available to Orion NPM, you must enable SNMP on your VMware ESXi and ESX Servers, as described in the following sections:

Note: VMware only makes a limited amount of information available to Orion NPM SNMP queries for VMware ESXi and ESX Servers version 4.0 and higher. To access additional information, Orion NPM uses the VMware API.

- Enabling SNMP on VMware ESXi
- Enabling SNMP on ESX Server version 3.5
- Enabling SNMP on ESX Server Version 4.0

Enabling SNMP on VMware ESXi

The following procedure enables SNMP on VMware ESXi.

Note: The following procedure to enable SNMP requires the vSphere command line interface (CLI). The vSphere CLI is not packaged with your ESXi Server by default, so you will need to download it from VMware, as indicated.

To enable SNMP on VMware ESXi:

1. Download and install the VMware vSphere command line interface from the VMware Download Center (<http://downloads.vmware.com/d/>).
2. Use the vSphere CLI to view your ESXi server SNMP settings, as indicated in the following procedure:
 - a. In the `Perl\bin` directory of your vSphere installation, execute the following script:

```
perl ..\..\bin\vicfg-snmp.pl --server ip_address -s
```

Notes:

- `C:\Program Files\VMware\VMware vSphere CLI\Perl\bin` is the default location of the vSphere `Perl\bin` directory.
 - Replace `ip_address` with the IP address of your ESXi server, and replace `cstring` with the community string you are adding. For most environments, the community string `public` should be sufficient.
- b. Enter an appropriate user name at the prompt.

Note: For most environments, `root` should be sufficient.
 - c. Enter the associated password at the prompt.

3. Use the vSphere CLI to enable SNMP on your ESXi server, as indicated in the following procedure:

- a. In the `Perl\bin` directory of your vSphere installation, execute the following script to add an appropriate community string:

```
perl ..\..\bin\vicfg-snmp.pl --server ip_address -c cstring
```

Note: Replace *ip_address* with the IP address of your ESXi server, and replace *cstring* with the community string you are adding. For most environments, the community string `public` should be sufficient.

- b. Enter an appropriate user name at the prompt.

Note: For most environments, `root` should be sufficient.

- c. Enter the associated password at the prompt.

- d. In the `Perl\bin` directory of your vSphere installation, execute the following script to enable SNMP:

```
perl ..\..\bin\vicfg-snmp.pl --server ip_address -E
```

Note: Replace *ip_address* with the IP address of your ESXi server.

- e. Enter an appropriate user name at the prompt.

Note: For most environments, `root` should be sufficient.

- f. Enter the associated password at the prompt.

4. Reboot your ESXi server to allow settings to take effect.

Enabling SNMP on ESX Server version 3.5

The following procedure enables SNMP on ESX Server version 3.5.

Note: For more information about ESX Server 3.5 and ESX Server MIBs, see the VMware document, “Basic System Administration - ESX Server 3.5, ESX Server 3i version 3.5, VirtualCenter 2.5”.

To enable SNMP on ESX Server version 3.5:

1. Log in to your ESX Server using an account with administrative privileges.
2. Open `snmpd.conf` in a text editor.

Notes:

- The default location for `snmpd.conf` is `root/etc/snmp/snmpd.conf`.
- To use the default text editor, `nano`, in a default ESX Server version 3.5 environment, enter `nano /etc/snmp/snmpd.conf` at the prompt.

3. Locate the `rocommunity` setting and replace the default community string `public` with an appropriate read-only community string for your environment.

Note: Use commas to separate multiple community strings.

4. Save `snmpd.conf`, and then close your editor.

Note: If you are using nano, press `Ctrl+X` to close nano, and then enter `y` to save `snmpd.conf`.

5. Enter `chkconfig snmpd on` to enable SNMP when you reboot your ESX Server.
6. Enter `esxcfg-firewall -e snmpd` to allow SNMP through the ESX Server firewall.
7. Enter `service snmpd start` to start the SNMP service.
8. Confirm that SNMP polling is enabled on your ESX Server by entering the following command:

```
snmpwalk -v1 -c cstring localhost .1.3.6.1.4.1.6876 | grep 6876.1
```

Note: Replace `cstring` with the community string you provided above.

9. After entering the `snmpwalk` command, your ESX Server should return information similar to the following:

```
SNMPv2-SMI::enterprises.6876.1.1.0 = STRING: "VMware ESX Server"
```

```
SNMPv2-SMI::enterprises.6876.1.2.0 = STRING: "3.5.0"
```

```
SNMPv2-SMI::enterprises.6876.1.3.0 = OID: SNMPv2-SMI::enterprises.6876.60.1.3.5.0
```

```
SNMPv2-SMI::enterprises.6876.1.4.0 = STRING: "153875"
```

Note: The MIB OID `SNMPv2-SMI::enterprises.6876.1.4.0` returns the build number for your product, so it may not be the same as the build number displayed above.

Enabling SNMP on ESX Server Version 4.0

The following procedure enables both the system default SNMP daemon `snmpd` and the proprietary VMware SNMP daemon `vmware-hostd` on VMware ESX Server version 4.0.

Note: For more information about ESX Server 4.0 and ESX Server MIBs, see the VMware document, “vSphere Basic System Administration - Update 1, ESX 4.0, ESXi 4.0, vCenter Server 4.0”.

To enable SNMP on ESX Server version 4.0:

1. Log in to your ESX Server using an account with administrative privileges.
2. Open `snmp.xml` in a text editor.

Notes:

- The default location for `snmp.xml` is `root/etc/vmware/snmp.xml`.
- To use the default text editor, `nano`, in a default ESX Server version 4 environment, enter `nano /etc/vmware/snmp.xml` at the prompt.

3. Locate the `communities` tag, and then replace the default community string `public` with an appropriate read-only community string for your environment.

Note: Use commas to separate multiple community strings.

4. Locate the `enable` tag, and then confirm it is set to `true`.
5. Locate the `port` tag and confirm it is set to `171`.
6. Locate the `targets` tag and confirm it is set to `127.0.0.1@162/cstring`.

Note: Replace `cstring` with the community string you provided above.

7. Save `snmp.xml`, and then close your editor.

Note: If you are using `nano`, press `Ctrl+X` to close `nano`, and then enter `y` to save `snmp.xml`.

8. Enter `service snmpd stop` to confirm that the SNMP service is stopped.
9. Open `snmpd.conf` in a text editor.

Notes:

- The default location for `snmpd.conf` is `root/etc/snmp/snmpd.conf`.
- To use the default text editor, `nano`, in a default ESX Server version 4 environment, enter `nano /etc/snmp/snmpd.conf` at the prompt.

10. Edit `snmpd.conf` to include the following two lines:

```
view systemview included .1.3.6.1.4.1.6876
proxy -v 1 -c cstring 127.0.0.1:171 .1.3.6.1.4.1.6876
```

Note: Replace *cstring* with the community string you provided above.

11. Save `snmpd.conf`, and then close your editor.

Note: If you are using nano, press `Ctrl+X` to close nano, and then enter `y` to save `snmpd.conf`.

12. Enter `service mgmt-vmware restart` to restart the `mgmt-vmware` service.
13. Enter `service snmpd start` to start the SNMP service.
14. Enter `chkconfig snmpd on` to enable SNMP when you reboot your ESX Server.
15. Enter `esxcfg-firewall -e snmpd` to allow SNMP through the ESX Server firewall.
16. Confirm that SNMP polling is enabled on your ESX Server by entering the following command:

```
snmpwalk -v1 -c cstring localhost .1.3.6.1.4.1.6876 | grep
6876.1
```

Note: Replace *cstring* with the community string you provided above.

17. After entering the `snmpwalk` command, your ESX Server should return information similar to the following:

```
SNMPv2-SMI::enterprises.6876.1.1.0 = STRING: "VMware ESX"
SNMPv2-SMI::enterprises.6876.1.2.0 = STRING: "4.0.0"
SNMPv2-SMI::enterprises.6876.1.4.0 = STRING: "208167"
```

Note: The OID `SNMPv2-SMI::enterprises.6876.1.4.0` returns your product build number, so it may not be the same as the build number above.

Creating ESX Server Credentials for Orion NPM

Orion NPM uses the VMware API to poll most performance data from devices running ESX Server versions 3.5 and 4.0. Before Orion NPM can start polling ESX Servers, you must ensure that you have created credentials on your ESX Servers for the Orion NPM polling engine, as shown in the following procedure.

Note: Credentials created for the Orion NPM polling engine must have read-only rights, at minimum.

To create ESX Server credentials for Orion NPM:

1. Log in to your ESX Server using an account with administrative privileges.

Note: Typically, the `root` user name and password is sufficient.

2. **If you are prompted with an untrusted SSL certificate warning**, click **Ignore** to continue using the current SSL certificate.
3. Open the Users & Groups tab, and then click **Users**.
4. Right-click the Users view, and then click **Add**.
5. On the Add New user window, complete the following procedure:

Note: The **User Name** and **Password** provided in this step must be provided either in your initial network discovery or whenever you use Web Node Management to add the current ESX Server to Orion NPM for monitoring.

- a. Provide both a **Login** and a **User Name** for the Orion NPM polling engine.
 - b. Enter and confirm a **Password**.
 - c. Click **OK**.
6. Open the Permissions tab.
 7. Right-click the Permissions view, and then click **Add Permission**.
 8. On the Assign Permissions window, click **Add**.
 9. Select the user you just created, and then click **Add**.
 10. Click **OK** on the Select Users and Groups window.
 11. Select an appropriate role in the Assigned Role area, and then click **OK** on the Assign Permissions window.

The credential you have created is now available to use for monitoring your ESX Server. For more information about adding your ESX Server to the Orion database for monitoring, see “Managing VMware Credentials in the Web Console” on page 126.

Managing VMware Credentials in the Web Console

Orion NPM allows you to manage VMware credentials like you manage SNMP credentials using either of the following methods:

- Before starting a network discovery, the Network Sonar Wizard provides the Local ESX Credentials for VMware view on which you can choose to poll for ESX devices and then provide required VMware credentials. For more information, see “Network Discovery Using the Network Sonar Wizard” on page 25.
- After completing a network discovery that found ESX servers, you can edit credentials associated with any monitored ESX Server on the Web Node Management view of the web console. For more information, see “Editing Device Properties” on page 83.

Adding ESX Servers for Monitoring

VMware ESX Servers are added to the Orion database in the same ways that other devices are added for monitoring in the Orion Web Console. Add ESX Servers to your Orion database using either of the following methods:

- Network Sonar Discovery is the recommended method for adding ESX Servers for monitoring in the Orion Web Console. With Network Sonar Discovery, you can define all required credentials at once on the Local ESX Credentials for VMware view. For more information, see “Network Discovery Using the Network Sonar Wizard” on page 25.
- Web Node Management is an alternative method that is optimal when you are only adding a few selected devices. For more information, see “Adding Devices for Monitoring in the Web Console” on page 78.

Chapter 10

Monitoring Wireless Networks

Orion NPM can monitor any 802.11 IEEE-compliant autonomous access point (AP) or wireless controller. Details about your access points (AP), wireless clients, wireless controllers, thin APs, and rogue APs can all be monitored using Orion NPM. Wireless device monitoring is configured, customized, and managed using the Orion Web Console, as shown in the following sections.

Getting Started

Orion Network Performance Monitor automatically recognizes your wireless APs and controllers as wireless devices after they have already been added to the Orion database. For more information on adding devices to Orion, see "Discovering and Adding Network Devices" on page 25.

The wireless interfaces are not found during discovery process. Instead, after the wireless device is added to Orion and an inventory is performed, each wireless interface found is added to the database and polling begins.

Migrating Data from the Wireless Networks Module

If you have already owned an older version of the Wireless Network module and it was installed, polling your wireless devices, before you upgraded to Orion NPM version 9.5, Orion NPM will automatically migrate your historical data to the new format used in Orion NPM version 9.5.

Notes:

- The wireless migration will not be performed during installation or configuration. The migration is performed in batches during scheduled database maintenance. For more information, see "Database Maintenance" on page 278.
- The migration will notify users when a given node is migrated and when all nodes have been migrated in the Orion event log.
- You will not see historical data immediately because this process is throttled.

Viewing Wireless Data

The Wireless Summary view in the Orion NPM Web Console displays a list of all wireless APs and clients connected to each AP. Access point details include IP address, device type, SSID, channels used, and the number of clients currently

connected. Client details include client name, SSID, IP Address, MAC Address, Received Signal Strength Indication (RSSI), time connected, data rate, bytes received and bytes transmitted. The following procedure presents the steps to view wireless access points and clients in Orion NPM.

Note: The wireless details views uses device-specific node details views to display statistics. For more information, see “Views by Device Type” on page 49.

To view wireless access points and clients:

1. Log in to the Orion Web Console as an administrator.
2. Click **Wireless** in the Views toolbar.
3. **If you want to view access points**, select `Access Points` from the **Show** list.
4. **If you want to view clients**, select `Clients` from the **Show** list.
5. **If you want to filter the view using groups**, select a method to group access points or clients from the Group by list.
6. **If an access point has clients currently connected**, expand the access point name to show the list of clients connected.
7. **If you want to search for access points or clients**, type your search string in the **Search** field, and then click **Search**.

Clicking any access point opens the Node Details view.

Removing a Wireless Device

Removing wireless devices from Orion NPM is performed the same way as removing any node from Orion. For more information, see "Deleting Devices from Monitoring" on page 81.

Note: All historical wireless statistics for removed devices are deleted from the database when nightly maintenance is next completed. For more information, see “Running Database Maintenance” on page 278.

Chapter 11

Monitoring Network Events

To ease your network management workload, Orion NPM logs all events that occur to any monitored devices on your network. Orion NPM then displays these events, both in the Orion Web Console and in System Manager, so you can view and acknowledge them as your network management policies require.

Viewing Event Details in the Web Console

Orion NPM logs network events and lists them in the readily customizable Events view of the Web Console. Events are shown in order of occurrence, and they may be viewed by device, date and time, and event or device type.

Note: The Network Event Log is maintained as part of the Nightly Database Maintenance plan defined within the Database Settings area of the Orion Polling Setting page in the Orion Web Console. Records are kept for the number of days specified Events Retention field (the default is 30 days). For more information, see “Orion Polling Settings” on page 101.

To view event details in the Web Console:

1. Click **Start > All Programs > SolarWinds Orion > Orion Web Console**.
2. Log in to the Orion Web Console, and then click **Events** in the Views toolbar.
3. *If you want to filter your events view by device*, select the **Network Object** or **Type of Device** to which you want to limit your view in the **Filter Devices** area.
4. *If you want to limit your events view to show only events of a specific type*, select the appropriate **Event Type** in the Filter Events area.
5. *If you only want to see events from a specific period of time*, complete either of the following options:
 - Select a predefined period from the **Time Period** menu.
 - Select **Custom** from the **Time Period** menu, and then click the appropriate fields to provide **Begin** and **End** dates and times.
6. In the **Show X Events** field, provide the maximum number of events you want to view.
7. *If you want to show all events, including events that have already been cleared*, check **Show Cleared Events**.
8. Click **Refresh** to complete your events view configuration.

Acknowledging Events in the Web Console

Acknowledging network events is straightforward in the Web Console, as shown in the following procedure.

To acknowledge events in the Web Console:

1. Click **Start > All Programs > SolarWinds Orion > Orion Web Console**.
2. Log in to the Orion Web Console, and then click **Events** in the Views toolbar.
3. Provide appropriate filter criteria for the displayed events. For more information, see “Viewing Event Details in the Web Console” on page 129.
4. Click **Refresh** to ensure that all selected view criteria take effect.
5. Check individual events to acknowledge or click **Select All**.
6. Click **Clear Selected Events**.

Viewing Event Details in System Manager

Orion NPM logs all network events and lists them in the Event Details window, with the most recent events at the top. Events may be viewed by any combination of Date and Time, Event Type, and Network Object.

Note: The Network Event Log is maintained as part of the Nightly Database Maintenance plan defined within the Database Settings area of the Orion Polling Setting page in the Orion Web Console. Records are kept for the number of days specified Events Retention field (the default is 30 days). For more information, see “Orion Polling Settings” on page 101.

To view event details:

1. Click **Start > All Programs > SolarWinds Orion > System Manager**.
2. Click **Events > Event Details** or click **Events** on the toolbar to view a log of all the events recorded by your system.
Note: The Current Events window displays current network events by default. Events are color-coded by type with corresponding icons.
3. ***If you want to view a summary of all recorded events, listed by defined type, click Events > Event Monitor.***
4. ***If you want to view network events by Date or Time, perform the following steps:***
 - a. Click **Past Events** at the bottom of the Current Events window.
 - b. Enter an appropriate **Start Date/Time** in mm/dd/yyyy hh:mm format.

- c. Enter an appropriate **End Date/Time** in mm/dd/yyyy hh:mm format.
 - d. *If you have finished entering criteria*, click **Search**.
5. *If you want to view network events by Type*, click **Past Events** at the bottom of the Current Events window, select the type of event from the **(All Events)** menu at the top of the Current Events window, and then click **Search**.
 6. *If you want to view network events by Network Object*, click **Past Events** at the bottom of the Current Events window, select the available network object from the **(All Network Objects)** menu at the top of the Current Events window, and then click **Search**.

Note: You may need to maximize the Past Network Performance Monitor Events window to see the **(All Network Objects)** menu.

Acknowledging Network Events in System Manager

Events may be acknowledged and cleared from the Event Details window individually, by type, or by selection. Upon acknowledgement, events are cleared from the Event Details view, but they are not cleared from the database.

Note: The Network Event Log, as displayed in the Event Details window, is maintained as part of the Nightly Database Maintenance plan defined within the Database Settings area of the Orion Polling Setting page in the Orion Web Console. Records are kept for the number of days specified Events Retention field (the default is 30 days). For more information, see “Orion Polling Settings” on page 101.

To acknowledge and clear events:

1. Click **Events > Event Monitor** to view a summary of all recorded events, listed by type.
2. *If you want to acknowledge and clear an individual event*, click **X** for the selected event in the Ack column of the Current Events window.
3. *If you want to acknowledge and clear all events of a particular type*, click **X** next to the event type you want to acknowledge in the Network Events window.

Note: The following types of events may also be acknowledged and cleared directly, using a right-click in the Current Events window:

- All events
- Informational events
- Node Up and Node Down events
- Selected events

4. ***If you want to acknowledge and clear events by selection***, complete the following procedure:
 - a. `Ctrl+Click` or `Shift+Click` the events that you want to acknowledge and clear in the Current Events window or `Ctrl+Click`, or `Shift+Click` the event types that you want to acknowledge and clear in the Network Events window.
 - b. Right-click a selected event, and then click **Clear Selected Events**.

Chapter 12

Creating and Managing Alerts

Alerts are generated for network events, and they may be triggered by the simple occurrence of an event or by the crossing of a threshold value for a monitored Interface, Volume, or Node. Alerts can be set to notify different people on different days, different times of the day, different people for different events, or any combination of times, events, and people. Alerts may be configured to notify the people who need to know about the emergent event by several mediums, including:

- Sending an e-mail or page
- Playing a sound on the Orion Network Performance Monitor server
- Logging the alert details to a file
- Logging the alert details to the Windows Event Log
- Sending a Syslog message
- Executing an external program
- Executing a Visual Basic script
- E-mailing a web page
- Changing the value of a interface or node property
- Playing a text to speech output
- Sending a Windows Net Message
- Dialing a paging or SMS service
- Sending an SNMP trap
- Posting a URL to a web server

Alerts Predefined by Default

By default, Orion NPM provides a number of advanced alerts that are configured at install. The following alerts are available and functional as soon as the Orion Web Console is installed, giving you immediate insight into the status and performance of your network:

- Alert when a node goes down
- Alert when a node reboots

- Alert when a device experiences high packet loss
- Alert when a device experiences high response time
- Alert when a device experiences high transmit percent utilization

If, when you first log on to the Orion Web Console, there are any devices on your network that trigger any of these alerts, the Active Alerts resource on the Network Summary Home view displays the triggered alerts with a brief description. For more information about configuring these default advanced alerts, see “Creating and Configuring Advanced Alerts” on page 145.

Viewing Alerts in the Orion Web Console

The Triggered Alerts for All Network Devices page provides a table view of your alerts log. You can customize the list view by using the following procedure to select your preferred alert grouping criteria.

To view alerts in the Web Console:

1. Click **Start > All Programs > SolarWinds Orion > Orion Web Console**.
2. Click **Alerts** in the Views toolbar.
3. ***If you want to filter your alerts table view by device***, select the device to which you want to limit your alerts view in the **Network Object** field.
4. ***If you want to filter your alerts table by type of device***, select the device type to which you want to limit your alerts view in the **Type of Device** field.
5. ***If you want to limit your alerts table to show a specific type of alert***, select the alert type in the **Alert Name** field.
6. In the **Show Alerts** field, provide the number of alerts you want to view.
7. ***If you want to show all alerts, even if they have already been cleared or acknowledged***, check **Show Acknowledged Alerts**.
8. Click **Refresh** to complete your Alerts view configuration.

Viewing Alerts in Orion NPM System Manager

The Active Alerts window displays a table view of your alerts log. You can customize the list view by using the following procedure to select your preferred alert grouping criteria.

To view alerts in System Manager:

1. Click **Start > All Programs > SolarWinds Orion > System Manager**.
2. Click **Alerts > Active Alerts**.

3. Select either Basic Alerts or Advanced Alerts, as appropriate.
4. **If you are viewing basic alerts**, customize your view as follows:
 - a. Select either **Type of Alert** or **Node** from the **Group By** list to change the Active Alerts display.
 - b. Order your alerts list by any of the following criteria by clicking the appropriate column title: **Alert Time**, **Network Object**, or **Current Value**.
5. **If you are viewing advanced alerts**, customize your Active Alerts display as follows:
 - a. Select from the following options in the **Group By** list to change your Active Alerts view: **Alert Name**, **Object Type**, **Object Name**, **Alert State**, **Acknowledged**, **Acknowledged By**, or **No Grouping**.
 - b. Order your Alerts list by any of the following criteria by clicking the appropriate column: **Acknowledged**, **Alert Name**, **Alert State**, **Object Name**, **Triggered Time**, **Acknowledged By**, or **Acknowledge Time**.
6. Click **Refresh** at any time to display the most recently triggered alerts.

Configuring Basic Alerts

As you add new alerts to the system, they are listed with a number of predefined alerts in the Configure Alerts window.

To open the Configure Alerts window:

1. Click **Start > All Programs > SolarWinds Orion > System Manager**.
2. Click **Alerts > Configure Basic Alerts**.

The following options are available in the Configure Alerts window:

- To set the status of an alert as active or inactive, simply check or uncheck the target alert. Alerts can be activated or deactivated on an individual basis.
- To add a new alert, click **New Alert**. For more information, see “Creating a New Basic Alert” on page 136.
- To copy an alert, check the alert you to copy, and then click **Copy Alert**.
Note: This option is useful for quickly creating multiple very similar alerts. For more information, see “Configuring Basic Alert Copies” on page 141.
- To modify the properties of an existing alert, select the alert to modify, and then click **Edit Alert**. For more information, see “Editing the Name of an Existing Basic Alert” on page 136.

- To remove an alert from the list in the Configure Alerts window, select the alert to delete, and then click **Delete Alert**.
Note: If you only want to temporarily disable an alert without deleting it, simply uncheck it in the Configure Alerts window.
- To test the configuration of selected alerts, click **Test Alerts**. For more information, see “Testing a Basic Alert” on page 140.
- To temporarily disable your alert configuration, check **Temporarily Disable all Actions for All Alerts** to disable configured actions for all alerts. Each alert will still be recorded in the log and displayed in the Alerts window, but alert actions will not occur. This feature is particularly useful when working on a known network issue where additional alert actions are only an annoyance.

Orion NPM allows you to set alerts for a broad range of network conditions. The following procedures present the steps to create, configure, and edit basic alerts.

Creating a New Basic Alert

The following steps enable a new basic alert.

To create a new basic alert;

1. Click **Start > All Programs > SolarWinds Orion > System Manager**.
2. Click **Alerts > Configure Basic Alerts**.
3. Click **New Alert**.
4. Enter the name of your new alert in the **Name of Alert** field.
5. Check **Enable this Alert**.

Editing the Name of an Existing Basic Alert

The name of a basic alert may be changed using the following procedure.

To change the name of a basic alert:

1. Click **Start > All Programs > SolarWinds Orion > System Manager**.
2. Click **Alerts > Configure Basic Alerts**.
3. Check the alert you want to edit, and then click **Edit Alert**.
4. Click the **General** tab.
5. Enter the new name of your alert in the **Name of Alert** field.
6. Select **Enable this Alert**.
7. **If you are finished configuring your alert,** click **OK**.

Selecting the Monitored Property of a Basic Alert

Use the following steps to select the monitored network property of a basic alert.

To select the monitored property of a basic alert:

1. Click **Start > All Programs > SolarWinds Orion > System Manager**.
2. Click **Alerts > Configure Basic Alerts**.
3. Check your alert.
4. Click **Edit Alert**.
5. Click the **Property to Monitor** tab,
6. Select the new network property you want to monitor.

Note: For most properties a description is displayed at the bottom of the window upon selection. The system only allows you to select one property per alert action, replacing the previous selection with each new selection, so you can click on each property and view its description without needing to deselect it later.

7. *If you are finished configuring your alert*, click **OK**.

Selecting the Network Objects Monitored by a Basic Alert

Select the monitored network objects of a basic alert with the following procedure.

To select the monitored network objects of a basic alert:

1. Click **Start > All Programs > SolarWinds Orion > System Manager**.
2. Click **Alerts > Configure Basic Alerts**.
3. Check your alert.
4. Click **Edit Alert**.
5. Click the **Monitored Network Objects** tab.
6. Check the network objects to which you want to apply your alert.

Note: By default, all objects are selected. Individually uncheck the objects that you do not want to monitor for this alert, or use the **Clear All** and **Select All** buttons as appropriate.

7. *If you are finished configuring your alert*, click **OK**.

Setting the Alert Trigger of a Basic Alert

Set the alert trigger of a basic alert with the following procedure.

To set the alert trigger of a basic alert:

1. Click **Start > All Programs > SolarWinds Orion > System Manager**.
2. Click **Alerts > Configure Basic Alerts**.
3. Check your alert, and then click **Edit Alert**.
4. Click the **Alert Trigger** tab, and then follow the on-screen instructions to set alert trigger and reset conditions.

Note: When an alert is triggered, the specified actions result. The actions will not be repeated until the reset condition has first been satisfied.

5. *If you are finished configuring your alert*, click **OK**.

Setting the Time of Day for a Basic Alert

Set the time of day for a basic alert with the following procedure.

To set the time of day of a basic alert:

1. Click **Start > All Programs > SolarWinds Orion > System Manager**.
2. Click **Alerts > Configure Basic Alerts**.
3. Check your alert, and then click **Edit Alert**.
4. Click the **Time of Day** tab.
5. Enter the time period you want your alert to monitor. Your alerts will only trigger if your trigger condition is met within the time period entered.
6. Select the days on which you want your alert to monitor your network. Your alerts will only trigger if your trigger condition is met on the days selected.
7. *If you are finished configuring your alert*, click **OK**.

Setting the Alert Suppression for a Basic Alert

Set the alert suppression of a basic alert with the following procedure.

To set the alert suppression of a basic alert:

1. Click **Start > All Programs > SolarWinds Orion > System Manager**.
2. Click **Alerts > Configure Basic Alerts**.
3. Check your alert, and then click **Edit Alert**.

4. Click **Alert Suppression**, and then select one of the following options:
 - **Do not configure Alert Suppression for this Alert** if there is no condition under which your alert should be suppressed.
 - **Suppress this Alert if ANY of the selected Suppressions are Active** if there are any conditions under which your alert should be suppressed.
 - **Suppress this Alert only if ALL of the selected suppressions are Active** if you only want to suppress your copied alert in the event that a number of conditions are all met.
5. *If you selected to enable either ANY or ALL alert suppressions*, the following procedure configures your alert suppressions:
 - a. Click **Add**.
 - b. Click **Property to Monitor**.
 - c. Select a property that is relevant to your suppression.
 - d. Click **Network Object**.
 - e. Select the network objects that should be monitored for your suppression property.
 - f. Click **Suppression Trigger**.
 - g. Select condition states for the selected network object and property that will suppress your initial alert.
 - h. Select the suppressions that should be applied to your alert.

Note: You may edit or delete suppressions as needed by selecting suppressions and clicking **Edit** or **Delete**, respectively. For more information, see “Basic Alert Engine Suppression Examples” on page 316.
6. *If you are finished configuring your alert*, click **OK**.

Selecting the Actions of a Basic Alert

Select the actions of a basic alert with the following procedure.

To select the actions of a basic alert:

1. Click **Start > All Programs > SolarWinds Orion > System Manager**.
2. Click **Alerts > Configure Basic Alerts**.
3. Check the alert to which you are adding an action.
4. Click **Edit Alert**.
5. Click **Actions**.

6. Click **Add Alert Action** to select the actions that you want to occur in the event of an alert.
7. Follow the given instructions to configure each action. For more information about adding alert actions, see “Adding Alert Actions” on page 158.
Note: You may edit or delete actions as needed by selecting actions and clicking **Edit Alert Action** or **Delete Selected Action**, respectively.
8. *If you are finished configuring your basic alert*, click **OK**.

Testing a Basic Alert

Basic alert actions may be tested before activation to ensure proper configuration. The following procedure presents the steps to test a basic alert.

To test a basic alert:

1. Click **Start > All Programs > SolarWinds Orion > Advanced Features > Test Fire Alerts**.
2. Select **Alert on Network Node**.
3. Choose the network node that your alert references.
4. *If you are alerting on an interface*, click **Alert on Network Interface**, and then choose the interface that your alert references on your selected network node.
5. *If you are alerting on a volume*, click **Alert on Volume**, and then choose the volume that your alert references on your selected network node.
6. Choose the alert that you want to test from the **Select an Alert to test fire** drop down menu.
7. Click **Test Alert Trigger** to start test.
Note: Click **Test Alert Reset** upon completion of test to reset all triggers.
8. *If there are errors*, click **View Alert Error Log** to review the log.
9. *If you are done viewing errors and you want to clear the error log*, click **Clear Alert Error Log**.
10. Repeat the preceding procedure for each alert that you want to test.
11. *If you are done testing alerts*, click **Done**.

Configuring Basic Alert Copies

You may need to enable multiple basic alerts with similar criteria or alert actions. Use the Copy Alert function of the System Manager to configure multiple similar alerts that differ in only one or a few characteristics.

To copy a basic alert:

1. Click **Start > All Programs > SolarWinds Orion > System Manager**.
2. Click **Alerts > Configure Basic Alerts**.
3. Check the alert that you want to copy, and then click **Copy Alert**.
4. Click **General**.
5. Enter the name of your alert copy in the **Name of Alert** field.
6. Check **Enable this Alert**.

Changing the Name of a Copied Alert

The name of a copied alert may be changed using the following procedure.

To change the name of a copied alert:

1. Click **Start > All Programs > SolarWinds Orion > System Manager**.
2. Click **Alerts > Configure Basic Alerts**.
3. Check the alert that you want to rename, and then click **Edit Alert**.
4. Click **General**, and then enter the new name of your alert copy in the **Name of Alert** field.
5. Check **Enable this Alert**.
6. *If you are finished configuring your copied alert*, click **OK**.

Changing the Monitored Property of a Copied Alert

Change the monitored property of a copied alert with the following procedure.

To change the monitored property of a copied alert:

1. Click **Start > All Programs > SolarWinds Orion > System Manager**.
2. Click **Alerts > Configure Basic Alerts**.
3. Check the copied alert to change.
4. Click **Edit Alert**.
5. Click **Property to Monitor**.

6. Check the new network property that you want to monitor.

Note: For most properties a description is displayed at the bottom of the window upon selection. The system only allows you to select one property per Alert action, replacing the previous selection with each new selection, so you can click on each property and view its description without needing to deselect it later.

7. *If you are finished configuring your copied alert*, click **OK**.

Changing Network Objects Monitored by a Copied Alert

Change the monitored network objects of a copied alert with the following procedure.

To change the monitored network objects of a copied alert:

1. Click **Start > All Programs > SolarWinds Orion > System Manager**.
2. Click **Alerts > Configure Basic Alerts**.
3. Check the copied alert to change, and then click **Edit Alert**.
4. Click **Monitored Network Objects**, and then check the network objects to which you want to apply your copied alert.

Note: By default, all objects are selected. Individually uncheck the objects you do not wish to monitor for this alert, or use the **Clear All** and **Select All** buttons as appropriate.

5. *If you are finished configuring your copied alert*, click **OK**.

Changing the Alert Trigger of a Copied Alert

Change the alert trigger of a copied alert with the following procedure.

To change the alert trigger of a copied alert:

1. Click **Start > All Programs > SolarWinds Orion > System Manager**.
2. Click **Alerts > Configure Basic Alerts**.
3. Check the copied alert to change, and then click **Edit Alert**.
4. Click **Alert Trigger**, and then follow the on-screen instructions to set alert trigger and reset conditions.

Note: When an alert is triggered, the specified actions result. The actions will not be repeated until the reset condition has first been satisfied.

5. *If you are finished configuring your copied alert*, click **OK**.

Changing the Time of Day of a Copied Alert

Change the time of day of a copied alert with the following procedure.

To change the time of day of a copied alert:

1. Click **Start > All Programs > SolarWinds Orion > System Manager**.
2. Click **Alerts > Configure Basic Alerts**.
3. Check the copied alert to change.
4. Click **Edit Alert**.
5. Click **Time of Day**.
6. Enter the time period when you want your copied alert to monitor your network.

Note: Your alerts will only trigger if your trigger condition is met within the time period entered.

7. Select the days that you want your copied alert to monitor your network.

Note: Your alerts will only trigger if your trigger condition is met on the days selected.

8. *If you are finished configuring your copied alert, click **OK**.*

Changing the Alert Suppression of a Copied Alert

Change the alert suppression of a copied alert with the following procedure.

To change the alert suppression of a copied alert:

1. Click **Start > All Programs > SolarWinds Orion > System Manager**.
2. Click **Alerts > Configure Basic Alerts**.
3. Check the copied alert to change.
4. Click **Edit Alert**.
5. Click **Alert Suppression**, and then select one of the following options:
 - **Do not configure Alert Suppression for the Alert** if there is no condition under which your alert should be suppressed.
 - **Suppress this Alert if ANY of the selected Suppressions are Active** if there are any conditions under which your alert should be suppressed.
 - **Suppress this Alert only if ALL of the selected suppressions are Active** if you only want to suppress your copied alert in the event that a number of conditions are all met.

6. **If you selected to enable either ANY or ALL alert suppressions**, the following procedure configures your alert suppressions:
 - a. Click **Add**
 - b. Click the Property to Monitor tab, and then select a property that is relevant to your suppression.
 - c. Click the Network Object tab to select the network objects that should be monitored for your suppression property.
 - d. Click the Suppression Trigger tab to select condition states for the selected network object and property that will suppress your initial alert.
 - e. Select the suppressions that should be applied to your alert.

Note: Edit or delete suppressions as needed by selecting suppressions and clicking **Edit** or **Delete**, respectively. For more information, see “Basic Alert Engine Suppression Examples” on page 316.
7. **If you are finished configuring your copied alert**, click **OK**.

Changing the Actions of a Copied Alert

Change the actions of a copied alert with the following procedure.

To change the actions of a copied alert:

1. Click **Start > All Programs > SolarWinds Orion > System Manager**.
2. Click **Alerts > Configure Basic Alerts**.
3. Check the copied alert to change, and then click **Edit Alert**.
4. Click **Actions**, and then click **Add Alert Action** to select the actions you want to occur in the event of an alert.
5. Follow the given instructions to configure each action.

Note: You may edit or delete actions as needed by selecting actions and clicking **Edit Alert Action** or **Delete Selected Action**, respectively.
6. **If you are finished configuring your copied alert**, click **OK**.

Deleting a Basic Alert

When you no longer want to maintain a specific basic alert, use the following procedure to delete it.

To delete a basic alert:

1. Click **Start > All Programs > SolarWinds Orion > System Manager**.
2. Click **Alerts > Configure Basic Alerts**.

3. Check the alert that you want to delete.
4. Click **Delete Alert**.

Deactivating a Basic Alert

Use the following procedure to deactivate any basic alert.

To deactivate a basic alert:

1. Click **Start > All Programs > SolarWinds Orion > System Manager**.
2. Click **Alerts > Configure Basic Alerts**.
3. Clear the checkbox for the alert you want to deactivate.

Creating and Configuring Advanced Alerts

The Orion NPM advanced alert engine allows you to configure alerts with the following features:

- Sustained state trigger and reset conditions
- Multiple condition matching
- Automatic alert escalation
- Separate actions for triggers and resets

Advanced alerts are configured using the Advanced Alert Manager. For more information about the Advanced Alert Manager, see “Using the Advanced Alert Manager” on page 154.

Note: If you want to configure advanced alert features, such as timed alert checking, delayed alert triggering, timed alert resets, or alert suppression, check **Show Advanced Features** at the lower left of any Advanced Alert windows. For the purposes of this document, **Show Advanced Features** is always enabled.

Creating a New Advanced Alert

The following procedure creates a new advanced alert.

To create a new advanced alert:

1. Click **Start > SolarWinds Orion > Alerting, Reporting, and Mapping > Advanced Alert Manager**.
2. Click **View > Configure Alerts**.
3. Click **New**.

The Edit Alert window displays, providing an array of configurable alerting options, including trigger and reset conditions, suppressions, and date and time limitations. The following sections provide more information about configuring alert options.

Naming, Describing, and Enabling an Advanced Alert

Use the following steps, after clicking **New**, **Copy**, or **Edit** from the Manage Alerts Window, to name and describe an advanced alert.

To name and describe an advanced alert:

1. Click **Start > SolarWinds Orion > Alerting, Reporting, and Mapping > Advanced Alert Manager**.
2. Click **View > Configure Alerts**.
3. Click **New** or select an alert from the list, and then click **Copy** or **Edit**, as appropriate.
4. Click **General**, and type the name of your alert in the **Name of Alert** field.
5. Type a description of your alert in the description field, and then check **Enable this Alert**.
6. Type the Alert Evaluation Frequency and select Seconds, Minutes, or Hours from the list to set the checking interval for your alert.

Setting a Trigger Condition for an Advanced Alert

You can set the specific conditions for triggering an advanced alert with the following procedure.

To set the trigger conditions for an advanced alert:

1. Click **Start > SolarWinds Orion > Alerting, Reporting, and Mapping > Advanced Alert Manager**.
2. Click **View > Configure Alerts**.
3. Click **New** or select an alert from the list.
4. Click **Copy** or **Edit**, as appropriate, and then click **Trigger Condition**.
5. Select the Type of Property to Monitor (**Node**, **Interface**, **Volume**, **Custom Node Poller**, **Custom Interface Poller**, **Virtual Machine**, **Wireless Access Point**, or **Wireless Controller**) from the list.

Note: Generate trigger conditions in the text field by selecting appropriate descriptors from the linked context menus and by clicking **Browse (...)** on the left of the text field.

6. Click the linked text to select the number of conditions that you want to apply (**all**, **any**, **none**, **not all**). For more information about linked text conditions, see “Understanding Condition Groups” on page 153.
7. Click **Browse (...)** to view the following condition options:
 - To generate a condition based on a comparison of device states, click **Add a Simple Condition**.
Note: The **has changed** condition is only valid for the **Last Boot**, **IOS Version**, and **IOS Image Family** device characteristics.
 - To generate a condition based on a comparison of device fields and values, click **Add a Complex Condition**.
Note: The **has changed** condition is only valid for the **Last Boot**, **IOS Version**, and **IOS Image Family** device characteristics.
 - To define more application conditions, click **Add a Condition Group**.
 - To remove a selected condition, click **Delete Current Condition**.
 - To change the order of your conditions, click **Move Down** or **Move Up**.
8. **If you need an additional condition**, click **Add**, and then select the type of condition you want to add.
9. **If you need to delete a condition**, select the condition from the condition list, and then click **Delete**.

Notes:

- Conditions may be exported for use with other alerts by clicking **Export Conditions** and saving as appropriate.
- Click **Import Conditions** to import existing conditions from other alerts.

Warning: Imported trigger conditions automatically overwrite any existing trigger conditions.

10. **If you want to specify a time duration for the condition to be valid**, type the time interval and select Seconds, Minutes, or Hours from the list.
Note: You may need to delay alert trigger actions until a condition has been sustained for a certain amount of time. For example, an alert based on CPU load would not trigger unless the CPU Load of a node has been over 80% for more than 10 minutes. To set up a sustained-state trigger condition, at the bottom of the Trigger Condition tab, provide an appropriate amount of time the alert engine should wait before any actions are performed. By default, the alert triggers immediately, if the trigger condition exists. The maximum alert action delay is eight hours after the trigger condition is met.
11. **If you are finished configuring your advanced alert**, click **OK**.

Setting a Reset Condition for an Advanced Alert

Set specific conditions for resetting an advanced alert using the following steps.

To set the conditions for resetting an advanced alert:

1. Click **Start > SolarWinds Orion > Alerting, Reporting, and Mapping > Advanced Alert Manager**.
2. Click **View > Configure Alerts**.
3. Click **New** or select an alert from the list and click **Copy** or **Edit**.
4. Click **Reset Condition**.
5. *If you want a simple alert reset when trigger conditions no longer exist*, select **Reset when trigger conditions are no longer true**.
6. *If you want a conditional alert reset*, select **Reset this alert when the following conditions are met**.

Notes: Generate reset conditions in the text field by selecting appropriate descriptors from the linked context menus and by clicking **Browse (...)** on the left of the text field.

7. *If you want to copy the condition used on the Trigger Condition tab*, click **Copy From Trigger**.
8. Click the linked text to select the number of conditions to apply. For more information, see “Understanding Condition Groups” on page 153.
9. Click **Browse (...)** to view the following condition options:
 - To generate a condition based on a comparison of device states, click **Add a Simple Condition**.
 - To generate a condition based on a comparison of device fields and values, click **Add a Complex Condition**.
 - To further define condition application, click **Add a Condition Group**.
 - To remove a selected condition, click **Delete Current Condition**.
 - To change the order of your conditions, click **Move Down** or **Move Up**.
10. *If you need an additional condition*, click **Add**, and then select the type of condition you want to add.

11. **If you need to delete a condition**, select the condition from the condition list, and then click **Delete**.

Notes:

- Conditions may be exported for use with other alerts by clicking **Export Conditions** and saving as appropriate.
- Conditions from other alerts may be imported to the current alert by clicking **Import Conditions**.

Warning: Imported trigger conditions automatically overwrite any existing trigger conditions.

- Because there are many situations where the reset conditions are the opposite of, or are very similar to, the trigger conditions, SolarWinds has provided a function that copies the trigger conditions to the reset conditions. Click **Copy From Trigger** to add the trigger condition.

12. **If you want to specify a time duration for the condition to be valid**, type the time interval and select Seconds, Minutes, or Hours from the list.

Note: It is often appropriate to delay alert reset actions until a condition has been sustained for a certain amount of time. For example, an alert based on node status would not reset until the node has been up for more than five minutes. To establish a sustained-state reset condition, provide an appropriate interval at the bottom of the Reset Condition tab for the amount of time that the alert engine should wait before any actions are performed. The default setting is to reset the alert immediately, once the reset condition exists. The maximum interval between when the trigger condition first exists and when the corresponding alert action is performed is eight hours.

13. **If you are finished configuring your advanced alert**, click **OK**.

Setting a Suppression for an Advanced Alert

You can set the specific conditions for suppressing an advanced alert using the following procedure.

Note: Alert Suppression is only available if you have checked **Show Advanced Features** in the lower left of the Edit Advanced Alert window.

To set conditions for advanced alert suppression:

1. Click **Start > All Programs > SolarWinds Orion > Alerting, Reporting, and Mapping > Advanced Alert Manager**.
2. Click **View > Configure Alerts**.
3. Click **New** or select an alert from the list.
4. Click **Copy** or **Edit**, as appropriate.

5. Click Alert Suppression.

Note: Generate suppression conditions in the text field by selecting appropriate descriptors from the linked context menus and by clicking **Browse (...)** on the left of the text field.

6. If you want to copy the condition used on the Trigger Condition tab, click Copy From Trigger.**7. Click the linked text to select the number of conditions that you want to apply (all, any, none, not all). For more information about linked text conditions, see “Understanding Condition Groups” on page 153.****8. Click Browse (...) to view the following condition options:**

- To generate a condition based on a comparison of device states, click **Add a Simple Condition**.
- To generate a condition based on a comparison of device fields and values, click **Add a Complex Condition**.
- To further define the application of your conditions, click **Add a Condition Group**.
- To remove a selected condition, click **Delete Current Condition**.
- To change the order of your conditions, click **Move Down** or **Move Up**.

9. If you need an additional condition, click Add and then select the type of condition you want to add.**10. If you need to delete a condition, select the condition from the condition list, and then click Delete.**

Note: Conditions may be exported for use with other alerts by clicking **Export Conditions** and saving as appropriate. Conditions from other alerts may be imported to the current alert by clicking **Import Conditions**.

Warning: Imported conditions automatically overwrite existing conditions.

11. If you are finished configuring your advanced alert, click OK.

Setting the Monitoring Period for an Advanced Alert

You can select the specific time periods and days that your advanced alert will monitor your network objects with the following procedure.

To set the monitoring time period and days for an advanced alert:

1. Click **Start > All Programs > SolarWinds Orion > Alerting, Reporting, and Mapping > Advanced Alert Manager**.
2. Click **View > Configure Alerts**.

3. Click **New** or select an alert from the list, and then click **Copy** or **Edit**.
4. Click **Time of Day**.
5. Enter the time period over which you want to monitor your network.
Note: Alerts will only trigger if your trigger condition is met within the time period entered.
6. Select the days on which you want to monitor your network.
Note: Alerts will only trigger if your trigger condition is met on the days selected.
7. *If you are finished configuring your advanced alert*, click **OK**.

Setting a Trigger Action for an Advanced Alert

Select actions that will occur when your advanced alert is triggered with the following procedure.

To set a trigger action for an advanced alert:

1. Click **Start > SolarWinds Orion > Alerting, Reporting, and Mapping > Advanced Alert Manager**.
2. Click **View > Configure Alerts**.
2. Click **New** or select an alert from the list, and then click **Copy** or **Edit**.
3. Click **Trigger Actions**.
4. *If you are adding a new advanced alert action*, click **Add New Action**, and then select the actions you want to occur when the alert triggers.
5. *If you are editing an existing advanced alert action*, select the existing alert action, and then click **Edit Selected Action**.
6. Follow the instructions to configure each action.
Note: Depending on the type of action selected, different options will be displayed to configure the alert action.
7. *If you need to delete an action*, select the action and then click **Delete Selected Action**.
8. *If you are finished configuring your advanced alert*, click **OK**.

Setting a Reset Action for an Advanced Alert

Select actions that will occur when your advanced alert is reset with the following procedure.

To set a reset action for an advanced alert:

1. Click **Start > SolarWinds Orion > Alerting, Reporting, and Mapping > Advanced Alert Manager**.
2. Click **View > Configure Alerts**.
3. Click **New Alert**, **Copy Alert**, or **Edit Alert**, as appropriate.
4. Click **Reset Actions**.
5. *If you are adding a new advanced alert action*, click **Add New Action**, and then select the actions you want to occur when the alert triggers.
6. *If you are editing an existing advanced alert action*, select the existing alert action, and then click **Edit Selected Action**.
7. Follow the instructions to configure each action.

Note: Depending on the type of action selected, different options display configuring the alert action. For more information on the Time of Day tab, see “Setting the Monitoring Period for an Advanced Alert” on page 150. For more information on the Alert Escalation tab, see “Alert Escalation” on page 153.

8. *If you need to delete a selected action*, click **Delete Selected Action**.
9. *If you are finished configuring your advanced alert*, click **OK**.

Alert Escalation

When editing any trigger or reset action, use the Alert Escalation tab, if it is available, to define additional alert action options. The following options are available on the Alert Escalation tab:

- To disable the action when the alert has been acknowledged, check **Do not execute this Action if the Alert has been Acknowledged**.
- To execute the action repeatedly as long as the trigger condition exists, check **Execute this Action repeatedly while the Alert is Triggered** and then provide an appropriate action execution interval.
- To delay the execution of the alert action, check **Delay the execution of this Action** and then provide an appropriate interval that the alert engine should wait after the alert condition is met before the alert action is executed.

For more information about escalated alerts, see “Escalated Alert” on page 178.

Understanding Condition Groups

A condition group is a set of user-defined rules governing alert triggers and resets. By default, the condition group `Trigger Alert when all of the following apply` is added when new alert triggers or reset conditions are created. Four different logical descriptors are used to create conditions: `all`, `any`, `none`, and `not all`, and clicking the word `all` and enables you to select different values. The following sections describe these logical descriptors.

All Condition Group

`Trigger Alert when all of the following apply` means that every condition in the group must be true before the alert is triggered.

In the following example, there are three conditions within the condition group:

- Node Status is equal to Up
- Percent Loss is greater than or equal to 75
- CPU Load is greater than or equal to 85

This alert will not trigger unless the Node is Up, packet loss is greater than or equal to 75%, and CPU load is greater than or equal to 85%.

When setting the condition group to `all`, picture every condition as being separated by an `and` statement. So, in this example, the alert trigger would read:

```
Alert when: (Node Status = Up) and (Percent Loss >= 75) and (CPU Load >= 85)
```

Any Condition Group

Changing the condition group to Trigger Alert when *any* of the following apply changes the logic to *or* statements. In this example, changing the condition group to *any* would change the alert trigger to:

```
Alert when: (Node Status = Up) or (Percent Loss >= 75) or (CPU Load >= 85)
```

In this situation, if **any** of the three conditions become true, the alert will trigger.

None Condition Group

Changing the condition group to Trigger Alert when *none* of the following apply means that all conditions in the group must be false before the alert is triggered.

In this example the alert trigger would read:

```
Alert when: (Node Status = Down) and (Percent Loss <= 75) and (CPU Load <= 85)
```

Each condition is separated by an *and* statement just like the *all* condition group; however, the conditions have been inverted (*Node Status = Down* instead of *Node Status = Up*).

Not All Condition Group

Changing the condition group to Trigger Alert when *not all* of the following apply means that any condition in the group must be false before the alert is triggered. So, in this example the alert trigger would read:

```
Alert when: (Node Status = Down) or (Percent Loss <= 75) or (CPU Load <= 85)
```

Each condition is separated by an *or* statement just like the *any* condition group; however, the conditions have been inverted (*Node Status = Down* instead of *Node Status = Up*).

Using the Advanced Alert Manager

The Advanced Alert Manager is an interface used to view network events and alerts. You can also use Advanced Alert Manager to create and manage advanced alerts. The following procedures introduce the main features of the Advanced Alert Manager showing how to configure and view advanced alerts.

Current Events Window

The Current Events window of the Advanced Alert Manager shows the most recent network events with their descriptions and other information from the events log.

To use the Current Events window to view network events:

1. Click **Start > All Programs > SolarWinds Orion > Alerting, Reporting, and Mapping > Advanced Alert Manager**.
2. Click **View > Current Events**.
3. Select one of the following **Group By** criteria for grouping events: **Event Type**, **Object Type**, **Network Node**, **Acknowledged**, or **No Grouping**.
4. ***If you want to change the viewable category columns in the Current Events window***, click **Include**, and then complete the following procedure:
 - a. Click the Event View Columns tab, and then select column IDs from the **All Columns** field.
 - b. Click the right arrow to move your column IDs into the **Selected Columns** field.
 - c. ***If there are any column IDs in the Selected Columns field that you do not want to view***, select them, and then click the left arrow to move your selected column IDs to the **All Columns** field.
 - d. Click the up or down arrows to change the order of your selected columns accordingly.
 - e. Position the slider to set the Event View refresh rate.
 - f. Type the number of events that you want to be able to review in the **Display a maximum of xxxx events in the Event View** field.
 - g. ***If you are finished configuring your Current Events View***, click **OK**.
5. Click **Refresh** to update the Current Events window with the latest events and column IDs.
6. ***If you want to acknowledge a network event***, click **X** next to the event.

Active Alerts Window

The Active Alerts window of the Advanced Alert Manager shows network alerts with their descriptions and other information from the alerts log.

To use the Active Alerts window to view active network alerts:

1. Click **Start > All Programs > SolarWinds Orion > Alerting, Reporting, and Mapping > Advanced Alert Manager**.
2. Click **View > Active Alerts**.
3. Select one of the **Group By** criteria for grouping alerts: **Alert Name, Object Type, Object Name, Alert State, Acknowledged, Acknowledged By, or No Grouping**.
4. Click **Include**, and then check the types of alerts that you want to view: **Acknowledged, Trigger Pending, Triggered, or Reset Pending**.
5. **If you want to change the viewable category columns in the Current Events window**, click **Include > Select Alert Columns**, and then complete the following procedure:
 - a. Select column IDs from the **All Columns** field.
 - b. Click the right arrow to move your column IDs into the **Selected Columns** field.
 - c. **If there are any column IDs in the Selected Columns field that you do not want to view**, select them, and then click the left arrow to move your selected column IDs to the **All Columns** field.
 - d. Click the up or down arrows to change the order of your selected columns accordingly.
 - e. Position the slider to set the Alert View refresh rate.
 - f. **If you are finished configuring your Active Alerts View**, click **OK**.
6. Click **Refresh** to update the Active Alerts window with the latest alerts and column IDs.
7. Click **Configure Alerts** to change the settings for individual alerts. For more information, see “Monitoring Network Events” on page 129.
8. **If you want to acknowledge an active alert**, check the alert in the **Acknowledged** column.

Note: As soon as the alert is acknowledged, the user information and date/time is recorded in the database.

Alert Viewer Settings

Alert views in the Orion Advanced Alert Manager are configured in the Alert Viewer Settings window, as presented in the following procedure.

To configure alert views in the Advanced Alert Manager:

1. Click **Start > All Programs > SolarWinds Orion > Alerting, Reporting, and Mapping > Advanced Alert Manager**.

2. Click **File > Settings**.

Note: The Configure Alerts tab of the Alert Viewer Settings window displays all available network alerts, and from this window you can create, copy, edit, and delete alerts. For more information, see “Creating and Configuring Advanced Alerts” on page 145.

3. Click **Alert View Columns**.

4. Select the information titles that you want to see about your alerts from the **All Columns** list, and then click the right arrow to transfer them to the **Selected Columns** list.

Note: The Selected Columns list provides a list of all the information that the Alert Viewer will show for each active alert.

5. ***If you want to remove titles from the Selected Columns list***, select titles that you want to remove from the active view in the **Selected Columns** list, and then click the left arrow.
6. ***If you want to rearrange the order in which the different pieces of alert information are presented in the Alert Viewer***, select titles from the **Selected Columns** list and use the up and down arrows to arrange the titles accordingly.

7. Position the slider at the bottom of the tab to set the Alert View refresh rate.

8. Click **Event View Columns**.

9. Select the information titles that you want to see about events from the **All Columns** list, and then click the right arrow to transfer them to the **Selected Columns** list.

Note: The Selected Columns list provides a list of all the information that the Alert Viewer will show for each recorded event.

10. ***If you want to remove titles from the Selected Columns list***, select titles that you want to remove from the active view in the **Selected Columns** list, and then click the left arrow.

11. **If you want to rearrange the order in which the different pieces of event information are presented in the Alert Viewer**, select titles from the **Selected Columns** list and use the up and down arrows to arrange the titles accordingly.
12. Position the slider at the bottom of the tab to set the Event View refresh rate.
13. Enter the number of events that you want to see in the Event View.

Adding Alert Actions

Orion Network Performance Monitor provides a variety of actions to signal an alert condition on your network. These alert actions are available for both basic and advanced alerts, and the following procedure assigns actions to the alert conditions that you have defined for your network.

To add an alert action:

1. Click **Start > All Programs > SolarWinds Orion > System Manager**.
2. Click **Alerts > Active Alerts**.
3. Click either **Configure Basic Alerts** or **Configure Advanced Alerts**, as appropriate.
4. Check the alert to which you want to add the action, and then click **Edit Alert**.
5. Click **Actions**, and then select the action you want to edit.
6. Click **Add Alert Action**, and then click the action to add to your chosen alert.

Available Alert Actions

The following sections detail the configuration of each available action type.

Note: If the configuration options differ for basic and advanced alerts, the following sections provide configuration procedures for both types of alert actions.

Send an E-mail / Page

The Edit E-mail/Page Action window includes several tabs for configuring e-mail/page actions.

Notes:

- Available options are slightly different for basic and advanced alerts, as shown in the following sections.
- Emails are sent in plain text.

Send an E-mail / Page for a Basic Alert

The following procedure configures an e-mail/page action for a basic alert.

To configure an email/page action for a basic alert:

1. Click **E-mail/Pager Addresses**, and then complete the **To**, **CC**, **BCC**, **Name**, and **Reply Address** fields.

Notes:

- You must provide at least one email address in the **To** field. When entering multiple addresses in a field, you may only separate addresses with a comma.
- Some pager systems require a valid reply address to complete the page.

2. Click **SMTP Server**, and then type the **Hostname or IP Address of your SMTP Server** and the designated **SMTP Port Number**.

Note: The SMTP server hostname or IP address field is required. You cannot send an email/page alert without identifying the SMTP server.

3. **If your SMTP server requires authentication**, check **This SMTP Server requires Authentication**.

4. Click the Trigger Message tab, and then type the **Subject** and **Message** of your alert trigger email/page.

Notes:

- Messaging is suppressed if both **Subject** and **Message** fields are empty.
- A default subject and message are provided that use variables. For more information on the use of variables in basic alerts and actions, see “Basic Alert Engine Variables” on page 309. For example messages that use variables, see “Example Messages Using Variables” on page 316.

5. **If you want to provide a message when the alert resets**, click the Reset Message tab, and then enter the **Subject** and **Message** of your alert reset email/page.

Notes:

- Messaging is suppressed if both **Subject** and **Message** fields are empty.
- A default subject and message are provided that use variables. For more information on the use of variables in basic alerts and actions, see “Basic Alert Engine Variables” on page 309. For example messages that use variables, see “Example Messages Using Variables” on page 316.

6. **If you are finished configuring your email/page alert action**, click **OK**.

Send an E-mail / Page for an Advanced Alert

The following procedure configures an e-mail/page action for an advanced alert.

To configure an email/page action for an advanced alert:

1. Click **E-mail/Pager Addresses**.
2. Complete the **To**, **CC**, **BCC**, **Name**, and **Reply Address** fields.

Notes:

- You must provide at least one email address in the **To** field. When entering multiple addresses in a field, you may only separate addresses with a comma.
- Some pager systems require a valid reply address to complete the page.

3. Click **Message**.
4. Type the **Subject** and **Message** of your alert trigger email/page.
Note: Messaging is disabled if both **Subject** and **Message** fields are empty.
5. **If you want to insert a variable into the Subject or Message field**, click the location of the new variable, and then complete the following procedure:

- a. Click **Insert Variable**.
- b. Select a **Variable Category**.
- c. Select the variable you want to add.
- d. **If you want to change the parser**, check **Change Parser**, and then select the parser you want to use.
- e. **If you want to define the SQL variable to copy to the clipboard**, check **Define SQL Variable**, and then click **Insert Variable From Above List**.
- f. Click **Build Selected Variable**.

Note: For more information on the use of variables, see “Alert Variables and Examples” on page 309. For more information about messages that use variables, see “Example Messages Using Variables” on page 316.

6. Click **SMTP Server**.
7. Type the **Hostname or IP Address of your SMTP Server** and the designated **SMTP Port Number**.
Note: The SMTP server hostname or IP address field is required. You cannot send an email/page alert without identifying the SMTP server.
8. **If your SMTP server requires authentication**, check **This SMTP Server requires Authentication**.

9. Click **Time of Day**.
10. Enter the time period over which you want to activate your alert action.
11. Select the days on which you want to activate your alert action.
12. **If you want to enable alert escalation**, click the Alert Escalation tab, and then check any of the following options, as appropriate for your alert:
 - To disable the action when the alert has been acknowledged, check **Do not execute this Action if the Alert has been Acknowledged**.
 - To execute the action repeatedly as long as the trigger condition exists, check **Execute this Action repeatedly while the Alert is Triggered** and then provide an appropriate action execution interval.
 - To delay alert action execution, check **Delay the execution of this Action**, and then provide an appropriate interval the alert engine should wait after the alert condition is met before the alert action is executed.
13. **If you are finished configuring your email/page alert action**, click **OK**.

Playing a Sound

Orion NPM can be configured to play a sound upon alert trigger or reset.

Note: Available options are slightly different for basic and advanced alerts, as shown in the following sections.

Play a Sound for a Basic Alert

The following procedure configures a sound to play for a basic alert.

To configure a play sound action for a basic alert:

1. Specify a sound file for the alert trigger by doing either of the following in the **Sound file to play when Alert is triggered** field:
 - Type the complete directory path and file name
 - Click **Browse (...)** to navigate your folder structure and select a file
2. Specify a sound file for the alert reset by doing either of the following in the **Sound file to play when Alert is reset** field:
 - Type the complete directory path and file name
 - Click **Browse (...)** to navigate your folder structure and select a file.
3. Click the musical note to the right of either text field to test the sound file you have specified.
4. **If you are finished configuring your play sound alert action**, click **OK**.

Play a Sound for an Advanced Alert

The following procedure configures a sound to play for an advanced alert.

To configure a play sound action for an advanced alert:

1. Click **Play Sound**.
2. Specify a sound file for the alert trigger by doing either of the following in the **Sound file to play** field:
 - Type the complete directory path and file name.
 - Click **Browse (...)** to navigate your folder structure and select a file.
3. Click the musical note button to the right of either text field to test the sound file you have specified.
4. Click **Time of Day**.
5. Enter the time period over which you want to activate your alert action, and then select the days on which you want to activate your alert action.
6. ***If you want to enable alert escalation***, click **Alert Escalation**, and then check any of the following options, as appropriate for your alert:
 - To disable the action when the alert has been acknowledged, check **Do not execute this Action if the Alert has been Acknowledged**.
 - To execute the action repeatedly as long as the trigger condition exists, check **Execute this Action repeatedly while the Alert is Triggered** and then provide an appropriate action execution interval.
 - To delay alert action execution, check **Delay the execution of this Action**, and then provide an appropriate interval the alert engine should wait after the alert condition is met before the alert action is executed.
7. ***If you are finished configuring your play a sound alert action***, click **OK**.

Logging Alerts to a File

Orion NPM can be configured to log alerts to a designated file. The following procedures will configure an alert log file.

Note: Available options are slightly different for basic and advanced alerts, as shown in the following sections.

Logging a Basic Alert to a File

The following procedure logs a basic alert to a designated file

To configure an alert log file for a basic alert:

1. Specify an alert log file by doing either of the following in the **Alert Log File** field:
 - Type the complete path and name of the target file
 - Click **Browse (...)** to navigate your folder structure and select the target file

Note: If the file specified does not exist, it will be created with the first alert occurrence.

2. *If you want to change the default message to log when the alert is triggered*, type your message in the **Message to log when the Alert is triggered** field.

Note: A default message is provided that uses variables. For more information on the use of variables in basic alerts and actions, see “Basic Alert Engine Variables” on page 309. For example messages that use variables, see “Example Messages Using Variables” on page 316.

3. *If you want to change the default message to log when the alert is reset*, type your message in the **Message to log when the Alert is reset** field.

Note: A default message is provided that uses variables. For more information on the use of variables in basic alerts and actions, see “Basic Alert Engine Variables” on page 309. For example messages that use variables, see “Example Messages Using Variables” on page 316.

4. *If you are finished configuring your alert log file*, click **OK**.

Logging an Advanced Alert to a File

The following procedure logs an advanced alert to a designated file

To configure an alert log file for an advanced alert:

1. Click **Event Log**, and then specify an alert log file by doing either of the following in the **Alert Log Filename** field:
 - Type the complete path and name of the target file
 - Click **Browse (...)** to navigate your folder structure and select the target file

Note: If the file specified does not exist, it will be created with the first alert occurrence.

2. Type the message you want to log to your alert log file in the **Message** field.
3. **If you want to insert a variable into the Message field**, complete the following procedure:
 - a. Click **Insert Variable**.
 - b. Select a **Variable Category**.
 - c. Select the variable you want to add.
 - d. **If you want to change the parser**, check **Change Parser**, and then select the parser you want to use.
 - e. **If you want to define the SQL variable to copy to the clipboard**, check **Define SQL Variable**, and then click **Insert Variable From Above List**.
 - f. Click **Build Selected Variable**.

Note: For more information on the use of variables, see “Alert Variables and Examples” on page 309.
4. Click **Time of Day**.
5. Enter the time period over which you want to activate your alert action.
6. Select the days on which you want to activate your alert action.
7. **If you want to enable alert escalation**, click the Alert Escalation tab, and then check any of the following options, as appropriate for your alert:
 - To disable the action when the alert has been acknowledged, check **Do not execute this Action if the Alert has been Acknowledged**.
 - To execute the action repeatedly as long as the trigger condition exists, check **Execute this Action repeatedly while the Alert is Triggered** and then provide an appropriate action execution interval.
 - To delay alert action execution, check **Delay the execution of this Action**, and then provide an appropriate interval the alert engine should wait after the alert condition is met before the alert action is executed.
8. **If you are finished configuring your alert log file**, click **OK**.

Logging an Alert to the Windows Event Log

You may specify that an alert be logged to the Windows Event Log on either the Orion Network Performance Monitor server or a remote server. The following procedure will configure an alert that writes to the Windows Event Log on a designated server.

Note: Available options are slightly different for basic and advanced alerts, as shown in the following sections.

Logging a Basic Alert to the Windows Event Log

The following procedure logs a basic alert to the Windows Event Log on a designated server.

To configure basic alert logging to the Windows Event Log:

1. Click **Target Machine**.
2. *If you want your alert to write to the Windows Event Log on your Orion NPM server*, select **Log Message in Event Log on NetPerfMon Server**.
3. *If you want your alert to write to the Windows Event Log on a remote server*, select **Log Message in Event Log on Remote Server**, and then provide the **Remote Server Name or IP Address**.
4. Click the **Trigger Message** tab, and then enter the message you want the triggered alert to log to the Windows Event Log on the designated server.
Note: You can use variables in the triggered alert log message. For more information on the use of variables in basic alerts and actions, see “Basic Alert Engine Variables” on page 309. For example messages that use variables, see “Example Messages Using Variables” on page 316.
5. Click the **Reset Message** tab, and then enter the message you want the reset alert to log to the Windows Event Log on the designated server.
Note: You can use variables in the reset alert log message. For more information on the use of variables in basic alerts and actions, see “Basic Alert Engine Variables” on page 309. For example messages that use variables, see “Example Messages Using Variables” on page 316.
6. *When you finish configuring your Windows Event Log action*, click **OK**.

Logging an Advanced Alert to the Windows Event Log

The following procedure logs an advanced alert to the Windows Event Log on a designated server.

To configure advanced alert logging to the Windows Event Log:

1. Click **Event Log**.
2. *If you want your alert to write to the Windows Event Log on your Orion NPM server*, select **Use Event Log Message on Network Performance Monitor Server**.
3. *If you want your alert to write to the Windows Event Log on a remote server*, select **Use Event Log Message on a Remote Server**, and then provide the **Remote Server Name or IP Address**.
4. Type the message you want to log to the Windows Event Log in the **Message to send to Windows Event Log** field.

5. **If you want to insert a variable into the Message field**, complete the following procedure:
 - a. Click **Insert Variable**.
 - b. Select a **Variable Category**.
 - c. Select the variable you want to add.
 - d. **If you want to change the parser**, check **Change Parser**, and then select the parser you want to use.
 - e. **If you want to define the SQL variable to copy to the clipboard**, check **Define SQL Variable**, and then click **Insert Variable From Above List**.
 - f. Click **Build Selected Variable**.

Note: For more information on the use of variables, see “Alert Variables and Examples” on page 309.
6. Click **Time of Day**.
7. Enter the time period and select the days over which you want to activate your alert action.
8. **If you want to enable alert escalation**, click **Alert Escalation**, and then check any of the following options, as appropriate for your alert:
 - To disable the action when the alert has been acknowledged, check **Do not execute this Action if the Alert has been Acknowledged**.
 - To execute the action repeatedly as long as the trigger condition exists, check **Execute this Action repeatedly while the Alert is Triggered** and then provide an appropriate action execution interval.
 - To delay alert action execution, check **Delay the execution of this Action**, and then provide an appropriate interval the alert engine should wait after the alert condition is met before the alert action is executed.
9. **If you are finished configuring your alert log file**, click **OK**.

Sending a Syslog Message

Orion NPM can log received alerts to the Syslog of a designated machine. The following procedures configure Orion NPM to send Syslog a message.

Note: Available options are slightly different for basic and advanced alerts, as shown in the following sections.

Configuring a Basic Alert to Send a Syslog Message

The following procedure configures a basic alert to send a message to a designated Syslog server.

To configure a basic alert to send a Syslog message:

1. Click **Target Machine**.
2. Type the **Target Hostname or IP Address** of the Syslog server to which you want to send messages on alert trigger and reset.
3. Click **Trigger Message**.
4. Select the **Severity** of your alert trigger Syslog message.

Note: For more information, see “Syslog Severities” on page 223.

5. ***If you want to change the default message that is sent to Syslog when an alert is triggered,*** enter your message in the **Syslog** field.

Note: A default message is provided that uses variables. For more information on the use of variables in basic alerts and actions, see “Basic Alert Engine Variables” on page 309. For example messages that use variables, see “Example Messages Using Variables” on page 316.

6. Click **Reset Message**.
7. Select the **Severity** of your alert reset Syslog message.
8. ***If you want to change the default message that is sent to Syslog when an alert is reset,*** enter your message in the **Syslog** field.

Note: A default message is provided that uses variables. For more information on the use of variables in basic alerts and actions, see “Basic Alert Engine Variables” on page 309. For example messages that use variables, see “Example Messages Using Variables” on page 316.

Configuring an Advanced Alert to Send a Syslog Message

The following procedure configures an advanced alert to send a message to a designated Syslog server.

To configure an advanced alert to send a Syslog message:

1. Click **Syslog Message**.
2. Type the **Hostname or IP Address of the Syslog Server** to which you want to send Syslog messages.
3. Select the **Severity** of your alert Syslog message.

Note: For more information, see “Syslog Severities” on page 223.

4. Select **Facility** of your alert Syslog message.

Note: For more information, see “Syslog Facilities” on page 222.

5. Type the **Syslog Message** you want to send.
6. **If you want to insert a variable into the Message field**, complete the following procedure:

- a. Click **Insert Variable**.
- b. Select a **Variable Category**.
- c. Select the variable you want to add.
- d. **If you want to change the parser**, check **Change Parser**, and then select the parser you want to use.
- e. **If you want to define the SQL variable to copy to the clipboard**, check **Define SQL Variable**, and then click **Insert Variable From Above List**.
- f. Click **Build Selected Variable**.

Note: For more information on the use of variables, see “Alert Variables and Examples” on page 309.

7. Click **Time of Day**.
8. Enter the time period over which you want to activate your alert action.
9. Select the days on which you want to activate your alert action.
10. **If you want to enable alert escalation**, click **Alert Escalation**, and then check any of the following options, as appropriate for your alert:
 - To disable the action when the alert has been acknowledged, check **Do not execute this Action if the Alert has been Acknowledged**.
 - To execute the action repeatedly as long as the trigger condition exists, check **Execute this Action repeatedly while the Alert is Triggered** and then provide an appropriate action execution interval.
 - To delay alert action execution, check **Delay the execution of this Action**, and then provide an appropriate interval the alert engine should wait after the alert condition is met before the alert action is executed.
11. **If you are finished with the configuration of your send Syslog message action**, click **OK**.

Executing an External Program

There are several circumstances where you may want to execute a program when a specific network event occurs. Use the Edit Execute Program Action window to specify the complete path and name of the executable that should be started when the specified alert is triggered or reset. The following procedure configures Orion NPM to execute an external program upon an alert trigger.

To configure alerts to execute an external program:

1. ***If you are configuring a basic alert to execute an external program,*** complete the following steps:
 - a. Specify a program to execute when the alert is triggered either by typing the complete path and name of the target file into the **Program to execute when Alert is Triggered** field or by clicking **Browse (...)** to browse your folder structure and select the target file.
 - b. Specify a program to execute when the alert is reset either by typing the complete path and name of the target file into the **Program to execute when Alert is Reset** field or by clicking **Browse (...)** to browse your folder structure and select the target file.
2. ***If you are configuring an advanced alert to execute an external program,*** complete the following steps:
 - a. Click **Execute Program**.
 - b. Specify a program to execute, either by typing the complete path and name of the target file into the **Program to execute** field or by clicking **Browse (...)**, to browse your folder structure and select the target file.
 - c. Click **Time of Day**, and then enter the time period when you want to execute the external program.
 - d. Select the days on which you want to execute the external program.
 - e. Click **Alert Escalation**, and then check any of the following options, as appropriate for your alert:
 - To disable the action when the alert has been acknowledged, check **Do not execute this Action if the Alert has been Acknowledged**.
 - To execute the action repeatedly, while the trigger condition exists, check **Execute this Action repeatedly while the Alert is Triggered**, and then provide an action execution interval.
 - To delay alert action execution, check **Delay the execution of this Action**, and then provide the interval the alert engine should wait.
3. ***If you are finished configuring your external program execution action,*** click **OK**.

Executing a Visual Basic Script

In some situations you may want to execute a Visual Basic (VB) script when a network event occurs. The Edit Execute VB Script Action window is used to specify the name and complete path of the file that shall be executed when the specified alert is triggered or reset.

To configure alerts to execute a Visual Basic (VB) script:

1. *If you are configuring a basic alert to execute a VB script*, complete the following steps:
 - a. Select an available **VB Script Interpreter**.
 - b. Specify a VB script to execute when the alert is triggered either by typing the complete path and name of the script into the **VB Script to execute when Alert is triggered** field or by clicking **Browse (...)** to browse your folder structure and select the script.
 - c. Specify a VB script to execute when the alert is reset either by typing the complete path and name of the target file into the **Program to execute when Alert is reset** field or by clicking **Browse (...)** to browse your folder structure and select the script.
2. *If you are configuring an advanced alert to execute a Visual Basic script*, complete the following steps:
 - a. Click **VB Script**, and then select an available **VB Script Interpreter**.
 - b. Specify a VB script to execute either by typing the complete path and name of the VB script into the **VB Script to execute** field or by clicking **Browse (...)** to browse your folder structure and select the script.
 - c. Click **Time of Day**, and then enter the time period and select the days on which you want to execute the selected VB script.
 - d. Click **Alert Escalation**, and then check any of the following options, as appropriate for your alert:
 - To disable the script when the alert has been acknowledged, check **Do not execute this Action if the Alert has been Acknowledged**.
 - To execute the script repeatedly as long as the trigger condition exists, check **Execute this Action repeatedly while the Alert is Triggered** and then provide an appropriate action execution interval.
 - To delay script execution, check **Delay the execution of this Action**, and then provide an appropriate interval the alert engine should wait after the alert condition is met before the script executes.
3. *If you are finished configuring your VB script execution action*, click **OK**.

E-mailing a Web Page

The Edit E-mail Web Page Action window includes several tabs for configuration. The following procedure will configure an email message to send a web page to a specified address upon alert.

Notes:

- Available options are slightly different for basic and advanced alerts, as shown in the following sections.
- Emails are sent in plain text.

E-mailing a Web Page for a Basic Alert

The following procedure configures a web page e-mail action for a basic alert.

To configure a web page e-mail action for a basic alert:

1. Click **E-mail a Web Page**, and then click **OK**.
2. Complete the **To**, **CC**, **BCC**, **Name**, and **Reply Address** fields.

Notes:

- You must provide at least one email address in the **To** field. When entering multiple addresses in a field, you may only separate addresses with a comma.
- Some pager systems require a valid reply address to complete the page.

3. Click **SMTP Server**.
4. Type the **Hostname or IP Address of your SMTP Server** and the designated **SMTP Port Number**.

Note: The SMTP server hostname or IP address field is required. You cannot email a web page without identifying the SMTP server.

5. **If your SMTP server requires authentication**, check **This SMTP Server requires Authentication**.
6. Click **Trigger URL**, and then provide the **Subject** and **Web Page URL** of your alert trigger web page email.

Notes:

- Messaging is disabled if **Subject** and **Web Page URL** fields are empty.
- A default subject is provided that uses variables. For more information on the use of variables in basic alerts and actions, see “Basic Alert Engine Variables” on page 309. For example messages that use variables, see “Example Messages Using Variables” on page 316.

7. *If you want to preview the URL you have provided*, click **Preview URL**.
8. *If the web server of the URL you want to email on alert trigger requires user access authentication*, provide both the **Web Server UserID** and the **Web Server Password** in the Optional Web Server Authentication area.
9. *If you want to provide a URL on alert reset*, click **Reset URL**, and then type the **Subject** and **Web Page URL** of your alert reset web page email.

Notes:

- Messaging is suppressed if both **Subject** and **Message** fields are empty.
- A default subject and message are provided that use variables. For more information about variables in basic alerts, see “Basic Alert Engine Variables” on page 309. For example messages that use variables, see “Example Messages Using Variables” on page 316.

10. *If you want to preview the URL you have provided*, click **Preview URL**.
11. *If the web server of the URL you want to email on alert reset requires user access authentication*, provide both the **Web Server UserID** and the **Web Server Password** in the Optional Web Server Authentication area.
12. *If you are finished configuring your email URL alert action*, click **OK**.

E-mailing a Web Page for an Advanced Alert

The following procedure configures an e-mail URL action for an advanced alert.

To configure an email web page action for an advanced alert:

1. Click **E-mail a Web Page**, and then then click **OK**.
2. Complete the **To**, **CC**, **BCC**, **Name**, and **Reply Address** fields.
Note: You must provide at least one address in the **To** field. When entering multiple addresses, you may only separate addresses with a comma. Some pager systems require a valid reply address to complete the page.
3. Click **SMTP Server**, and then type the **Hostname or IP Address of your SMTP Server** and the designated **SMTP Port Number**.
Note: The SMTP server hostname or IP address field is required. You cannot email a web page without identifying the SMTP server.
4. Click **URL**, and then type the **Subject** of your alert email.
Note: Messaging is disabled if both **Subject** and **URL** fields are empty.

5. **If you want to insert a variable into the Subject field**, click the location of the new variable, and then complete the following procedure:
 - a. Click **Insert Variable**, select a **Variable Category**, and then select the variable to add.
 - b. **If you want to change the parser**, check **Change Parser**, and then select the parser you want to use.
 - c. **If you want to define the SQL variable to copy to the clipboard**, check **Define SQL Variable**, and then click **Insert Variable From Above List**.
 - d. Click **Build Selected Variable**.

Note: For more information on the use of variables, see “Alert Variables and Examples” on page 309. For more information about messages that use variables, see “Example Messages Using Variables” on page 316.
6. Provide the **URL** of your alert email.

Note: Messaging is disabled if both **Subject** and **URL** fields are empty.
7. **If the web server of the URL you want to email requires user access authentication**, provide both the **Web Server UserID** and the **Web Server Password** in the Optional Web Server Authentication area.
8. Click **Time of Day**, and then enter the time period and select the days when you want to activate your alert action.
9. **If you want to enable alert escalation**, click **Alert Escalation**, and then check any of the following options, as appropriate for your alert:
 - To disable the action when the alert has been acknowledged, check **Do not execute this Action if the Alert has been Acknowledged**.
 - To execute the action repeatedly, as long as the trigger condition exists, check **Execute this Action repeatedly while the Alert is Triggered** and then provide an appropriate action execution interval.
 - To delay alert action execution, check **Delay the execution of this Action**, and then provide an appropriate interval for the alert engine to wait after the alert condition is met before executing the alert action.
10. **If you are finished configuring your URL email alert action**, click **OK**.

Changing a Custom Property

You may specify that a basic alert changes a custom property value when the basic alert is either triggered or reset. This is useful when you have limited the users of an Orion Web Console view based on a property value, thus showing the users a moving depiction of the devices they need to monitor. You may also

populate the property with a custom URL for each issue needing monitoring. For more information, see “Setting Account Limitations” on page 93 and “Creating Custom Properties” on page 251.

The following procedure configures a change in a custom property upon the trigger or reset of a basic alert.

To change a custom property when a basic alert triggers or resets:

1. Enter the custom property name in the **Property** field.
Note: You must enter the name of the property exactly as it appears in the table header of the **Edit** view within the Custom Property Editor application. For more information, see “Creating Custom Properties” on page 251.
2. *If you want to change the above property upon an alert trigger*, enter the new value into the **Value to set when Alert is Triggered** field.
3. *If you want to change the above property upon an alert reset*, enter the new value into the **Value to set when Alert is Reset** field.
4. *If you are finished configuring your custom property change action*, click **OK**.

Using Text to Speech Output

You may specify a phrase that will be spoken upon alert trigger and a separate phrase for the alert reset. Orion NPM uses Microsoft Speech Synthesis Engine version 5.0, as included with Windows 2003 and XP Professional. If you have Orion NPM maintenance, you may also install and use other text-to-speech engines by visiting the SolarWinds website. The following procedures configure text-to-speech output for an alert trigger or reset.

Note: Available options are slightly different for basic and advanced alerts, as shown in the following sections.

Text-to-Speech Output Action for a Basic Alert

The following procedure configures a text-to-speech alert action.

To configure text-to-speech output for a basic alert trigger or reset:

1. Click **General**, and then select an available speech engine.
2. Position the **Speed**, **Pitch**, and **Volume** sliders as appropriate.
3. Click **Trigger Phrase**.

Note: A default triggered alert phrase is provided that uses variables. You may change this text if you wish. For more information on the use of variables, see “Alert Variables and Examples” on page 309.

4. **If you want to change the phrase that is spoken upon an alert trigger**, enter the new phrase into the **Phrase to speak when Alert is Triggered** field.
5. **If you want to test your text-to-speech message**, click **Speak**.
Note: If it is available with your speech engine, click **Pronunciation Dictionary** to adjust word pronunciation as you prefer.
6. Click **Reset Phrase**.
7. **If you want a phrase to be spoken upon an alert reset**, enter the new phrase into the **Phrase to speak when Alert is Reset** field.
8. **If you want to test your text-to-speech message**, click **Speak**.
Note: If it is available with your speech engine, click **Pronunciation Dictionary** to adjust word pronunciation as you prefer.
9. **If you are finished configuring your text-to-speech action**, click **OK**.

Sending a Windows Net Message

Alerts can be configured to display a pop-up Windows Net Message either on a specific computer or on all computers in a selected domain or workgroup. The following steps configure Windows Net messaging for triggered or reset alerts.

Note: Windows Server 2008 does not support Windows Net Messaging, so the Send a Windows Net message alert action is not available to Orion NPM installations on Windows Server 2008.

To configure Orion NPM to send a Windows Net message upon alert:

1. Click **Target Machine or IP Address**.
2. Enter the **Computer Name or IP Address** of the machine where you want to send a Windows Net message upon an alert trigger or reset.
3. **If you want to send the message to all computers in the domain or workgroup of your target computer**, check **Send to all Computers in the Domain or Workgroup**.
4. **If you want to change the default Windows Net message that is sent when an alert is triggered**, click the **Trigger Message** tab, and then enter your message in the **Message to send when Alert is Triggered** text box.
Note: You may use variables in this message. For more information on the use of variables, see "Alert Variables and Examples" on page 309.

5. **If you want to send a Windows Net message when an alert is reset**, click the Reset Message tab, and then enter your message in the **Message to send when Alert is Reset** text box.

Note: You may use variables in this message. For more information on the use of variables, see “Alert Variables and Examples” on page 309.

6. **If you are finished with the configuration of your send Windows Net message action**, click **OK**.

Sending an SNMP Trap

The following steps configure an alert to send an SNMP trap on trigger or reset.

To configure Orion NPM to send an SNMP trap upon alert:

1. Click **Target Machines**.
2. Enter the hostname or IP address of the destination Orion NPM server for your SNMP traps into the **Add Trap Destination** field, and then click **Add**.

Note: Repeat this step for each additional destination machine.

3. **If there is a machine in the Send SNMP Traps to the following machines field that you no longer want as an SNMP trap destination**, select the machine from the list, and then click **Delete** to remove it.
4. Enter the **SNMP Community String** for your network in the designated field.
5. Click **Trap to Send on Trigger**.
6. Select the type of trap to send on alert trigger from the **Trap Template** list.

Note: Some trap templates may use an alert message, so a default message that uses variables is provided for the triggered alert message. You may change this text, if you want, but it is important that you understand the use of variables beforehand. For more information about using variables, see “Alert Variables and Examples” on page 309.

7. **If you want to change the default message sent with the SNMP trap when the selected alert is triggered**, enter the text of your new SNMP trap message in the **Some Trap templates may use an Alert Message** text box.
8. Click **Trap to Send on Reset**.
9. Select the type of trap to send on alert reset from the **Trap Template** list.
10. **If you want to send an SNMP trap when an alert is reset**, enter the text of your SNMP trap message in the **Some Trap templates may use an Alert Message** text box.
11. **If you are finished with the configuration of Orion NPM to send SNMP traps**, click **OK**.

Using GET or POST URL Functions

Orion NPM can be configured to communicate alerts using HTTP GET or POST functions. As an example, a URL may be used as an interface into a trouble ticket system, and, by correctly formatting the GET function, new trouble tickets may be created automatically. The following procedure configures Orion NPM to use GET or POST HTTP functions to communicate alert information.

To configure Orion NPM to use GET or POST URL functions with alerts:

1. Select either **Use HTTP GET** or **Use HTTP POST** to set the function that you want to use to communicate alert information.
2. Enter the URL that you want to GET or POST, as designated, upon an alert trigger in the **URL when Alert is Triggered** field.
3. Enter the URL that you want to GET or POST, as designated, upon an alert reset in the **URL when Alert is Reset** field.
4. *If you are finished with the configuration of Orion NPM to use HTTP GET or POST URL functions*, click **OK**.

Acknowledging Advanced Alerts in the Web Console

Orion NPM allows you to acknowledge both basic and advanced alerts using either the System Manager or the Orion Web Console. Acknowledging alerts eliminates lost time incurred when multiple users attempt to resolve the same issue or an issue has already been resolved. For information on acknowledging alerts in System Manager, see “Acknowledging Advanced Alerts in System Manager” on page 178.

To acknowledge advanced alerts using the Orion Web Console:

1. Log in to the Orion Web Console using an account that has been granted alert acknowledgement privileges.
Note: For more information about access privileges for Orion Web Console users, see “User Account Access Settings” on page 92.
2. Click **Alerts** on the Views toolbar.
3. *If you want to limit the list of alerts to only those dealing with a single device*, select the specific device from the **Network Object** list.
Note: This option is only available if alerts fire on multiple network devices.
4. *If you want to limit the list of alerts to only those dealing with a single type of device*, select the device type from the **Type of Device** list.
Note: This option is only available if Orion NPM is monitoring multiple types of network devices.

5. **If you want to limit the list of alerts to only those of a single type**, select the specific alert type from the **Alert Name** list.
Note: This option is only available when multiple types of Orion NPM alerts have been triggered.
6. Confirm the number of alerts displayed in the **Show Alerts** field.
7. **If you want acknowledged alerts to remain in the Alerts view, even after they have been acknowledged**, check **Show Acknowledged Alerts**.
8. Click **Refresh** to update the alerts list with your new settings.
9. Check **Acknowledged** next to the alerts you want to acknowledge.
10. Click **Acknowledge Alerts**.

Acknowledging Advanced Alerts in System Manager

Orion NPM allows you to acknowledge both basic and advanced alerts using either the System Manager or the Orion Web Console. Acknowledging alerts eliminates lost time incurred when multiple users attempt to resolve the same issue or an issue has already been resolved. For information on acknowledging alerts using the Orion Web Console, see “Acknowledging Advanced Alerts in the Web Console” on page 177. For more information about viewing alerts in System Manager, see “Viewing Alerts in System Manager” on page 262.

To acknowledge advanced alerts using the Orion System Manager:

1. Click **Start > All Programs > SolarWinds Orion > System Manager**.
2. Click **Alerts > Active Alerts**.
3. Click **Advanced Alerts**.
4. Check **Acknowledged** next to alerts you want to acknowledge.

Escalated Alerts

By creating an escalated alert, Orion NPM enables you to customize a series of alerts to trigger successive actions as an alert condition persists. The following sections provide both a scenario where an escalated alert may be useful and the steps required to create one using the Orion Advanced Alert Manager.

Escalated Alert Example

WidgetCo is a business with a small IT staff, consisting of two technicians and an IT manager. To ensure that issues are addressed appropriately, the IT manager has created multiple escalated alerts for a range of potential network events, including device failures and excessive disk space or bandwidth usage. Typically, the escalated alerts configured by the WidgetCo IT manager proceed as follows:

1. Immediately, as soon as Orion NPM recognizes an alert condition, Orion NPM generates both an email and a page that are sent to one of the two technicians. An entry is also recorded in the Orion events log.
2. If the alert is not acknowledged in the Orion Web Console within 20 minutes, a second alert is fired, generating another email and another page, both sent to both technicians. An entry is also recorded in the Orion events log.
3. If the second alert is not acknowledged within 20 minutes, Orion NPM fires a third alert that sends both an email and a page to both technicians and to the IT manager. An entry is also recorded in the Orion events log.

Escalated alerts ensure that everyone on the WidgetCo IT staff is notified of any significant network alert conditions within 45 minutes without burdening the IT manager with excessive alert notifications. The following section provides a procedure to create a similar escalated alert scheme.

Creating a Series of Escalated Alerts

The following procedure creates a series of escalated alerts similar to the scheme described in the preceding example.

Note: Repeat these steps to create a separate alert for each notification level. The example provided in the previous section uses a three-level escalated alert. The following procedure should be completed three times, once for each alert, to replicate the escalated alert of the previous section.

To create an escalated alert:

1. Click **Start > All Programs > SolarWinds Orion > Alerting, Reporting, and Mapping > Advanced Alert Manager**.
2. Click **Configure Alerts**.
3. Click **New**, and then click **General**.
4. Type `Level X`, where X is the level corresponding to the currently configured alert, as the name of your escalated alert in the **Name of Alert** field.

Note: The example provided in the previous section uses a three-level escalated alert.

5. Type a description of your first level escalated alert in the description field, and then check **Enable this Alert**.
6. Type the Alert Evaluation Frequency and select Seconds, Minutes, or Hours from the list to set the checking interval for your alert.
7. Click **Trigger Condition**.

Note: For more information about configuring trigger conditions, see "Setting a Trigger Condition for an Advanced Alert" on page 146.

8. Select **Node** as the Type of Property to Monitor.
9. Confirm that the linked text in the alert definition field displays **all**.
Note: Click the linked text to select the number of conditions that you want to apply (**all**, **any**, **none**, **not all**). For more information about linked text conditions, see “Understanding Condition Groups” on page 153.
10. Click **Browse (...)**, and then click **Add a Simple Condition**.
11. Click the first asterisk (*), and then select **Network Nodes > Node Details > Node Name**.
12. Confirm that **is equal to** is the linked condition text in the trigger definition.
Note: Click the linked text to select the condition you want to apply (**equal**, **greater**, **less**, ...). For more information about linked text conditions, see “Understanding Condition Groups” on page 153.
13. Click the second asterisk (*), and then select your production web server from the list of monitored nodes.
14. Click **Add**, and then click **Simple Condition**.
15. Click the first asterisk (*) in the second condition, and then select **Network Nodes > Node Status > Node Status**.
16. Confirm that **is equal to** is the linked condition text in the second trigger definition.
Note: Click the linked text condition to select the condition you want to apply (**equal**, **greater**, **less**, ...). For more information about linked text conditions, see “Understanding Condition Groups” on page 153.
17. Click the second asterisk (*) in the second condition, and then select **Down**.
18. *If you want to apply any reset conditions to your escalated alert*, click **Reset Condition**, and then provide appropriate conditions. For more information, see “Setting a Reset Condition for an Advanced Alert” on page 148.
19. *If you want to apply any alert suppressions to your escalated alert*, click **Alert Suppression**, and then provide appropriate suppression conditions. For more information, see “Setting a Suppression for an Advanced Alert” on page 149.
20. *If you want to restrict when your escalated alert is valid*, click **Time of Day**, designate the Valid Time of Day for your escalated alert, and then select the Days of the Week on which your escalated alert is valid. For more information, see “Setting the Monitoring Period for an Advanced Alert” on page 150.
Note: By default, your escalated alert is always valid.

21. Click **Trigger Actions**, and then click **Add New Action**.
22. Select **Send an E-mail / Page**, and then click **OK**.
23. Click **E-mail/Pager Addresses**, and then complete the **To**, **CC**, **BCC**, **Name**, and **Reply Address** fields for your Level 1 contact.

Note: You must provide at least one email address in the **To** field. When entering multiple addresses in a field, you may only separate addresses with a comma.

24. Click **Message**, and then type the **Subject** and **Message** of your escalated alert email.

Notes:

- Messaging is disabled if both **Subject** and **Message** fields are empty.
- For more information about variables in email subjects and messages, see “Send an E-mail / Page for an Advanced Alert” on page 160.

25. Click **SMTP Server**, and then provide the **Hostname or IP Address of your SMTP Server** and the designated **SMTP Port Number**.

Note: The SMTP server hostname or IP address field is required. You cannot send an email/page alert without identifying the SMTP server.

26. *If your SMTP server requires authentication*, check **This SMTP Server requires Authentication**.
27. *If you want to restrict when your escalated alert is valid*, check **Execute this Action only between specific hours**, and then configure the appropriate settings.

Note: By default, your escalated alert is always valid. For more information, see “Setting the Monitoring Period for an Advanced Alert” on page 150.

28. Click **Alert Escalation**.
29. Check **Do not execute this Action if the Alert has been Acknowledged**.
30. *If you want to execute the action repeatedly as long as the trigger condition exists*, check **Execute this Action repeatedly while the Alert is Triggered**, and then provide an appropriate action execution interval.
31. *If you want to delay alert action execution*, check **Delay the execution of this Action**, and then provide an appropriate interval the alert engine should wait after the alert condition is met before the alert action is executed.

Note: Typically, if you are configuring the first level alert, you should leave this option unchecked. If you are configuring the second level alert, check this option and provide the desired delay between the first and second notifications. If you are configuring the third level alert, check this option and provide the desired delay between the first and third notifications.

32. Click **OK**.

33. *If you want your escalated alert to perform any actions upon reset*, click the Reset Action tab, and then configure appropriate actions. For more information, see “Setting a Reset Action for an Advanced Alert” on page 152.

34. *If you are finished configuring your escalated alert*, click **OK**.

Chapter 13

Creating Network Maps

Orion Network Atlas is a powerful tool for creating custom maps and network diagrams. The maps created in Orion Network Atlas enable users to view a graphical depiction of their network in the Orion Web Console. You can also use the maps to create network documentation, which can then be printed and exported as needed.

Map objects may include monitored Orion NPM nodes, interfaces, and volumes; Orion APM applications and components; nested maps; and network links. The numerous presentation options for your network maps include the following:

- A large set of predefined background colors, textures, and images is available for you to use in your maps. You can also provide your own custom background graphics.
- Real-time weather or natural disaster maps may be projected directly onto your network maps using linked web graphics as a background.
- The shape, size, color, and style of map links may be customized to illustrate the status or the relative bandwidth of associated objects.
- Map objects may be presented in a unique set of graphical styles to portray network status
- Maps may be nested to selectively reveal increasing levels of map detail, and the status of nested map child objects may be bubbled up to the parent map

Orion Network Atlas is also fully compatible with all network maps created with Orion Map Maker in earlier versions of Orion NPM. For more information about Orion Network Atlas, see the *SolarWinds Orion Network Atlas Administrator Guide* at www.solarwinds.com.

Chapter 14

Creating Reports

Over time, your Orion Network Performance Monitor database accumulates a great deal of information. SolarWinds has developed Report Writer to provide a quick and easy way for you to extract data from your database and present it in a useful form. Several standard reports that you can modify are included in the Report Writer distribution, and you can create new reports as necessary. Report Writer includes powerful tools to help you format your information and easily preview your reports before you display them. When you have finished editing your reports, you can print them with the click of a button, and most reports are also enabled for viewing through the Orion Network Performance Monitor Web Console, by default. For more information about adding reports to Orion Web Console views, see “Customizing Views” on page 46.

Note: Report Writer capabilities are enhanced when used in conjunction with the Custom Property Editor. Once added, properties are available for report sort and filter functionality. For more information, see “Creating Custom Properties” on page 251.

Viewing Reports

All reports, custom or predefined, are available for viewing in both the Orion Web Console and in Report Writer, as shown in the following procedures:

- Viewing Reports in the Orion Web Console
- Viewing Reports in the Orion NPM Report Writer

Note: By default, no report folder is configured for newly created users. If a new user is not seeing reports, you may need to select a **Report Folder** for the new user. For more information, see “Configuring an Account Report Folder” on page 96.

Viewing Reports in the Orion Web Console

The following procedure opens reports for viewing in the Orion Web Console.

To view reports in the Orion Web Console:

1. Click **Start > All Programs > SolarWinds Orion > Orion Web Console**.
2. Log in to the Orion Web Console.
3. Click **Home > Reports**.

4. Select a report group name to expand the report group.
5. Click the title of the report you want to view.

The selected report opens directly in the web console browser.

Viewing Reports in the Orion NPM Report Writer

The following procedure opens reports for viewing in the Orion NPM Report Writer.

To view reports with Orion NPM Report Writer:

1. Click **Start > All Programs > SolarWinds Orion > Alerting, Reporting, and Mapping > Report Writer**.
2. *If report groups are not already expanded in the left pane*, click + next to a report group name to expand the group, and then click the title of the report you want to view.
3. Click **Preview**.

Predefined Reports

The following sections describe the reports that are immediately available with your Orion NPM installation. These reports may be modified, as necessary, to suit your network performance reporting requirements.

Note: If the report you require is not listed in any of the following sections, you can use Orion Report Writer to create your own custom report. For more information about creating your own custom reports, see “Getting Started with Report Writer” on page 198.

Availability

The following network availability reports are provided by default with Orion NPM.

Availability – Last Month

Displays the IP address and average availability of all monitored nodes over the last month.

Availability – This Year

Displays the IP address and average availability of all monitored nodes over the last year.

Availability – Yesterday

Displays the IP address and average availability of all monitored nodes over the previous day.

Availability of Entire Network – Last Month

Displays the availability of all monitored nodes on the entire network over the last month.

Top 25 Percent Down – Last Month

Displays the top 25 nodes, by percent downtime, over the last month.

Current Interface Status

The following interface status reports are provided by default with Orion NPM.

Current Percent Utilization - Top 25 Interfaces

Displays the top 25 monitored interfaces by current percent utilization. Interfaces are listed with their parent node, average sum of transmit and receive percent utilization, and transmit and receive traffic rates.

Current Traffic - All Interfaces

Displays a detailed report of the current traffic load on all monitored Interfaces. All monitored nodes are listed with their respective interfaces. For each interface, this report displays transmit and receive traffic rates and transmit and receive percent utilization.

Current Traffic - Top 25 Interfaces

Displays a detailed report of the top 25 monitored interfaces, listed current traffic load. For each interface, this report displays respective parent nodes, transmit and receive traffic rates, and transmit and receive percent utilization.

Down Interfaces

Displays a list of all monitored interfaces that are currently down.

Current Node Status

The following node status reports are provided by default with Orion NPM.

Average Response Time

Displays both average and peak response times for all monitored nodes.

Current CPU Load

Displays current CPU load percentage for all monitored nodes with CPUs.

Current Response Time

Displays the IP address and current, average, and peak response times for all monitored nodes.

Current Status of each Node

Displays the IP address and a verbal statement of the current operational status of all monitored nodes.

Down Nodes

Displays all monitored nodes that are currently down.

Last Boot Time for each Node

Displays the machine type and the date and time of last boot for all nodes.

Current Volume Status

Orion NPM provides an **Available Space on each Volume** report by default. This report displays the volume size, available space on the volume, and a percentage measure of the available space on the volume for all monitored volumes. Volumes are listed beneath their respective parent nodes.

Daily Node Availability

The following node availability reports are provided by default with Orion NPM.

Availability - Last Month

Displays the IP address and average daily availability of all monitored nodes over the current month.

Availability - This Month

Displays the IP address and average daily availability of all monitored nodes over the current month.

Availability - This Year

Displays the IP address and average daily availability of all monitored nodes over the last 12 months.

EnergyWise Reports

The following reports on EnergyWise-enabled devices are provided by default with Orion NPM.

Note: For more information about monitoring devices featuring EnergyWise energy management, see “Monitoring EnergyWise Devices” on page 111.

Current EnergyWise Status per Interface

Displays a list of all interfaces on the EnergyWise-enabled devices on your network. For each listed interface, this report provides interface identification,

including the Caption, Entity Name, and Role for the interface and the following EnergyWise-related information:

- Interface Status
- Current EnergyWise Energy Level
- EnergyWise Events Count

For more information, see “Monitoring EnergyWise Devices” on page 111.

EnergyWise Readiness Report

Displays a list of devices currently monitored by Orion NPM with a report answering the following EnergyWise-related questions for each device:

- Is EnergyWise enabled on this device, True or False?
- Does this device IOS support EnergyWise, True or False?
- Does this device hardware support EnergyWise, True or False?

Additionally, for each listed device this report tells you the device IP Address, the device Vendor, and the IOS Image and Version for the listed device. For more information, see “Monitoring EnergyWise Devices” on page 111.

Total Energy Consumption and Savings Network-Wide – Last 7 Days

Displays the Average and Maximum Energy Usage and the Average Energy Savings for all EnergyWise capable devices on your network over the last 7 days. For more information about EnergyWise energy management, see “Monitoring EnergyWise Devices” on page 111.

Total Energy Consumption and Savings Network-Wide – Last Month

Displays the Average and Maximum Energy Usage and the Average Energy Savings for all EnergyWise-enabled devices on your network during the previous calendar month. For more information about EnergyWise energy management, see “Monitoring EnergyWise Devices” on page 111.

Total Energy Consumption and Savings Network-Wide – This Month

Displays the average and maximum energy usage and the average energy savings for all EnergyWise-enabled devices on your network during the current calendar month. For more information about EnergyWise energy management, see “Monitoring EnergyWise Devices” on page 111.

Total Energy Consumption and Savings per EnergyWise Device – Last 7 Days

Displays the Average and Maximum Energy Usage and the Average Energy Savings for a selected EnergyWise capable device on your network over the

last 7 days. The node name and IP address are also provided for each listed EnergyWise-enabled device. For more information about EnergyWise energy management, see “Monitoring EnergyWise Devices” on page 111.

Total Energy Consumption and Savings per EnergyWise Device – Last Month

Displays the Average and Maximum Energy Usage and the Average Energy Savings for a selected EnergyWise capable device on your network during the previous calendar month. The node name and IP address are also provided for each listed EnergyWise-enabled device. For more information about EnergyWise, see “Monitoring EnergyWise Devices” on page 111.

Total Energy Consumption and Savings per EnergyWise Device – This Month

Displays the Average and Maximum Energy Usage and the Average Energy Savings for a selected EnergyWise capable device on your network during the current calendar month. The node name and IP address are also provided for each listed EnergyWise-enabled device. For more information about EnergyWise, see “Monitoring EnergyWise Devices” on page 111.

Total Energy Consumption and Savings per EnergyWise Entity – Last 7 Days

Displays the Average and Maximum Energy Usage and the Average Energy Savings for all EnergyWise entities on a selected EnergyWise capable device on your network during the last 7 days. The name and role are also provided for each listed EnergyWise-enabled entity. For more information about EnergyWise energy management, see “Monitoring EnergyWise Devices” on page 111.

Total Energy Consumption and Savings per EnergyWise Entity – Last Month

Displays the Average and Maximum Energy Usage and the Average Energy Savings for all EnergyWise entities on a selected EnergyWise capable device on your network during the previous calendar month. The name and role are also provided for each listed EnergyWise-enabled entity. For more information about EnergyWise energy management, see “Monitoring EnergyWise Devices” on page 111.

Total Energy Consumption and Savings per EnergyWise Entity – This Month

Displays the Average and Maximum Energy Usage and the Average Energy Savings for all EnergyWise entities on a selected EnergyWise capable device on your network during the current calendar month. The name and role are also provided for each listed EnergyWise-enabled entity. For more

information about EnergyWise energy management, see “Monitoring EnergyWise Devices” on page 111.

Events

The following network events reports are provided by default with Orion NPM.

All Down Events

Displays a list of all events in the database involving nodes that have stopped responding to polling over the last 12 months. For each down event, this report displays the down event date and time, the node name and IP address, and a verbal statement of the down event.

Down Events - Windows Devices

Displays a list of all events in the database involving Windows devices that have stopped responding to polling over the last month. For each down event, this report displays the down event date and time, the node name, and a verbal statement of the down event.

Last 250 Events

Displays the last 250 events involving any monitored device. For each event, this report displays the event date and time, the node involved, and a message describing the event.

Nodes that went down - Last 24 Hours

Displays a list of all nodes that have stopped responding over the last 24 hours. For every event of a node going down, this report displays the event date and time, an icon representing the current node status, the node name, and a verbal statement of the down event.

Triggered Alerts - Last 30 Days

Displays a list of all triggered alerts over the past 30 days. For each triggered alert event, this report displays the date and time of the alert trigger, the node that triggered the alert, and a message describing the triggered alert event.

Triggered and Reset Alerts - Last 30 Days

Displays a list of all triggered and reset alerts over the past 30 days. For each triggered or reset alert event, this report displays the date and time of the alert event, the node that triggered or reset the alert, and a message describing the alert event.

Historical Cisco Buffer Miss Reports

The following Cisco buffer miss reports are provided by default with Orion NPM.

Cisco Buffer Misses - Last 7 Days

Displays all buffer misses on monitored Cisco devices over the past 7 days. For all Cisco devices with buffer misses, this report displays a count of all buffer misses combined and counts of small, medium, big, large, and huge buffer misses.

Cisco Buffer Misses - Last Month

Displays all buffer misses on monitored Cisco devices over the previous calendar month. For all Cisco devices with buffer misses, this report displays a count of all buffer misses combined and counts of small, medium, big, large, and huge buffer misses.

Cisco Buffer Misses - This Month

Displays all buffer misses on monitored Cisco devices over the current calendar month. For all Cisco devices with buffer misses, this report displays a count of all buffer misses combined and counts of small, medium, big, large, and huge buffer misses.

Historical CPU and Memory Reports

Orion NPM provides a **CPU Load - Last Month** report by default. This report displays the vendor icon and average and peak CPU load percentages for all monitored nodes with CPUs over the previous calendar month.

Historical Response Time Reports

The following response time reports are provided by default with Orion NPM.

Response Time - Last Month

Displays average and peak response times for all monitored nodes over the previous calendar month.

Response Time - Top 10 Last Month

Displays the average and peak response times for the top ten monitored nodes over the previous calendar month.

Historical Traffic Reports

The following network traffic reports are provided by default with Orion NPM.

95th Percentile Traffic Rate - Last 7 Days

Displays 95th percentile traffic rates for all monitored interfaces over the last 7 days. For each interface, the interface ID, parent node, interface name, and receive, transmit and maximum 95th percentile traffic rates are shown.

95th Percentile Traffic Rate - Last Month

Displays 95th percentile traffic rates for all monitored interfaces over the last month. For each interface, the interface ID, parent node, interface name, and receive, transmit and maximum 95th percentile traffic rates are shown.

95th Percentile Traffic Rate - This Month

Displays 95th percentile traffic rates for all monitored interfaces in the current month. For each interface, the interface ID, parent node, interface name, and receive, transmit and maximum 95th percentile traffic rates are shown.

Average and Peak Traffic Rates - Last 7 Days

Displays the average and peak receive and transmit traffic rates for all monitored interfaces over the last 7 days. Interfaces are listed under their respective parent nodes.

Average and Peak Traffic Rates - Last Month

Displays the average and peak receive and transmit traffic rates for all monitored interfaces over the last month. Interfaces are listed under their respective parent nodes.

Average and Peak Traffic Rates - This Month

Displays the average and peak receive and transmit traffic rates for all monitored interfaces during the current month. Interfaces are listed under their respective parent nodes.

Average and Peak Traffic Rates - WAN Interfaces Last 7 Days

Displays the average and peak receive and transmit traffic rates, with MAC addresses, for all monitored WAN interfaces over the last 7 days. Interfaces are listed under their respective parent nodes.

Total Bytes Transferred by Cisco Devices - Last Month

Displays the total bytes transferred (receive + transmit) and total bytes transmitted and received for all monitored Cisco devices over the last month.

Total Bytes Transferred by Interface - Last Month

Displays the total bytes transferred (receive + transmit) and total bytes transmitted and received for all monitored interfaces over the last month. Interfaces are listed under their respective parent nodes.

Total Bytes Transferred by Interface - This Month

Displays the total bytes transferred (receive + transmit) and total bytes transmitted and received for all monitored interfaces during the current month. Interfaces are listed under their respective parent nodes.

Total Bytes Transferred by Node - Last 7 Days

Displays the total bytes transferred (receive + transmit) and total bytes transmitted and received for all monitored nodes over the last 7 days.

Total Bytes Transferred by Node - Last Month

Displays the total bytes transferred (receive + transmit) and total bytes transmitted and received for all monitored nodes over the last month.

Total Bytes Transferred by Node - This Month

Displays the total bytes transferred (receive + transmit) and total bytes transmitted and received for all monitored nodes during the current month.

Historical VMware ESX Server Reports

Orion NPM provides the following VMware ESX Server performance reports are provided by default with Orion NPM.

Network Traffic by VM for Last 7 Days

For each monitored VMware ESX Server, this report displays the average daily network traffic on the ESX Server per hosted VM for the last 7 days.

Network Traffic by VM for Last Month

For each monitored VMware ESX Server, this report displays the average daily network traffic on the ESX Server per hosted VM for the last month.

Percent of CPU by VM for Last 7 Days

For each monitored VMware ESX Server, this report displays the average daily CPU load on the ESX Server due to each hosted VM for the last 7 days.

Percent of CPU by VM for Last Month

For each monitored VMware ESX Server, this report displays the average daily CPU load on the ESX Server due to each hosted VM for the last month.

Percent of Memory by VM for Last 7 Days

For each monitored VMware ESX Server, this report displays the average daily memory load on the ESX Server due to each hosted VM for the last 7 days.

Percent of Memory by VM for Last Month

For each monitored VMware ESX Server, this report displays the average daily memory load on the ESX Server due to each hosted VM for the last month.

Percent of Time Running vs. Stopped

For each monitored VMware ESX Server, this report displays both the percentage of time that each hosted VM has been running and the percentage of time that each hosted VM has been stopped.

Historical Volume Usage Reports

Orion NPM provides an **Average Disk Space Used - Last 12 Months** report by default. For all monitored volumes, this report displays the volume type and size, percentage of the volume space that is currently available, amount of the available space that is currently used, and the amount of volume space that is currently available. Volumes are listed beneath their respective parent nodes.

Inventory

The following network inventory reports are provided by default with Orion NPM.

All Disk Volumes

For all monitored volumes, this report displays the volume type and size, available space on the volume, amount of the available space that is currently used, and the peak amount of the available space that has been used on the volume, with the month in which peak usage occurred, over the last 12 months. Volumes are listed beneath their respective parent nodes.

Device Types

Displays a list of monitored machine types and the number of each type that are currently monitored.

IOS Versions of Cisco Devices

For all monitored Cisco devices, this report displays the device name, machine type, and Cisco IOS Version and Image.

Interface Bandwidth

Displays the name and configured transmit and receive bandwidths for all monitored Interfaces. Interfaces are listed under respective parent nodes.

Interface Types

Displays a list of monitored interface types and the number of each type that are currently monitored.

Wireless Reports

The following reports of monitored wireless access points and clients are provided by default with Orion NPM.

Availability of Wireless Access Points – Last 7 Days

Displays the availability of all monitored wireless access points over the last 7 days.

Availability of Wireless Access Points – Last Month

Displays the availability of all monitored wireless access points over the last month.

Availability of Wireless Access Points – This Month

Displays the availability of all monitored wireless access points during the current month.

Average and Peak Number of Clients by Access Point – Last 7 Days

Displays both the average and the peak number of clients hosted by each monitored wireless access point over the last 7 days.

Average and Peak Number of Clients by Access Point – Last Month

Displays both the average and the peak number of clients hosted by each monitored wireless access point over the last month.

Average and Peak Number of Clients by Access Point – This Month

Displays both the average and the peak number of clients hosted by each monitored wireless access point during the current month.

Average and Peak Traffic Rates by Access Point – Last 7 Days

Displays both the average and the peak traffic rates for each monitored wireless access point over the last 7 days.

Average and Peak Traffic Rates by Access Point – Last Month

Displays both the average and the peak traffic rates for each monitored wireless access point over the last month.

Average and Peak Traffic Rates by Access Point – This Month

Displays both the average and the peak traffic rates for each monitored wireless access point during the current month.

Rogue Access Points – Last 7 Days

Displays a list of all rogue wireless access points, identified by MAC address, detected over the last 7 days.

Rogue Access Points – Last Month

Displays a list of all rogue wireless access points, identified by MAC address, detected over the last month.

Rogue Access Points – This Month

Displays a list of all rogue wireless access points, identified by MAC address, detected during the current month.

Top 25 Wireless Clients by Traffic Rates over the Last 7 Days

Displays the traffic rates for the top 25 monitored wireless clients over the last 7 days.

Total Bytes Transferred by Access Point – Last 7 Days

Displays the total bytes both transmitted and received by each monitored wireless access point over the last 7 days.

Total Bytes Transferred by Access Point – Last Month

Displays the total bytes both transmitted and received by each monitored wireless access point over the last month.

Total Bytes Transferred by Access Point – This Month

Displays the total bytes both transmitted and received by each monitored wireless access point during the current month.

Getting Started with Report Writer

Before using Report Writer, you must have collected at least a few minutes worth of data in a database populated with devices you want to monitor. A variety of reports are included with Report Writer, and icons that precede report names distinguish available report types. The following procedure starts Report Writer.

To start Report Writer:

1. Click **Start > All Programs > SolarWinds Orion > Alerting, Reporting, and Mapping > Report Writer**.
 2. Click **File > Settings**.
 3. In the General tab of the Report Writer Settings window, select either of the following as a default viewing mode:
 - **Preview** displays the report as it will appear in printed form. For more information, see “Preview Mode” on page 198.
 - **Report Designer** is the report creation and editing interface. For more information, see “Design Mode” on page 199.
- Note:** You can toggle between Preview and Report Designer modes at any time by clicking **Preview** or **Design**, respectively, on the toolbar.
4. **If you want to separate the data for individual network objects with horizontal lines**, click **Report Style**, and then check **Display horizontal lines between each row**.
 5. Click **OK** to exit Report Writer Settings.

Preview Mode

Preview mode shows a report as it will print. When you open a report in Preview mode, or switch to Preview mode from Design mode, Orion NPM runs the query to generate the report, and then Report Writer displays the results.

The Preview window toolbar provides the following actions and information:

- Current page number and total number of pages in the report.
 - Page navigation buttons: First Page, Page Up, Page Down, and Last Page
 - Zoom views
- Note:** Double-click a preview to zoom in and double-right-click to zoom out.
- Print report

Design Mode

Use Design mode to create new reports and modify or rename existing reports. The options available for both creating and modifying reports are the same. Design mode options are also dynamic, based upon the type of report, included report data, and report presentation. Available options differ according to the type of report that you are designing, but all reports require that you select the data to include and decide how that data will be sorted, ordered, filtered, and presented.

Creating and Modifying Reports

Use the following procedure to modify or create reports in Report Writer.

To open a report with Report Writer:

1. **If you want to modify an existing report**, click an existing report from the inventory in the left pane of the main Report Writer window.
2. **If you want to create a new report**, click **File > New Report**, select the type of report that you would like to create, and then click **OK**.

Each report offers different configuration options, so, depending on the report, some formatting tabs described in the following sections may not be available.

Notes:

- The SQL query used to generate a report may be viewed in an additional tab. Click **Report > Show SQL** to add a read-only SQL tab to the Design window.
- A preview of your report is also available at any time. Click **Preview** to enter Preview Mode, and then click **Design** to return to Design Mode.

General Options Tab

The General tab opens by default and shows titling and display options.

To configure General options:

1. Specify the **Report Group**, **Report Title**, **Subtitle**, and **Description**.
Note: If you use an existing report group name, the new report is added to that existing group in the left pane of the main window.
2. Select the display **Orientation** of your report.
3. **If you are configuring an historical report and you do not want to group data by days**, clear **Group historical data by days**.

Note: By default, data in some availability and historical reports is grouped by days when displayed in the Orion Web Console. Data grouping by days is not viewable in Report Viewer.

4. **If you do not want to make this report available on your Orion Web Console**, clear **Make this Report available from the Orion website**.

Note: By default, most reports are made available for display in the Orion Web Console. For more information about adding reports to Orion Web Console views, see “Customizing Views” on page 46.

Select Fields Options Tab

The Select Fields tab allows you to select the data fields in a report.

To select and configure fields:

1. Click Select Fields.
2. **If you are creating a new report or adding fields to an existing report**, click the ellipsis, select **Add a new field**, and then dynamically define each new report field as follows:
 - a. Click the asterisk after **Field**.
 - b. Select the type of information to include in the current report field.
 - c. **If you want to sort the data in the current field**, click the **sort** asterisk and select a sort order.
 - d. **If you want to perform an operation on the data in the current field**, click the **function** asterisk and select an operation.
3. **If you are modifying an existing report**, click the **Field**, **sort**, or **function** that you want to change and select a new value as follows.
 - a. Click the asterisk after **Field**.
 - b. Select the type of information to include in the current report field.
 - c. **If you want to sort the data in the current field**, click the **sort** asterisk and select a sort order.
 - d. **If you want to perform an operation on the data in the current field**, click the **function** asterisk and select an operation.
4. **If you want to test your selections as you assemble your report**, click **Execute SQL Query** to view the current query results.
5. **If you want to delete a field or rearrange the order of the fields that are listed in your report**, select a field, click **Browse (...)**, and then select the appropriate action.

Note: Unchecked fields are not displayed in your report, but their sort and function configurations are retained.
6. **If you want to preview your report**, click **Preview**.

Filter Results Options Tab

The Filter Results tab allows you to generate filter conditions for field data by selecting appropriate descriptors from the linked context menus. Results filters are configured as follows.

To configure results filters:

1. Click **Browse (...)**, and then select from the following options:
 - Select **Add a new elementary condition** to generate a condition that is based on a direct comparison of network object data fields.
 - Select **Add a new advanced elementary condition** to generate a condition based on a comparison of device data fields and values.
 - Select **Add a new complex condition** to define a condition that filters other defined conditions.
 - Select **Delete current condition** to remove a selected condition.
 - Select **Move current condition forward** or **Move current condition backward** to change the order of your conditions accordingly.

Note: The lists of available linked descriptors are dynamically generated in consideration of all other variables within the same condition. For more information about condition groups and their application, see “Understanding Condition Groups” on page 153.

2. Check or clear individual filter conditions to enable or disable their application, respectively, to your report.

Top XX Records Options Tab

The Top XX tab allows you to limit the number of records that are shown in your report to either a top *number* or a top *percentage* of all results. Top XX options are configured as shown in the following procedure.

To configure Top XX records:

1. **If you want to show all records in your report**, select **Show All Records**.
2. **If you want to specify a truncated list of eligible items for your report**, complete the following steps:
 - a. select either **Show only the Top *number* Records** or **Show the Top *percentage* % of Records**
 - b. Provide appropriate *number* or *percentage* values.

Time Frame Options Tab

The Time Frame options tab allows you to limit the scope of your report to a specific period of time. To configure Time Frame options, select a **Named**, **Relative**, or **Specific Time Frame** for your report, and then select or provide required values.

Notes:

- If you receive a SQL Timeout error message, you may edit the timeout setting in the SWNetPerfMon.db file. By default, this file is located in the C:\Program Files\SolarWinds\Orion directory
- Since the **Relative Time Frame** is continuously variable, reports run with it may show different results, even if they are run close together in time.

Summarization Options Tab

The Summarization tab allows you to generate summaries of your results over specific periods of time. Summarization options are configured as follows.

To configure results summarization:

1. *If you do not want to summarize your results*, confirm that **Do not Summarize the Results** is selected.
2. *If you want to summarize your results*, complete the following steps:
 - a. Select **Summarize the Results by Hour, Date, Month, etc**, and then select the summarization period.
 - b. Specify the location of the summary field for your report.
 - c. Select a location for the **Summary Date/Time** field.

Report Grouping Options Tab

The Report Grouping tab allows you to group results by field descriptor within your report. Add, edit and delete report groups to organize the data in your report. Establish and edit report groups as follows.

To add and edit report groups:

1. *If you want to add a new report group*, select a field from the list to define your group, and then click **Add Report Group** to add your selected field to the **Report Groups** list.

Note: Use up and down arrows to change the grouping order accordingly.

2. *If you want to edit an existing report group*, select the field from the Report Groups list, and then click **Edit Report Group**.

3. The following options may be changed as needed:
 - The **Group Header** is the text that designates groups on your report.
 - The **Web URL** is the dynamic location of your published report with respect to your Orion Web Console.
 - **Font** size, face, color, and background may all be modified by clicking associated ellipses.
 - **Alignment** may be left, center, or right.
 - Check **Transparent Background** for better results when publishing your report to the Web.
 - If you want to change the grouping order, use the up and down arrows to change the grouping order accordingly.

Field Formatting Options Tab

The Field Formatting tab allows you to customize the format of the various results fields in your report. To format results fields, select the field you want to format, and then edit labels and select options as appropriate.

Notes:

- The formatting options available for each field may be different according to the nature of the data contained in that field.
- Check **Hidden Field** to hide any field in your report.
- To view your changes at any time, click **Preview**.

Customizing the Report Header and Footer Image

The image that is displayed at the top and bottom of each report can be changed. To add your company logo as the report header and footer, save your logo as `Header.jpg` in the `SolarWinds\Common\WebResources` folder, typically located in `C:\Program Files\`, and then click **Refresh**.

Note: The image must be in JPEG format with a height of 150 pixels or less.

Exporting Reports

Orion Report Writer gives you the ability to present your created reports in any of the following industry-standard formats:

- Comma-delimited (*.csv, *.cdf)
- Text (*.txt)

- HTML (*.htm, *.html)
- MIME HTML, with embedded images (*.mhtml)
- Excel® spreadsheet (*.xls)
- Adobe® PDF (*.pdf)
- Image (*.gif)

The following procedure presents the steps required to export an open report from Orion Report Writer into any of the previously listed formats.

To export a report from Report Writer:

1. Select a report to export by clicking any of the following:
 - Select a report from the file tree in the left pane
 - **File > Open** to open an existing report
 - **File > New Report** to create a new report. For more information about creating reports, see “Creating Reports” on page 185.
2. Select **File > Export** and then click the format in which you want to export your report:
3. Check the fields in your open report that you want to export into the selected format, and then click **OK**.
4. Select a location to save your file.
5. Provide a **File name**, and then click **Save**.

Example Report

The following procedure generates an example report of network device availability information over the previous week. The final report is sorted so that the worst errors are viewed first. Down nodes that are still down are at the top with all devices listed in order of increasing availability.

Note: At any point during the creation of a report (or perhaps at many points), you may save what you have done by clicking **File > Save**. The first time you save you must give your report a filename or accept the default, which will be the report title that you assign in the following procedure.

To generates an example report of network device availability information:

1. Click **File > New Report**.
2. The example calls for a report on availability over the past week, so select **Historical Availability Details**, and then click **OK**.

3. Type `My Reports` in the **Report Group** field.
4. Enter `Last Week's Availability` as the **Report Title**.
5. Select **Portrait** for the paper orientation.
6. Click **Select Fields**.
7. Click the ellipsis, and then select **Add a new field**.
8. Click the **Field** asterisk, and then select **Network Nodes > Node Details > Node Name**.
9. Click the ellipsis, and then select **Add a new field**.
10. Click the **Field** asterisk, and then select **Network Nodes > Node Status > Status**.
11. Click the ellipsis, and then select **Add a new field**.
12. Click the **Field** asterisk, and then select **Network Nodes > Node Status > Status Icon**.

Note: While this field makes a distinct visual difference for a report viewed in color, it will make little or no difference if printed in black and white.

13. Click **Execute SQL Query** to view the report data in the preview window.
14. *If you want to see the status icon before the status description*, click **Status Icon** to move **Browse (...)** to the Status Icon line, and select **Move Current Field Backward**.
15. Click **Execute SQL Query**.

Note: The report should show information about both current and historical status. Current status entries must be relabeled to avoid confusion.

16. Click **Field Formatting**.
17. Select **Status** from the field list.
18. Change the **Column Header** entry to `Current Status`.
19. Select **Status_Icon** from the field list.
20. Change the **Column Header** entry to `Current Status`.
21. Click **Execute SQL Query**.

Note: Column widths are adjustable. To change a column width, place your cursor on the column divider and drag it to a different position.

22. Click **Select Fields**.
23. Click the **sort** asterisk on the Status field line, and then select **descending**.
24. Click **Execute SQL Query** to confirm your choice.

25. Click the ellipsis, and then select **Add a new field**.
26. Click the **Field** asterisk, and then select **Historical Response Time and Availability > Availability**.
27. Click the **sort** asterisk on the new line, and then select **ascending**.
28. Click **Execute SQL Query** to view the report.
29. Click Time Frame.
30. Select **Relative Time Frame**, type 7 in the text field, and then select **Days** from the list.
31. *If you want to break down the report day-by-day*, click Summarization and specify your choices.
32. *If you want to filter your report*, click Filter Results and specify filter rules.
33. Click **File > Save** to save your work.

Using Orion Report Scheduler

Orion NPM provides the Orion Report Scheduler to configure reports for automatic generation and distribution.

Creating a Scheduled Report Job

The following procedure creates a scheduled report job for regularly printed or emailed Orion reports.

To schedule a report:

1. Click **Start > All Programs > SolarWinds Orion > Alerting, Reporting, and Mapping > Orion Report Scheduler**.
2. Click **Edit > Add New Job**.
3. Type a name for your new scheduled report job, and then click **Continue**.
4. Click **Continue**.
5. Click **Browse (...)**, to locate the URL for the report you want to send in the Orion Web Console, and then click **Use Current URL**.
6. *If you need to provide Windows login credentials to view the report you are scheduling*, click the NT Account login tab, and then provide the user account details needed to log in.
7. *If you want to create a printable report that excludes the Orion NPM web page banner and menu bar*, on the Orion Web Login tab, check **Retrieve a Printable Version of this Page**.

8. **If the report you are scheduling requires a Orion NPM user account**, on the Orion Web Login tab, check **Send Orion Username / Password in URL**, and then provide the required user credentials to view the Orion NPM report.
9. Click **Continue**.
10. Configure the scheduling for your report job, and then click **Continue**.
11. **If you want to email the report**, complete the following procedure:
 - a. Confirm that **Email the Web Page** is selected.
 - b. Provide required email addresses and a subject in the appropriate fields on the Email To tab.
 - c. Provide a name and reply address on the Email From tab.
 - d. On the SMTP Server tab, type the hostname or IP address of the SMTP server used to send email from the Orion server.
 - e. Confirm the suggested SMTP Port Number on the SMTP server for sending email from the Orion server.
12. **If you want to print the report**, select **Print the Web Page**, and then select the Printer, Orientation, and number of Copies you want to print.
13. Click **Continue**.
14. Provide required Windows user account details, and then click **Continue**.
15. Type any comments you want to add to the job description.
16. Click **Finish**.

Using Orion Report Scheduler with HTTPS

If you are using HTTPS to view reports in the Orion Web Console, your HTTPS server may require the Orion Report Scheduler to provide a trusted certificate before the requested report may be printed or sent. To use Orion Report Scheduler with HTTPS, either provide valid certificates to all users accounts requesting reports from the HTTPS server using Orion Report Scheduler or disable certificate checking in each of the browsers used by your Orion Report Scheduler users, as shown in the following procedure.

To disable certificate checking:

1. **If you are configuring Internet Explorer**, complete the following steps:
 - a. Open Internet Explorer on the user computer.
 - b. Click **Tools > Internet Options**, and then click the Advanced tab.

- c. In the Security section, confirm that the following options are cleared:
 - **Check for publisher's certificate revocation**
 - **Check for server certificate revocation (requires restart)**
 - **Warn about invalid site certificates**
 - d. Click **OK**.
2. **If you are configuring Mozilla Firefox**, complete the following steps:
- a. Open Mozilla Firefox on the user computer.
 - b. Click **Tools > Options**.
 - c. Click **Advanced**, and then click the Encryption tab.
 - d. In the Protocols area, clear both **Use SSL 3.0** and **Use TLS 1.0**.
 - e. In the Certificates area, select **Select one automatically**, and then click **Validation**.
 - f. Clear the option **Use the Online Certificate Status Protocol (OCSP) to confirm the current validity of certificates**, and then click **OK**.

Reports and Account Limitations

Reports created with Orion Report Writer respect Orion Web Console account limitations. For security, by default, reports are not available to users with limited accounts unless an Orion NPM administrator specifically provides access. The following procedure creates a reports folder for an account-limited user and configures the account-limited user to access Orion reports from it.

Note: For more information about creating user accounts, see “Creating New Accounts” on page 91. For more information about applying account limitations to user accounts, see “Setting Account Limitations” on page 93.

To allow account-limited users access to reports:

1. Open the Orion Reports folder.

Note: All reports created or predefined in Orion Report Writer are, by default, stored, in `C:\Program Files\Solarwinds\Orion\Reports`.
2. Create a new folder using the name of the account-limited user.
3. Copy the reports you want the account-limited user to see from the Orion Reports folder into the new, account-limited user folder.
4. Click **Start > All Programs > SolarWinds Orion > Orion Web Console**.
5. Log in to the Orion Web Console as an administrator.
6. Click **Settings** in the top right of the web console.

7. Click **Account Manager** in the Accounts grouping of the Orion Website Administration page.
8. Select the account-limited user, and then click **Edit**.
9. In the Default Menu Bar and Views section, select the **Report Folder** you created in the Orion Reports folder for the account-limited user.
10. Click **Submit**.

Chapter 15

Monitoring Syslog Messages

Syslog messages are one type of realtime notification that network devices can send in response to specific, designated network events. Orion NPM provides you with the SolarWinds Syslog Service, giving you the ability to receive Syslog messages from any monitored network device. The SolarWinds Syslog Service also has the ability to open multiple connections to your SQL server, so it can handle large numbers of simultaneously incoming Syslog messages from all your monitored network devices.

Orion NPM uses the SolarWinds Syslog Service to listen on UDP port 514 for incoming Syslog messages. Received messages are then decoded and stored in the Orion database. Until they are acknowledged, Syslog messages are available for viewing either in the web console Syslog view or in the Syslog Viewer application. The Syslog view in the Orion Web Console provides quick access to current messages, filtered by any or all of the following criteria:

- Network Object sending the message.
- Type of device sending the message.
- Message Severity or Facility.
- Message Type or Pattern.
- Time Period in which the message was sent.

The Syslog Viewer application also allows you to tailor your view of Syslog messages using fully customizable rules. Additionally, the Syslog Viewer gives you the ability both to search your Orion database and to configure Syslog-specific alerts for received Syslog messages.

Note: When configuring your network devices to send Syslog messages, confirm that messages are sent to the IP address assigned to your Orion NPM server. To ensure the proper configuration of a network device for Syslog messaging, refer to the documentation supplied by the device vendor.

Syslog Messages in the Web Console

The Orion Web Console provides both Syslog-specific resources and a Syslog view that provides a table view of Syslog messages received by your Orion NPM server. The following sections provide an overview of available Syslog resources and procedures for viewing and acknowledging Syslog messages within the Orion Web Console.

Syslog Resources

Orion NPM provides the following Syslog-related resources for inclusion within web console views.

Advanced Syslog Counts

Every Syslog message has a designated severity. For more information about Syslog severities, see “Syslog Severities” on page 223. The Advanced Syslog Counts resource groups by severity all Syslog messages received by the currently viewed node. For each severity, this resource provides the number of received Syslog messages.

Advanced Syslog Parser

The Advanced Syslog Parser resource provides a comprehensive view of the Syslog messages most recently received by the viewed node. The most recent messages of each severity are listed. For more information about Syslog severities, see “Syslog Severities” on page 223.

Advanced Syslog Summary

The Advanced Syslog Summary resource groups by message type all Syslog messages received by the currently viewed node, where the message type is encoded in the Syslog message packet. For each message type, this resource provides the severity, the hostname or IP address of the message originator, and the total number of Syslog messages received.

Last 25 Syslog Messages

The Last 25 Syslog Messages resource provides a list of the last 25 syslog messages that have been sent by monitored network devices to the viewed node. For each message, this resource presents the date and time the message was sent, the hostname and IP address of the device sending the message, and the message text.

Clicking the hostname, IP address, or message text opens the corresponding Orion NPM *device* Details page, providing extensive diagnostic information about the device sending the message.

Clicking **Edit** opens the Edit Last 25 Syslog Messages page where you can set the maximum number of displayed messages, select the time period for viewing messages, and establish filters to limit the messages this resource displays. For more information, see “Using Node Filters” on page 65.

Syslog Summary

The Syslog Summary resource lists the number of Syslog messages received by the viewed node from monitored network devices over a specified period of time.

Viewing Syslog Messages in the Web Console

You can customize the list view by using the following procedure to select your preferred message grouping criteria.

To view Syslog messages in the Web Console:

1. Click **Start > All Programs > SolarWinds Orion > Orion Web Console**.
2. Log in to the Orion Web Console.
3. Click **Syslog** in the Views toolbar.
4. *If you want to filter your Syslog messages table view by device*, select the device to which you want to limit your view in the **Network Object** field.
5. *If you want to filter your Syslog messages table by device type*, select the type to which you want to limit your view in the **Type of Device** field.
6. *If you want to filter your Syslog messages table by severity*, select the severity level to which you want to limit your view in the **Select Severity** field.

Note: For more information, see “Syslog Severities” on page 223.

7. *If you want to filter your Syslog messages table by facility*, select the facility to which you want to limit your view in the **Select Facility** field.

Note: For more information, see “Syslog Facilities” on page 222.

8. *If you want to limit your Syslog messages table to show only messages of a designated type*, type the appropriate string in the **Message Type** field.
9. *If you want to limit your Syslog messages table to show only messages containing a designated pattern*, provide the appropriate string in the **Message Pattern** field.

Note: An asterisk (*) is required as a wildcard character, both before and after the pattern string, unless the provided pattern is any of the following:

- The beginning of the message
 - The end of the message
 - The full message
10. *If you only want to see Syslog messages from a specific period of time*, select a time period from the **Time Period** menu.
 11. Confirm the number of messages displayed in the **Show Messages** field.
 12. *If you want cleared or acknowledged messages to remain in the Syslog view*, check **Show Cleared Messages**.
 13. Click **Refresh** to update the Syslog messages list with your new settings.

Acknowledging Syslog Messages in the Web Console

Acknowledging Syslog messages is straightforward in the Orion Web Console, as shown in the following procedure.

To acknowledge Syslog messages in the Orion Web Console:

1. Click **Start > All Programs > SolarWinds Orion > Orion Web Console**.
2. Log in to the Orion Web Console.
3. Click **Syslog** in the Views toolbar.
4. Provide filter criteria for the Syslog messages table. For more information, see “Viewing Syslog Messages in the Web Console” on page 213.
5. Click **Refresh** to ensure that all selected view criteria take effect.
6. Check the messages you want to acknowledge, and then click **Clear Selected Messages**.

Using the Syslog Viewer

Orion NPM also provides the standalone Syslog Viewer application for viewing and acknowledging Syslog messages on your network. Syslog Viewer collects Syslog messages from your network and presents them in a readily reviewable and searchable list so that you can easily monitor your network. The following sections provide a guide to using the Syslog Viewer application for viewing, acknowledging, and triggering alerts in response to Syslog messages on your network.

To open the Syslog Viewer, click **Start > All Programs > SolarWinds Orion > Syslog and SNMP Traps > Syslog Viewer**.

Viewing and Acknowledging Current Messages

The Syslog Viewer makes it easy to view and acknowledge messages. The following procedure views and then acknowledges current Syslog messages.

To view and acknowledge current Syslog messages:

1. Click **View > Current Messages**
2. Acknowledge current messages using either of the following methods:
 - Right-click any message, and then select **Acknowledge Selected**.
 - Add an **Acknowledged** column to the Syslog Viewer, and then check each message that you want to acknowledge. For more information, see “Syslog Server Settings” on page 215.

Searching for Syslog Messages

Collected Syslog messages may be searched within Syslog Viewer. The following steps both search for Syslog messages and format search results.

To search the Syslog message list:

1. Click **View > Search Messages**.
2. Enter appropriate search criteria, and then click **Search Database**.
3. *If you want to group messages for easier navigation*, select the type of grouping from the **Grouping** list.

Note: Messages can be acknowledged in the search results just as they can be acknowledged in the **Current Messages** view. For more information, see “Syslog Server Settings” on page 215.

4. *If you want to limit the number of messages that are shown*, enter or select a number in the **Maximum number of messages to display** field.
5. *If you want to view messages that meet your search criteria as they arrive*, select a number for the **Auto Refresh every *number* seconds** field.

Note: Auto Refresh is only available when you are viewing current messages. The **Date/Time Range** must be set to **Today**, **Last 24 Hours**, **Last 2 Hours**, or **Last Hour**.

Syslog Server Settings

Use the following procedure as a guide to starting and configuring the Syslog Viewer.

To start and configure the Syslog Viewer:

1. Click **Start > All Programs > SolarWinds Orion > Syslog and SNMP Traps > Syslog Viewer**.
2. Click **File > Settings**.
3. Click the General tab in the Syslog Server Settings window.
4. Adjust the **Maximum number of messages to display in Current Messages view** slider to set the number of messages you want to display.
5. *If you want to Automatically Refresh the Current Messages View*, check the option accordingly, and then set the refresh rate with the middle slider.
6. Adjust **Retain Syslog messages for how many days?** to set the length of time Syslog messages should stay in the database.
7. Click the Displayed Columns tab.

8. Use the arrow keys to select and order the fields of information you want to see in the Current Messages view.
Note: You can make it easier to acknowledge Syslog messages by selecting the **Acknowledged** column to add to your view.
9. *If you want to wrap Syslog message text in the Current Messages view*, check **Word wrap long messages**.
10. *If you do not expect to use Syslog Server as your primary viewer for Syslog messages*, select the Message Parsing tab, and then complete the following steps:
Note: The following data points are saved within the Syslog tables in your Orion database. Removing the added data from each record helps you to proactively reduce the size of your database.
11. Check **Remove embedded Date/Time from Syslog Messages**, **Remove Message Type from Syslog Messages**, and **Remove Domain Name from DNS Lookups**.

Configuring Syslog Viewer Filters and Alerts

The Syslog Viewer can be configured to signal Orion NPM alert actions when Syslog messages that are received from network devices match defined rules. The steps in the following procedure establish rules that filter Syslog messages and initiate alert actions as you determine.

Note: Syslog rules may not be applied to nodes in an unmanaged state. For more information about designating nodes as unmanaged, see “Setting Device Management States” on page 86.

To configure Syslog Viewer filters and alerts:

1. Click **Start > All Programs > SolarWinds Orion > Syslog and SNMP Traps > Syslog Viewer**.
2. Click **File > Settings**.
3. Click **Alerts/Filter Rules**.
4. *If you are creating a new rule*, click **Add New Rule**.
5. *If you are editing an existing rule*, select the rule, and then click **Edit Selected Rule**.
6. On the General tab, complete the following steps:
 - a. Provide or edit the **Rule Name**, and then check **Enabled**.
 - b. Select appropriate servers from the **Apply this Rule to** list.

- c. Enter the IP addresses or subnets to which this rule applies in the Source IP Addresses area.

Note: Use the examples provided on this tab to ensure that the list of source IP addresses is properly formatted.

7. ***If you want to limit the rule to only messages from specific hosts, domains, or hostname patterns,*** on the DNS Hostname tab enter a DNS Hostname Pattern.

Note: When **Use Regular Expressions in this Rule** is checked, you may use regular expressions in place of “like” statements. For more information about using regular expressions in Orion NPM, see “Regular Expression Pattern Matching” on page 345.

8. ***If you want to limit the rule to only specific message types or text within a Syslog message,*** on the Message tab enter rules as appropriate for **Message Type Pattern** and **Syslog Message Pattern**.

Notes:

- Use the examples listed on this tab to format the list properly.
- When **Use Regular Expressions in this Rule** is checked, regular expressions can be used in place of “like” statements. For more information about regular expressions, see “Regular Expression Pattern Matching” on page 345.

9. ***If you want to apply specific severity or facility types,*** on the Severity / Facility tab check the severity and facility types you want to apply.

Note: By default, all message severities and facilities are selected. For more information about Syslog severities and facilities, see “Syslog Message Priorities” on page 222.

10. ***If you want to limit rule application to within a specific period of time,*** select the Time of Day tab, check **Enable Time of Day checking**, enter the time period, and then check the days of the week on which to apply the rule.

Notes:

- Enabling Time of Day checking creates more overhead for the CPU.
- Messages received outside the specified timeframe will not trigger alerts.

11. If you want to suppress alert actions until a specified number of messages arrive that match the rule, complete the following procedure:

- a. Select the Trigger Threshold tab.
- b. Check **Define a Trigger Threshold for this Rule**.
- c. Enter option values as appropriate.

Note: When **Suspend further Alert Actions for** is checked, alert actions are not sent until the specified amount of time has expired. Once the time period has expired, only new alerts are sent. All alerts suppressed during the time period are discarded.

12. Configure Syslog alert actions on the Alert Actions tab, as shown in the following steps:

- a. **If you are associating a new action to the rule,** click **Add New Action**. For more information about available actions, see “Available Syslog Alert Actions” on page 218.
- b. **If you want to edit an existing action for the rule,** select an action from the list, and then click **Edit Selected Action**.
- c. Configure the action as appropriate. For more information about available actions, see “Available Syslog Alert Actions” on page 218.

Note: Syslog alerts use a unique set of variables. For more information about available Syslog variables, see “Syslog Alert Variables” on page 334.

- d. **If you need to delete an action,** select the action, and then click **Delete Action**.
- e. Use the arrow buttons to set the order in which actions are performed.
Note: Actions are processed in the order listed, from top to bottom.
- f. Click **OK** to save all changes and return to Syslog Viewer Settings.

13. Use the arrow buttons to arrange the order in which the rules are applied.

Note: Rules are processed in the order they appear, from top to bottom.

Available Syslog Alert Actions

The following list provides definitions of the actions available for each Syslog alert type. For more information about how to assign alert actions, see “Configuring Syslog Viewer Filters and Alerts” on page 216.

Discard the Syslog Message

Allows you to delete unwanted Syslog messages sent to the Syslog server.

Tag the Syslog Message

Allows you to add a custom tag to received Syslog messages. Ensure you include the Tag column in the viewer when assigning a tag.

Modify the Syslog Message

Modify the severity, facility, type, or contents of a Syslog message.

Log the Message to a file

Allows you to specify a file and a series of variables with which to tag Syslog messages sent to the file. Ensure you have already created the log file you want to use. The alert cannot create a file.

Windows Event Log

Write a message to local or remote Windows Event Logs.

Forward the Syslog message

Specify the IP address or hostname and the port to forward a Syslog event.

Send a new Syslog message

Trigger a new Syslog message, sent to a specific IP address or hostname, on a specific port, with a customizable severity, facility, and message.

Send an SNMP Trap

Allows you to send a trap to an IP address following a specific trap template and using a specific SNMP community string.

Play a sound

Allows you to play a sound when a matching Syslog message is received.

Text to Speech output

Define the speech engine, speed, pitch, volume, and message to read.

Execute an external program

Allows you to specify an external program to launch. This action is used when creating realtime change notifications in Orion NPM.

Execute an external VB Script

Allows you to launch a VB Script using the selected script interpreter engine and a saved script file.

Send a Windows Net Message

Allows you to send a net message either to a specific computer or to an entire domain or workgroup.

Note: Windows Server 2008 does not support Windows Net Messaging, so the Send a Windows Net Message syslog action is not available to Orion NPM installations on Windows Server 2008.

Send an E-mail / Page

Send an email from a specified account to a specified address, using a specific SMTP server, and containing a customizable subject and message.

Stop Processing Syslog Rules

Stops the processing of Syslog rules for the matching Syslog message.

Forwarding Syslog Messages

The Syslog message forwarding action allows you to forward received Syslog messages. Additionally, if you have WinPCap version 3.0 or higher installed on your Orion NPM server, you can forward Syslog messages as spoofed network packets. The following procedure configures available options for forwarded Syslog messages.

Note: The following procedure assumes you are editing a Forward the Syslog Message alert action. For more information about Syslog alert actions, see “Configuring Syslog Viewer Filters and Alerts” on page 216.

To configure the forward syslog message action:

1. Provide the hostname or IP address of the destination to which you want to forward the received Syslog message.
2. Provide the **UDP Port** you are using for Syslog messaging.

Note: The default is UDP port 514.

3. ***If you want to retain the IP address of the source device***, complete the following steps:
 - a. Check **Retain the original source address of the message**.
 - b. ***If you want to designate a specific IP address or hostname as the Syslog source***, check **Use a fixed source IP address (or hostname)**, and then provide the source IP address or hostname.
 - c. ***If you want to spoof a network packet***, check **Spoof Network Packet**, and then select an appropriate **Network Adapter**.
4. Click **OK** to complete the configuration of your Syslog forwarding action.

Syslog Alert Variables

The following variables can be used in Syslog alert messages. Each variable must begin with a dollar sign and be enclosed in curly braces as, for example, `${VariableName}`. Syslog alerts also support the use of Node alert variables. For more information, see “Alert Variables and Examples” on page 309.

Syslog Date/Time Variables

Syslog Date/Time Variable	Description
<code>\${AbbreviatedDOW}</code>	Current day of the week. Three character abbreviation.
<code>\${AMPMP}</code>	AM or PM corresponding to current time (before or after noon)
<code>\${D}</code>	Current day of the month
<code>\${DD}</code>	Current day of the month (two digit number, zero padded)
<code>\${Date}</code>	Current date. (Short Date format)
<code>\${DateTime}</code>	Current date and time. (Windows control panel defined “Short Date” and “Short Time” format)
<code>\${DayOfWeek}</code>	Current day of the week.
<code>\${DayOfYear}</code>	Numeric day of the year
<code>\${H}</code>	Current hour
<code>\${HH}</code>	Current hour. Two digit format, zero padded.
<code>\${Hour}</code>	Current hour. 24-hour format
<code>\${LocalDOW}</code>	Current day of the week. Localized language format.
<code>\${LongDate}</code>	Current date. (Long Date format)
<code>\${LocalMonthName}</code>	Current month name in the local language.
<code>\${LongTime}</code>	Current Time. (Long Time format)
<code>\${M}</code>	Current numeric month
<code>\${MM}</code>	Current month. Two digit number, zero padded.
<code>\${MMM}</code>	Current month. Three character abbreviation.
<code>\${MediumDate}</code>	Current date. (Medium Date format)
<code>\${Minute}</code>	Current minute. Two digit format, zero padded.
<code>\${Month}</code>	Full name of the current month
<code>\${N}</code>	Current month and day
<code>\${S}</code>	Current second.
<code>\${Second}</code>	Current second. Two digit format, zero padded.
<code>\${Time}</code>	Current Time. (Short Time format)
<code>\${Year2}</code>	Two digit year
<code>\${Year}</code>	Four digit year

Other Syslog Variables

Syslog Variable	Description
\$(Application)	SolarWinds application information
\$(Copyright)	Copyright information
\$(DNS)	Fully qualified node name
\$(Hostname)	Host name of the device triggering the alert
\$(IP_Address)	IP address of device triggering alert
\$(Message)	Status of device triggering alert
\$(MessageType)	The name of the triggered alert
\$(Severity)	A network health score providing 1 point for an interface in a warning state, 1000 points for a down interface, and 1 million points for a down node.
\$(Version)	Version of the SolarWinds software package

Syslog Message Priorities

Included at the beginning of each Syslog message is a priority value. The priority value range spans between 0 and 191 and is enclosed in angle bracket (< and >) delimiters. The priority value is calculated using the following formula:

$$\text{Priority} = \text{Facility} * 8 + \text{Severity}$$

Syslog Facilities

The facility value indicates which machine process created the message. The Syslog protocol was originally written on BSD Unix, so Facilities reflect the names of UNIX processes and daemons, as shown in the following table.

Note: If you are receiving messages from a UNIX system, consider using the `User` Facility as your first choice. Local0 through Local7 are not used by UNIX and are traditionally used by networking equipment. Cisco routers, for example, use Local6 or Local7.

Number	Source	Number	Source
0	kernel messages	12	NTP subsystem
1	user-level messages	13	log audit
2	mail system	14	log alert
3	system daemons	15	clock daemon
4	security/authorization messages	16	local use 0 (local0)
5	messages generated internally by Syslog	17	local use 1 (local1)
6	line printer subsystem	18	local use 2 (local2)
7	network news subsystem	19	local use 2 (local3)
8	UUCP subsystem	20	local use 2 (local4)

Number	Source	Number	Source
9	clock daemon	21	local use 2 (local5)
10	security/authorization messages	22	local use 2 (local6)
11	FTP daemon	23	local use 2 (local7)

Syslog Severities

The following table provides a list of Syslog severity levels with descriptions and suggested actions for each.

Number	Severity	Suggested Actions
0	Emergency	A "panic" condition affecting multiple applications, servers, or sites. System is unusable. Notify all technical staff on call.
1	Alert	A condition requiring immediate correction, for example, the loss of a backup ISP connection. Notify staff who can fix the problem.
2	Critical	A condition requiring immediate correction or indicating a failure in a primary system, for example, a loss of a primary ISP connection. Fix CRITICAL issues before ALERT-level problems.
3	Error	Non-urgent failures. Notify developers or administrators as errors must be resolved within a given time.
4	Warning	Warning messages are not errors, but they indicate that an error will occur if required action is not taken. An example is a file system that is 85% full. Each item must be resolved within a given time.
5	Notice	Events that are unusual but are not error conditions. These items might be summarized in an email to developers or administrators to spot potential problems. No immediate action is required.
6	Informational	Normal operational messages. These may be harvested for network maintenance functions like reporting and throughput measurement. No action is required.
7	Debug	Information useful to developers for debugging an application. This information is not useful during operations.

Chapter 16

Monitoring SNMP Traps

SNMP traps signal the occurrence of significant events by sending unsolicited SNMP messages to a monitoring device. The SolarWinds Trap Server listens for incoming trap messages on UDP port 161 and then decodes, displays, and stores the messages in the Orion NPM database. The SolarWinds Trap Service allows Orion NPM to receive and process SNMP traps from any type of monitored network device, and, because the SolarWinds Trap Service is multi-threaded, it can handle large numbers of simultaneously incoming traps.

You can view SNMP traps in the Trap Viewer application. The Trap Viewer application allows you to configure trap-specific alerts, to view and search traps, and to apply powerful trap filtering.

Note: When configuring devices to send SNMP traps, confirm that traps are sent to the IP address assigned to the Orion NPM server. To ensure proper configuration, refer to the documentation supplied by the vendor of your devices.

The SNMP Trap Protocol

SNMPv1 (Simple Network Management Protocol) and SNMPv2c, along with the associated Management Information Base (MIB), allow you to take advantage of trap-directed notification. When monitoring a large number of devices, where each device may have a large number of its own connected objects, it can become impractical to request information from every object on every device. Consider having each managed device notify the Orion NPM SNMP Trap Server of any issues without solicitation. In this configuration, a problem device notifies the server by sending a message. This message is known as a trap of the event. After receiving the event, the Trap Viewer displays it, allowing you to choose to take action or automatically trigger an action based on the nature of the event.

Viewing SNMP Traps in the Web Console

Customize the Traps view as shown in the following procedure.

To view SNMP traps in the Web Console:

1. Click **Start > All Programs > SolarWinds Orion > Orion Web Console**.
2. Click **Traps** in the Views toolbar.
3. **If you want to filter your traps table view by device**, select the device to which you want to limit your view in the **Network Object** field.

4. **If you want to filter your traps table by device type**, select the device types you want to view in the **Type of Device** field.
5. **If you want to limit your traps table to show only traps of a designated type**, select the appropriate type in the **Trap Type** field.
6. **If you want to limit your traps table to show only traps originating from a specific IP address**, type the IP Address in the **Source IP Address** field.
7. **If you want to limit your traps table to show only traps with a designated community string**, select the appropriate community string in the **Community String** field.
8. **If you only want to see traps from a specific period of time**, select the time period from the **Time Period** menu.
9. Confirm the number of traps displayed in the **Show Traps** field.
10. Click **Refresh** to update the Traps view with your new settings.

Using the Trap Viewer

After the monitored devices on your network are configured to send traps to the Orion NPM server, configure the Orion Trap Viewer to display received trap information, as shown in the following sections.

Notes:

- To ensure proper configuration of your network devices, refer to the documentation supplied by the vendor of your network devices.
- The SNMP port used by the Orion Trap Viewer to monitor traps is the same port (UDP 161) used by Orion NPM for statistics collection.

Viewing Current Traps

Trap Viewer makes it easy to view trap messages, as shown in the following steps.

To view current trap messages:

1. Click **Start > All Programs > SolarWinds Orion > Syslog and SNMP Traps > Trap Viewer**.
2. Click **View > Current Traps**.
3. Click a column header to order listed traps by the selected trap characteristic.
4. Configure the Trap Viewer by clicking and dragging columns to order the presentation of trap characteristics.

Searching for Traps

Collected trap messages may be searched within Trap Viewer. The following steps both search for trap messages and format the search results list.

To search the trap message list:

1. Click **Start > All Programs > SolarWinds Orion > Syslog and SNMP Traps > Trap Viewer**.
2. Click **View > Search Traps**.
3. Enter appropriate search criteria, and then click **Search Database**.
4. *If you want to group messages for easier navigation*, select the type of grouping from the **Grouping** list.
5. *If you want to limit the number of messages that are shown*, enter or select a number in the **Maximum number of messages to display** field.
6. *If you want to view messages that meet your search criteria as they arrive*, select a number for the **Auto Refresh every *number* seconds** field.

Note: Auto Refresh is only available when you are viewing current messages. The **Date/Time Range** must be set to **Today, Last 24 Hours, Last 2 Hours**, or **Last Hour**.

7. *If you want to hide the search criteria pane*, toggle the pane open and closed by clicking the double up arrows in the top right of the page.

Trap Viewer Settings

Use the following procedure to start and configure the Trap Viewer.

To start and configure the Trap Viewer:

1. Click **Start > All Programs > SolarWinds Orion > Syslog and SNMP Traps > Trap Viewer**.
2. Click **File > Settings**.
3. On the General tab, configure the following Trap server settings:
 - a. Position the top slider to set the **Maximum number of traps to display in Current Traps view**.
 - b. *If you want Orion NPM to Automatically Refresh the Current Traps View*, check the option accordingly, and then position the middle slider to set the refresh rate.
 - c. Position the **Retain Trap messages for how many days?** slider to set the length of time that traps remain in the database.

4. On the Displayed Columns tab, use the arrow keys to select and order the fields of information you want to see in the Current Traps view.
5. ***If you do not need the domain name from your trap messages***, check **Remove Domain Name from DNS Lookups** on the Message Parsing tab.

Note: Checking this option will remove the domain name from your trap messages, and this will help to reduce the size of your database.

Configuring Trap Viewer Filters and Alerts

The Trap Viewer can be configured to trigger Orion NPM alert actions when received trap messages match defined rules. The following steps establish rules to filter trap messages and initiate alert actions as you determine.

Notes:

- With the exception of the asterisk (*) wildcard, SolarWinds recommends against using non-alphanumeric characters in filter definitions.
- Trap rules are not applied to unmanaged nodes. For more information, see “Setting Device Management States” on page 86.

To configure Trap Viewer filters and alerts:

1. Click **Start > All Programs > SolarWinds Orion > Syslog and SNMP Traps > Trap Viewer**.
2. Click **File > Settings**, and then click the Alerts / Filter Rules tab.
3. ***If you are creating a new rule***, click **Add Rule**.
4. ***If you are editing an existing rule***, click **Edit Rule**.
5. Click the General tab,
6. Enter a **Rule Name**.
7. Check **Enabled** to enable the rule.
8. Select appropriate servers from the **Apply this Rule to** list.
9. Enter the IP addresses or subnets to which this rule applies.

Note: Use the examples listed on this tab to format the list properly.

10. ***If you want the rule limited to messages from specific hosts, domains, or hostname patterns***, click DNS Hostname, and then enter a DNS Hostname Pattern.

Note: When **Use Regular Expressions in this Rule** is checked, regular expressions can be used in place of “like” statements. For more information, see “Regular Expression Pattern Matching” on page 345.

11. **If you want the rule limited on the basis of content within the Trap Details field**, click Trap Details, and then enter a Trap Details Pattern.

Note: When **Use Regular Expressions in this Rule** is checked, regular expressions can be used in place of “like” statements. For more information, see “Regular Expression Pattern Matching” on page 345.

12. **If you want the rule limited to specific community strings**, click Community String, and then enter appropriate patterns in the **Community String Pattern** field.

Notes: When **Use Regular Expressions in this Rule** is checked, regular expressions can be used in place of “like” statements. For more information, see “Regular Expression Pattern Matching” on page 345.

13. Click Conditions, and then generate trigger conditions for rule application in the text field as follows:

- Select appropriate object identifiers and comparison functions from the linked context menus.
- Click **Browse (...)** to **Insert an “OR” condition**, to **Insert an “AND” condition**, or to **Delete a condition** as necessary.

Note: For more information about conditions and condition groups, see “Understanding Condition Groups” on page 153.

14. **If you want to limit rule application to within a specific period of time**, click Time of Day, check **Enable Time of Day checking**, enter the time period, and then select days of the week on which to apply the rule.

Notes:

- Enabling Time of Day checking creates more overhead for the CPU.
- Messages received outside the specified timeframe will not trigger alerts.

15. **If you want to suppress alert actions until a specified number of traps arrive that match the rule**, click Trigger Threshold, check **Define a Trigger Threshold for this Rule**, and then enter option values as appropriate.

Note: When **Suspend further Alert Actions for** is checked, alert actions are not sent until the specified amount of time has expired. Once the time period has expired, only new alerts are sent. All alerts that are suppressed during the time period will never be sent.

16. Click Alert Actions.

17. **If you are associating a new action to the rule**, click **Add New Action**, and then select an action from the list to configure. For more information about adding alert actions, see “Adding Alert Actions” on page 158.

18. **If you are editing an existing action for the rule**, select an action from the list, click **Edit Action**, and then configure the action. For more information about adding alert actions, see “Adding Alert Actions” on page 158.
19. Use the arrow buttons to set the order in which actions are performed.
Note: Actions are processed in the order they appear, from top to bottom.
20. **If you need to delete an action**, select the action, and then click **Delete Action**.
21. Click **OK** to save all changes and return to Trap Viewer Settings.
22. Use the arrow buttons to arrange the order in which the rules are applied.
Note: Rules are processed in the order they appear, from top to bottom.

Available Trap Alert Actions

The following actions are available for trap alerts. For more information about assigning alert actions, see “Adding Alert Actions” on page 158.

Discard the Trap

Allows you to delete unwanted traps sent to the SNMP Trap server.

Tag the Trap

Allows you to add a custom tag to received traps. Ensure you include the Tag column in the viewer when assigning a tag.

Flag the Trap with a specific color

Allows you to assign a specific color for display in the Orion Web Console and the Trap Viewer to flag traps matching the rule.

Log the Trap to a file

Allows you to specify a file and a series of variables with which to tag traps sent to the file. Ensure you have already created the log file you want to use. The alert cannot create a file.

Windows Event Log

Allows you to write a message to the local Windows Event Log or to a remote Windows Event Log.

Forward the Trap

Allows you to specify the IP address or hostname and the port on which to forward the trap. Specify the IP address or hostname of the trap destination and the port on which the trap should be sent. Check **Include Source Address** to include the IP address of the trap source.

Play a sound

Allows you to play a sound when a matching SNMP trap is received.

Text to Speech output

Allows you to define a specific speech engine, the speed, pitch, volume, and message to read.

Execute an external program

Allows you to specify an external program to launch. This action is used when creating realtime change notifications in Orion NPM.

Execute an external VB Script

Allows you to launch a VB Script using the selected script interpreter engine and a saved script file.

Send a Windows Net Message

Allows you to send a Windows Net message either to a specific computer or to an entire domain or workgroup.

Note: Windows Server 2008 does not support Windows Net Messaging, so this action is not available to Orion installations on Windows Server 2008.

Send an E-mail / Page

Allows you to send an email from a specified account to an address, using a specific SMTP server, and containing a customizable subject and message.

Stop Processing Trap Rules

Stops the processing of SNMP trap rules for the matching trap.

Change the status of an interface

Orion NPM can change the status of the interface from which a trap is received. Designate the status to which the interface should change.

Trap Alert Variables

The following variables can be used in trap alert messages with the Orion NPM Trap Server. You must begin each variable with a dollar sign and enclose each variable identifier in curly braces as, for example, `${VariableName}`.

Note: Trap alerts may also use any valid node variables. For more information about node alert variables, see “Alert Variables and Examples” on page 309.

Trap Date/Time Variables

Trap Date/Time Variable	Description
\$(AbbreviatedDOW)	Current day of the week. Three character abbreviation.
\$(AbbreviatedMonth)	Current month of the year. Three character abbreviation.
\$(AMPM)	AM or PM corresponding to current time (before or after noon)
\$(D)	Current date. (MM/DD/YYYY format)
\$(DD)	Current day of the month (two digit number, zero padded)
\$(Date)	Current date. (MM/DD/YYYY format)
\$(DateTime)	Current day, date and time. (DAY NAME MONTH DD, YYYY HH:MM AM/PM)
\$(Day)	Current date. (MM/DD/YYYY format)
\$(DayOfWeek)	Current day of the week.
\$(DayOfYear)	Numeric day of the year
\$(H)	Current hour. 24-hour format
\$(HH)	Current hour. Two digit format, zero padded.
\$(Hour)	Current hour. 24-hour format
\$(LocalDOW)	Current day of the week. Localized language format.
\$(LongDate)	Current date. (DAY NAME, MONTH DAY, YEAR)
\$(LongTime)	Current Time. (HH:MM:SS AM/PM)
\$(M)	Current numeric month
\$(MM)	Current month. Two digit number, zero padded.
\$(MMM)	Current month. Three character abbreviation.
\$(MMMM)	Full name of the current month
\$(MediumDate)	Current date. (DAY NAME, MONTH DAY, YEAR)
\$(MediumTime)	Current Time. (HH:MM:SS AM/PM)
\$(Minute)	Current minute. Two digit format, zero padded.
\$(MonthName)	Full name of the current month
\$(S)	Date-time to current second (YYYY-MM-DDTHH:MM:SS)
\$(Second)	Current second. Two digit format, zero padded.
\$(Time)	Current Time. (HH:MM AM/PM)
\$(Year)	Four digit year
\$(Year2)	Two digit year

Other Trap Variables

Trap Variable	Description
\$(Application)	SolarWinds application information
\$(Community)	Node community string
\$(Copyright)	Copyright information

Trap Variable	Description
<code>\${DNS}</code>	Fully qualified node name
<code>\${Hostname}</code>	Host name of the device triggering the trap
<code>\${IP}</code>	IP address of device triggering alert
<code>\${IP_Address}</code>	IP address of device triggering alert
<code>\${Message}</code>	Message sent with triggered trap and displayed in Trap Details field of Trap Viewer
<code>\${MessageType}</code>	Name or type of trap triggered
<code>\${Raw}</code>	Raw numerical values for properties sent in the corresponding incoming trap.
<code>\${RawValue}</code>	Raw numerical values for properties sent in the corresponding incoming trap. The same as <code>\${Raw}</code> .
<code>\${vbData1}</code>	Trap variable value pair
<code>\${vbName1}</code>	Trap variable binding name

Chapter 17

Monitoring MIBs with Universal Device Pollers

Using Universal Device Pollers, Orion Network Performance Monitor has the ability to monitor more than just network status, availability, bandwidth, and errors. With Orion Universal Device Pollers, you can monitor virtually any statistic that your network devices can record, including:

- Interface traffic
- CPU temperature
- Addressing errors
- UPS battery status
- Current connections to a website

Universal Device Pollers collect both realtime and historical data associated with object IDs maintained in the extensive SolarWinds MIB database and provided by SolarWinds users. As a result, Universal Device Pollers can retrieve data for nearly any conceivable network metric. Additionally, with Universal Device Poller transforms, you can mathematically manipulate the results of multiple pollers to create your own custom network performance metrics. All network information collected from Universal Device Pollers is easily accessible within the Orion Web Console.

Warning: Universal Device Pollers do not collect information from Hot Standby Engines. If an Orion NPM server fails, data collection stops for any Universal Device Pollers on that server. Any Universal Device Pollers polling that server will be unable to report any information for the failed Orion NPM server, even if it fails-over to an Orion Hot Standby Engine. For more information about Orion Hot Standby Engines, see “Orion Hot Standby Engine” on page 289.

Note: Universal Device Pollers are tied directly to the individual Orion NPM polling engines on which they are hosted. As a result, all Universal Device Pollers assigned to a monitored node that is moved from one Orion NPM polling engine to another must be moved to the new polling engine as well.

Downloading the SolarWinds MIB Database

SolarWinds maintains a MIB database that serves as a repository for the OIDs used to monitor a wide variety of network devices. This MIB database is updated regularly, and, due to its size, it is not included in the initial Orion NPM installation package. If you are either updating your existing MIB database or using the

Universal Device Poller for the first time, you will need to download the SolarWinds MIB database as detailed in the following procedure.

Note: You may need to restart the Universal Device Poller after installing the new MIB database.

To download and install the SolarWinds MIB database:

1. **If you are prompted to download and install the SolarWinds MIB database**, click **Yes**.

Note: This prompt is typically only encountered by first-time users.

2. **If you are using Internet Explorer and it prompts you to add the SolarWinds downloads site** <http://solarwinds.s3.amazonaws.com>, complete the following steps to start the MIB database download:
 - a. Click **Add** on the warning window.
 - b. Click **Add** on the Trusted Sites window, and then click **Close**.
 - c. Refresh your browser.
3. Click **Save** on the File Download window.
4. Navigate to an appropriate file location, and then click **Save**.
5. After the download completes, extract `MIBs.zip` to a temporary location.
6. Open the folder to which you extracted `MIBs.zip`, and then copy `MIBs.cfg` to the SolarWinds folder in either of the following locations on your default install volume, depending on your Orion NPM server operating system:
 - `\Documents and Settings\All Users\Application Data\ON Windows Server 2003 and XP.`
 - `\Documents and Settings\All Users\ProgramData\on Windows Server 2008 and Vista.`

Creating Universal Device Pollers

The following procedure creates and defines a new Universal Device Poller.

To create and define a new universal device poller:

1. Click **Start > All Programs > SolarWinds Orion > Universal Device Poller**.
2. **If you are prompted to download and install the MIB database**, click **Yes**, and then download and install the MIB database. For more information, see “Downloading the SolarWinds MIB Database” on page 235.
3. Click **File > New Universal Device Poller**.

4. **If you know the OID of the object you want to poll**, type it in the **OID** field.
5. **If you do not know the OID of the object you want to poll and you want to browse available MIB object definitions**, complete the following steps:
 - a. Click **Browse MIB Tree**.
 - b. Expand the MIB tree in the left pane to navigate until you locate the object you want to poll.
 - c. Select the object you want to poll, and then click **Select**.

Note: Details describing the selected poller display in the right pane.

6. **If you do not know the OID of the object you want to poll and you want to search available MIB object definitions**, complete the following procedure:

- a. Click **Browse MIB Tree**.
- b. Click **Search MIBs** in the top right corner of the Browse MIBs window.
- c. Select a criterion to **Search By** (**Name**, **Description** keyword, or **OID**).
- d. Provide search strings in the Search field, and then click **Search**.
- e. Select the object you want to poll, and then click **Select**.

Note: The OID Details below the Search fields include a description of the corresponding object and indicate the MIB you are currently searching. If an existing OID exactly matches the OID string provided, details for the matching OID display below the Search field. Searching by name or description returns all OIDs with names or descriptions, respectively, containing the provided search string.

7. **If you want to test the validity of a selected object for a specific node**, select an appropriate test node in the right pane, and then click **Test**.

Note: A green check icon indicates that the selected object was successfully polled for the selected node, returning the indicated value. A yellow warning icon indicates that the test poll was not successful for the reason indicated.

8. **If you tested your poller and it failed**, check the following:
 - Are you using the correct community string for the node that is being polled for the test? For more information about providing community strings, see “Managing Devices in the Web Console” on page 77.
 - Does the selected device support the polled MIB/OID? Refer to device documentation to confirm the MIBs supported by your device.
 - Can your Orion NPM server access the device? Ping the device or use a SolarWinds Toolset application, such as IP Network Browser, to confirm that the device is responding to both ICMP and SNMP requests.

9. Click **Select** when you have located the OID you need.
10. If necessary, edit the provided **Name** for your poller, and then edit the optional **Description**.

Notes:

- A poller name is required. Orion NPM uses this name to refer to your poller throughout the Orion Web Console. Names are recorded without spaces, so any spaces that are included in the name are removed
- The description is optional, but it may be helpful in identifying the type of information collected by your poller.

11. *If you want to change the advanced poller option defaults*, click + next to **Show Advanced Options**, and then complete the following steps:

- a. Select the **MIB Value Type** for the selected poller.

Note: Depending on the type of poller, the poller returns statistics formatted as a **Rate**, a **Counter**, or a **Raw Value**.

- b. *If you selected Rate or Counter as your MIB Value Type*, provide an appropriate **Unit** and **Time Frame**.
- c. *If you selected Raw Value as your MIB Value Type*, select the appropriate **Format** in which the polled raw values should appear.

Note: If you are using the **Enumerated** format, click **Map Values** to provide strings corresponding to the values returned by the poller.

- d. Select the **SNMP Get Type** appropriate for the object you are polling.
- e. Select **Node** or **Interface**, as appropriate for the object you are polling.

12. *If you want to maintain historical data collected by your poller*, select **Yes** for the **Keep Historical Data** option.

Note: SolarWinds recommends that you keep historical data to take full advantage of the data display features present in Orion NPM. Select **Yes** if you want to display collected poller data in charts and gauges within the Orion Web Console.

13. *If you want the poller to begin polling immediately upon configuration*, confirm that **Enabled** is selected as the poller **Status**.

Note: If you select **Disabled**, the poller will not collect statistics until you enable the poller.

14. In the **Group** field, either select an existing group or provide a new group name to aid in organizing your pollers, and then click **Next**.

15. Click **+** to expand the node tree as necessary, and then check all the nodes to which you want to apply your new poller.

Note: Available groups are listed in the **Group By** field. Select a group to selectively limit number of nodes listed in the node tree.

16. ***If you want to see the current results for your poller on the nodes you have checked***, click **Test**.

Note: A green check icon indicates that the poller successfully polled the selected node, returning the indicated value. A yellow warning icon indicates that the test poll was not successful for the reason indicated.

17. ***If you tested your poller and it failed***, check the following:

- Are you using the correct community string for the node that is being polled for the test? For more information about providing community strings, see “Managing Devices in the Web Console” on page 77.
- Does the device support the MIB/OID that is being polled? Refer to the documentation supplied by the device vendor to confirm the MIBs supported by your device.
- Can you access the device from the Orion Network Performance Monitor server? Ping the device to see if it responds or use a SolarWinds Toolset application, such as IP Network Browser, to confirm that the device is responding to both ICMP and SNMP requests.

18. Click **Next**.

19. ***If you want to display poller results in Orion Web Console views***, confirm that **Yes** is selected, and then, for each available Orion NPM view, check the types of poller results resources, if any, that you want to display.

Note: Click **Preview** to see how your poller resource will display in the selected Orion Web Console view.

20. ***If you only want to display the poller results resource in the event that the poller returns valid results***, check **Do not show this poller if it is not assigned**.

21. Click **Finish**.

Assigning Pollers to Nodes or Interfaces

In addition to the Universal Device Pollers that you create, Orion NPM is packaged with a few predefined example pollers. To use any of these pollers you need to assign the poller to a network device, and then enable the poller.

Note: For more information about creating your own Universal Device Pollers, see “Creating Universal Device Pollers” on page 236.

To enable and assign a poller to nodes or interfaces:

1. Click **Start > All Programs > SolarWinds Orion > Universal Device Poller**.
2. Click **File > Assign Pollers**.
3. Click **+**, as necessary, to expand the poller tree, and then check the pollers you want to assign.

Notes:

- By default, Orion NPM provides two poller groups: Example and Default Group. The Example group contains all predefined Orion NPM pollers, and Default Group is the group that contains all user-defined Universal Device Pollers if they are not assigned to any other group.
 - Checking a poller group automatically checks all pollers in the group. If you do not want to assign a specific poller in a checked group, click **+** next to the poller group name, and then uncheck the specific pollers that you do not want to assign.
 - If you need to assign multiple pollers either to a single node or to a group of nodes, check all the pollers you want to apply on this view. These pollers are assigned to nodes in the next step.
4. After you have checked all the pollers you want to assign, click **Next**.
 5. Click **+** to expand the node tree down to the interface level, if necessary, and then check the elements to which you want to apply the selected pollers.

Notes:

- Available groups are listed in the **Group By** field. Select a group to selectively limit the node tree.
- When assigning an interface poller, checking a node automatically assigns the selected poller to all interfaces on the checked node. If you do not want to apply the poller to a specific interface on any parent node, click **+** next to the parent node, and then uncheck the specific interfaces to which the poller should not be assigned.
- Interfaces are not displayed unless you are assigning an interface poller.

6. If you want to see the current results of the selected pollers on the nodes and interfaces you have checked, click Test.

Note: A green check icon indicates that the poller successfully polled the selected node, returning the indicated value. A yellow warning icon indicates that the test poll was not successful for the reason indicated.

7. If you tested your poller and it failed, check the following:

- Are you using the correct community string for the node that is being polled for the test? For more information about providing community strings, see “Managing Devices in the Web Console” on page 77.
- Does the device support the MIB/OID that is being polled? Refer to the documentation supplied by the device vendor to confirm the MIBs supported by your device.
- Can you access the device from the Orion Network Performance Monitor server? Ping the device to see if it responds or use a SolarWinds Toolset application, such as IP Network Browser, to confirm that the device is responding to both ICMP and SNMP requests.

8. Once you have completed your poller assignments, click Finish.

Disabling Assigned Pollers

By default, as soon as a poller is assigned, it collects statistics on the selected elements to which it is assigned. If you want to suspend data collection for a poller without deleting it, complete the following procedure to disable the poller.

Note: To disable multiple pollers, repeat the following procedure for each poller you want to disable.

To temporarily disable a Universal Device Poller:

1. Click **Start > All Programs > SolarWinds Orion > Universal Device Poller**.
2. In the All Defined Pollers pane of the Orion Universal Device Poller window, click **+**, as necessary, to expand the poller tree, and then click the poller you want to disable.
3. Confirm you have selected the poller you want to disable by viewing the poller properties in the main Orion Universal Device Poller window. Click **Show all Properties** in the lower left of the main window to show more details, if necessary.
4. Click **Edit Properties** in the top right of the main window.
5. Set **Status** to **Disabled**, and then click **Finish**.

Duplicating an Existing Poller

Existing pollers are easily duplicated in Orion NPM. The following procedure provides the required steps to duplicate an existing poller.

To duplicate an existing poller in Orion NPM:

1. Click **Start > All Programs > SolarWinds Orion > Universal Device Poller**.
2. In the All Defined Pollers pane of the Orion Universal Device Poller window, click **+**, as necessary, to expand the poller tree, and then click the poller you want to duplicate.
3. Confirm that you have selected the poller you want to duplicate by viewing the poller properties in the main Orion Universal Device Poller window.
4. Click **Show all Properties** in the lower left of the main window to show more details, if necessary.
5. Right-click the name of the poller you want to duplicate, and then select **Duplicate Poller**.
6. Change the **Name** of the duplicate poller, and then edit the definition of the duplicate poller, as necessary, in the same way that you would create a new Universal Device Poller. For more information about creating a Universal Device Poller, see “Creating Universal Device Pollers” on page 236.

Importing MIB Pollers

Orion NPM provides the ability to import custom pollers both from previous Orion NPM versions and from Universal Device Pollers. Though you cannot import MIBs directly into the SolarWinds MIB Database, the import mechanism does allow you to import the association between a MIB and a Universal Device Poller. The poller can then be associated with a device in your environment. Use the following procedure to import a Universal Device Poller.

To import a Universal Device Poller:

1. Click **Start > All Programs > SolarWinds Orion > Universal Device Poller**.
2. Click **File > Import Universal Device Pollers**.
3. For each poller you want to import, complete the following steps:
 - a. Click **Open**, and then navigate to the location of the poller to import.
 - b. Select the poller to import, and then click **Open**.
4. Select the pollers to import from the list on the left, and then click **Import**.

5. **If you want to remove a selected poller from the list of pollers to import**, click the poller to remove, and then click **Remove**.

Notes:

- To select multiple pollers, hold down **SHIFT** or **CTRL**, and then click the pollers you want.
- To collapse all folders and see just the group names, hold down **SHIFT**, and then click - next to any of the group names.

6. Click **OK**.

7. **If you want the imported poller to begin polling immediately upon assigning network devices**, complete the following steps:

- a. Select your new, imported poller in the All Defined Pollers pane on the left of the Orion Universal Device Poller window.
- b. Click **Edit Properties**.
- c. Confirm that **Enabled** is selected as the poller **Status**,

8. **If you do not want the poller to begin polling immediately upon assigning network devices**, complete the following steps:

- a. Select your new, imported poller in the All Defined Pollers pane on the left of the Orion Universal Device Poller window.
- b. Click **Edit Properties**.
- c. Select **Disabled** as the poller **Status**,

Note: If **Disabled**, the poller will not collect data until you enable the poller.

9. Assign nodes or interfaces to the imported poller. For more information, see “Assigning Pollers to Nodes or Interfaces” on page 240.

As soon as the imported poller has been enabled and assigned to appropriate network devices, the poller begins collecting statistics. To view these statistics, log in to the Orion Network Performance Monitor Web Console and browse to a node or interface that was just assigned to the poller. For more information, see “Viewing Universal Device Poller Statistics” on page 249.

Exporting Universal Device Pollers

Orion NPM provides the ability to export Universal Device Pollers you have created using the following procedure.

To export a Universal Device Poller:

1. Click **Start > All Programs > SolarWinds Orion > Universal Device Poller**.
2. Click **File > Export Universal Device Pollers**.

- In the Pollers pane on the left, click **+**, as necessary, to expand the poller tree, and then select the pollers you want to export.

Note: Selecting a group name selects all pollers in the group, and multiple pollers may be selected using `Shift+click` and `Ctrl+Click`.

- If you have selected all the pollers you want to export, click **Export**.
- If you want to remove a selected poller from the list of pollers to export, click the poller to remove, and then click **Remove**.

Note: Selecting a group name selects all pollers in the group, and multiple pollers may be selected using `Shift+click` and `Ctrl+Click`.

- Click **Save**.
- Navigate to the location where you want to export the selected pollers, provide a **File name**, and then click **Save**.

Transforming Poller Results

Often, the results provided by a MIB poller are more easily understood after they have been manipulated with a simple mathematical calculation. For example, though a poller may return temperature values in Celsius, it may be easier to work with the poller results if they are presented in Fahrenheit. The following sections detail both currently available poller transformations and the creation of new poller transformations.

Available Poller Transformations

Orion NPM provides a number of predefined transformation functions that may be applied to one or more pollers to generate mathematically manipulated poller results. The following table lists transformation functions that are currently available with the Universal Device Poller in Orion NPM:

Poller Transformation	Definition
Average	Provides an average of the results of multiple pollers
Minimum	Provides the minimum of multiple poller results
Maximum	Provides the maximum of multiple poller results
Truncate	Truncates a polled value to a designated number of decimal places; e.g. <code>Truncate({HiPrecision}, 4)</code> truncates the result of the poller named <code>HiPrecision</code> to four decimal places.
ColumnAverage	Provides an average of the column values in a polled table
ColumnMinimum	Gives the minimum of a column of values in a polled table
ColumnMaximum	Gives the maximum of a column of values in a polled table
ColumnSum	Provides the sum of a column of values in a polled table
Temperature > Celsius to Fahrenheit	Provides the Fahrenheit equivalent of a poller result originally presented in Celsius

Poller Transformation	Definition
Temperature > Fahrenheit to Celsius	Provides the Celsius equivalent of a poller result originally presented in Fahrenheit
X to Kilobyte	Provides the number of Kilobytes equivalent to a poller result originally presented in Bytes
X to Megabyte	Provides the number of Megabytes equivalent to a poller result originally presented in Bytes
X to Gigabyte	Provides the number of Gigabytes equivalent to a poller result originally presented in Bytes
X to Terabyte	Provides the number of Terabyte s equivalent to a poller result originally presented in Bytes
Kilobyte to Megabyte	Provides the number of Megabytes equivalent to a poller result originally presented in Kilobytes
Kilobyte to Gigabyte	Provides the number of Gigabytes equivalent to a poller result originally presented in Kilobytes
Kilobyte to Terabyte	Provides the number of Terabytes equivalent to a poller result originally presented in Kilobytes
Megabyte to Gigabyte	Provides the number of Gigabytes equivalent to a poller result originally presented in Megabytes
Megabyte to Terabyte	Provides the number of Terabytes equivalent to a poller result originally presented in Megabytes
Gigabyte to Terabyte	Provides the number of Terabytes equivalent to a poller result originally presented in Gigabytes

Creating a Poller Transformation

The following procedure provides the steps required to develop powerful poller transformations with Universal Device Pollers.

To transform poller results:

1. Click **Start > All Programs > SolarWinds Orion > Universal Device Poller**.
2. Click **File > Transform Results**.
3. Click **Next** on the page of example poller transformations.
4. Type a transformation **Name**, and then provide an optional **Description**.

Notes:

- A transformation name is required. Orion NPM uses this name to refer to your defined poller transformation throughout the Orion Web Console.
- Names are recorded without spaces, so any included spaces in the name are removed.
- The description is optional, but it may be helpful in identifying the type of information generated by your poller transformation.

5. **If you want to maintain historical data generated by your poller transformation**, select **Yes** for the **Keep Historical Data** option.

Note: SolarWinds recommends that you keep historical data to take full advantage of the data display features present in Orion NPM. Select **Yes** if you want to display transformed poller data in charts and gauges within the Orion Web Console.

6. **If you want your poller transformation to begin calculating transformed results immediately upon configuration**, confirm that **Enabled** is selected as the poller transformation **Status**.

Note: If you select **Disabled**, the poller will not transform poller statistics until you enable the poller transformation.

7. In the **Group** field, either select an existing group or provide a new group name to aid in organizing your poller transformations.
8. Click **Next**.
9. Provide the mathematical definition of your poller transformation in the **Formula** field, as shown in the following steps:
- Click **Add Function**, and then
 - Select the function you want to apply to one or more pollers.
 - Click within the function parentheses.
 - Click **Add Poller**, and then select a poller to transform.

Notes:

- Repeat for each additional poller you want to add to the transformation formula.
- Separate pollers with commas, as shown in the following example that averages the results of three pollers:

```
avg({poller1},{poller2},{poller3})
```

- Standard mathematical operations, as shown in the following example, are also valid as formulas:

```
{poller1}+{poller2}
```

- Poller transformation formulas are also nestable, as shown in the following example that returns the average of two poller comparisons:

```
avg(min({poller1},{poller2}),max({poller3},{poller4}))
```

10. If you want to test the validity of a selected poller transformation formula for a specific node, use the available criteria to select a device to test, and then click **Test**.

Note: Test results for each poller in the formula display with the result of the defined poller transformation.

11. If you tested your poller transformation and it failed, check the following:

- Is your transformation formula syntactically correct? Ensure that all braces and parentheses are balanced, that there are no unnecessary spaces, and that all pollers return the same type of values.
- Are you using the correct community string for the node that is being polled for the test? For more information about providing community strings, see “Managing Devices in the Web Console” on page 77.
- Does the device support the polled MIB/OID? Refer to documentation supplied by the device vendor to confirm supported MIBs for your device.
- Can you access the device from the Orion Network Performance Monitor server? Ping the device to see if it responds or use a SolarWinds Toolset application such as IP Network Browser to confirm that the device is responding to both ICMP and SNMP requests.

12. Click Next.

13. Click + to expand the node tree down to the interface level, if necessary, and then check all the monitored devices to which you want to apply your defined poller transformation.

Notes:

- Available groups are listed in the **Group By** field. Select a group to selectively limit the node tree.
- Interfaces are not displayed unless your poller transformation operates on a defined interface poller.
- When assigning an interface poller transformation, checking a node automatically assigns the selected transformation to all interfaces on the checked node. If you do not want to apply the poller transformation to a specific interface on any parent node, click **+** next to the parent node, and then uncheck the specific interfaces to which the transformation should not be assigned.

14. If you want to see the current results of the selected pollers on the nodes and interfaces you have checked, click Test.

Notes:

- A green check icon indicates a valid poller transformation, and the transformation result is displayed.
- A yellow warning icon indicates that the poller transformation was not successful for the reason indicated.

15. If you tested your poller and it failed, check the following:

- Is your transformation formula syntactically correct? Ensure that all braces and parentheses are balanced, that there are no unnecessary spaces, and that all pollers return the same type of values.
- Are you using the correct community string for the node that is being polled for the test? For more information about providing community strings, see “Managing Devices in the Web Console” on page 77.
- Does the device support the polled MIB/OID? Refer to documentation supplied by the device vendor to confirm supported MIBs for your device.
- Can you access the device from the Orion Network Performance Monitor server? Ping the device to see if it responds or use a SolarWinds Toolset application such as IP Network Browser to confirm that the device is responding to both ICMP and SNMP requests.

16. Click Next.

17. If you want to display poller results in Orion Web Console views, confirm that **Yes** is selected, and then, for each available view, check the types of poller results resources, if any, that you want to display.

Note: Click **Preview** to see how your poller resource will display in the selected web console view.

18. If you only want to display the poller results resource in the event that the poller transformation returns valid results, check Do not show this poller if it is not assigned.

19. Click Finish.

Viewing Universal Device Poller Statistics

Once you have configured and enabled a Universal Device Poller, you can view the statistics that it records on any view within the Orion Web Console. The following procedure includes poller resources in Orion Web Console views.

To add poller resources to web console views:

1. Click **Start > All Programs > SolarWinds Orion > Universal Device Poller**.
2. In the All Defined Pollers pane of the Orion Universal Device Poller window, click **+**, as necessary, to expand the poller tree, and then click the poller you want to add as a web console resource.
3. Confirm that you have selected the poller you want to duplicate by viewing the poller properties in the main Orion Universal Device Poller window.
4. Right-click the poller to add as a resource, and then click **Web Display**.
5. Confirm that **Yes** is selected, and then, for each available Orion NPM view, check the types of poller resources that you want to display.

Note: Click **Preview** to see how your poller resource will display in the selected Orion Web Console view.

6. *If you only want to display the poller resource when the poller returns valid results*, check **Do not show this poller if it is not assigned**.
7. Click **Finish**.

Creating Alerts for Universal Device Pollers

Alerts for Universal Device Pollers are configured using the Advanced Alert Manager. For more information, see “Configuring Advanced Alerts” on page 145.

Notes:

- In some cases, the table name may be required for variables used in Universal Device Poller alerts, as in `${CustomPollers.Description}`.
- When creating a new alert for a Universal Device Poller, on the Trigger Condition tab, change the alert type to **Node Poller** or **Interface Poller**, as appropriate.

Chapter 18

Creating Custom Properties

Orion Network Performance Monitor features the Custom Property Editor, which allows you to add a custom property to any interface, node, or volume. Custom properties are additional fields, such as *country*, *building*, *asset tag*, or *serial number*, that you can define and store in your Orion NPM database. After properties are added, they are available for display and filtering both within the Orion Web Console and within the Report Writer application. A few more examples of how custom properties may be used are as follows:

- Add information to nodes, such as contact, owner, or support contract.
- Add a name property to nodes and then configure an alert to e-mail a server named by the property. For more information on changing custom property values with an alert, see “Changing a Custom Property” on page 173.
- Add a custom property that is used as an account limitation on nodes.
- Add a custom property to nodes for grouping them on the web or in a report.
- Add a custom property to interfaces to display a custom description.
- Add a custom property and display it as an annotation on a chart.

Custom Property Editor lets you choose from a provided collection of the most commonly used properties, or you can easily and efficiently build your own custom properties. For more information, see “Creating a Custom Property” on page 251. Once your custom property is defined, the Import Wizard allows you to populate your new property from either a text- or comma-delimited file. For more information, see “Importing Custom Property Data” on page 255. Alternatively, if you only have a few individual changes or additions, you may choose to make those changes using the Edit view. For more information, see “Editing Custom Properties” on page 253.

Creating a Custom Property

The following procedures present an introduction to the startup, function and features of Custom Property Editor.

To create a property with Custom Property Editor:

1. Click **Start > All Programs > SolarWinds Orion > Grouping and Access Control > Custom Property Editor**.
2. Click **Add Custom Property**.

3. **If you want to add predefined properties**, complete the following procedure:
 - a. Select **Add Predefined Properties**.
 - b. Check **Show Advanced Properties** to view additional predefined properties.
 - c. Check the properties you want to add, and then click **OK**.
4. **If you want to generate a completely new custom property**, complete the following procedure:
 - a. Select **Build a Custom Property from scratch**.
 - b. Select the Orion NPM database table to which you want to add the new custom property.
 - c. Provide the new **Property Name**.

Notes:

- To ensure full custom property functionality, do not leave the **Property Name** field empty.
- Although most non-alphanumeric characters used in custom property names are replaced by underscores (_) when names are stored in the Orion database, SolarWinds recommends against using non-alphanumeric characters in custom property names. Hash characters (#) are not allowed in any property name.

- d. Select the **Property Type**.
- e. Enter a **Max. Text length**.

Note: Regardless of the value provided in this field, Orion NPM does not support custom properties defined with more than 4000 characters.

- f. Click **OK**.

Removing a Custom Property

Custom properties are easily removed using the Custom Property Editor, as shown in the following procedure.

To remove a custom property:

1. Click **Start > All Programs > SolarWinds Orion > Grouping and Access Control > Custom Property Editor**.
2. Click **Properties > Remove Custom Properties**.

3. Check each property you want to remove.
4. **If you are satisfied with your selections**, click **OK**.

Editing Custom Properties

The Custom Property Editor allows you to easily modify custom properties.

To edit a custom property:

1. Click **Start > All Programs > SolarWinds Orion > Grouping and Access Control > Custom Property Editor**.
2. Click **Properties > Edit Object Properties**, where *Object* is **Node**, **Interface**, or **Volume**, as appropriate.
3. Click the cells in the table that you want to edit, and then enter or modify the cell contents, as necessary.
4. **If you want to create or edit a filter for your custom properties**, click **No Active Filter** or **Filter Active**, and then define the filter that you want to apply. For more information, see “Using Filters in Edit View” on page 253.
5. **If you are satisfied with your edits**, click **OK**.

Using Filters in Edit View

Filtering is available in the Edit Custom Properties windows for all devices, and you can apply filters to manipulate available data views. Custom Property Editor allows you to edit the text within custom property fields to which a filter is applied. The following procedures show how to use filters within Custom Property Editor.

Creating Custom Properties Filters

The following procedure creates a custom properties filter.

To create a filter:

1. Click **Start > All Programs > SolarWinds Orion > Grouping and Access Control > Custom Property Editor**.
2. Click **Properties > Edit Object Properties**, where *Object* is **Node**, **Interface**, or **Volume**, as appropriate.
3. Click **Filter Active** or **No Active Filter**, and then click **Apply Filter**.
Note: The text of the **Filter Active** / **No Active Filter** button changes dynamically, indicating the filter status for the currently viewed data.
4. Click the hyperlinked text to select the appropriate criteria.

5. Click the ellipsis, and then select from the following options:

Note: The lists of available linked descriptors are dynamically generated in consideration of all other variables within the same condition. For more information, see “Understanding Condition Groups” on page 153. Click **Browse (...)** to select a condition type.

- Select **Add a new elementary condition** to generate a condition that is based on a direct comparison of network object data fields.
 - Select **Add a new advanced elementary condition** to generate a condition based on a comparison of device data fields and values.
 - Select **Add a new complex condition** to define a condition that filters other defined conditions.
 - Select **Delete current condition** to remove a selected condition.
 - Select **Move current condition forward** or **Move current condition backward** to change the order of your conditions accordingly.
6. Continue to click hyperlinked text and use the cascading menus to select filtering criteria.
 7. **If you have completed the configuration of your filter**, click **OK**.

Note: The Edit *Object* Properties view changes, based upon the selected filter, and the text of the **Filter Active / No Active Filter** now displays “Filter Active”, indicating that the filter is being applied to the currently viewed properties.

Removing Custom Properties Filters

The following procedure removes a custom properties filter.

To remove a filter:

1. Click **Start > All Programs > SolarWinds Orion > Grouping and Access Control > Custom Property Editor**.
2. Click **Properties > Edit *Object* Properties**, where *Object* is **Node**, **Interface**, or **Volume**, as appropriate.
3. Click **Filter Active**, and then click **Remove Filter**.

Note: The Edit *Object* Properties view now displays all custom properties.

Importing Custom Property Data

Once you have defined custom properties, the Custom Property Editor Import tool assists in populating the custom property data. For example, you may already possess a spreadsheet listing the asset tags of all your network nodes, and you would like to have this information available for reporting and publication in the web console. In this scenario, Asset Tag is added as a custom property, and then the import wizard is used to populate the asset tag values from the spreadsheet. The following steps outline the process for importing custom properties data. For more information, see “Creating Custom Properties” on page 251.

To import custom property data:

1. Click **Start > All Programs > SolarWinds Orion > Grouping and Access Control > Custom Property Editor**.
2. Click **File > Import**, and then select **Import from Comma Delimited File** or **Import from Text File** as appropriate.
3. Navigate to the file that contains your custom property data.
4. Select the file that contains your custom property data, and then click **Open**.
5. Select the delimiter that separates the data in your file.
6. **If your data file contains a header row**, check **First row contains field names**.
7. Specify the characters that may surround text fields in your file.
8. Click **Next**.
9. Select the data table that has the custom properties into which you want to import your data.
10. Click **Next**.
11. Use the drop down menus to select the key field from your file on the left and the corresponding field of the table on the right.
Note: Depending on your file data, you may need to specify multiple key fields so that the import wizard properly matches your data to the table fields.
12. Click **Next**.
13. Specify the fields from your file on the left that you want to import by clicking corresponding blank cell on the right, and then select the target field that you want your data field to populate.

Note: Click the cell to enable a menu. Use the menu items to select the target NPM field that you want your data to populate.

14. **If you have specified all cell matches between your data and the Orion NPM database**, click **Import**.
15. **If your import is successful**, confirm the count of successfully imported rows, and then click **OK**.

Custom Property Editor Settings

The Custom Property Editor Settings window allows you to customize the display for nodes, interfaces, and volumes.

To configure Custom Property Editor settings:

1. Click **Start > All Programs > SolarWinds Orion > Grouping and Access Control > Custom Property Editor**.
2. Click **File > Settings**.
3. Click Node Editing and check the system properties you want to see in the Edit Node Properties window. Repeat for Interface and Volume Editing.
4. **If you want to enable Auto-Search**, click Auto-Search, and then check **Enable Auto-Search**.

Note: With Auto-Search enabled, the current column is searched as you type. Select a cell and then press `Enter` to edit its contents. With Auto-Search disabled, typing will begin editing the cell.

Chapter 19

Creating Account Limitations

The Account Limitation Builder application allows you to create and customize account limitations for the Orion Web Console. These limitations ensure that users of the web console can only view the nodes and interfaces that are pertinent to their job duties. The following are but a few examples of the uses of account limitation in the Orion Web Console:

- Limit customer views to specific network nodes
- Limit views by department or functional area
- Limit views by device type or device role
- Limit views based on the geographic location of devices

Orion NPM provides predefined account limitations that use built-in Orion NPM property to limit user access. For greater flexibility, however, you can use the Account Limitation Builder to create your own account limitations based on predefined or custom properties.

For more information about enabling account limitations in the Orion Web Console, see “Setting Account Limitations” on page 93. For more information about custom properties, see “Creating Custom Properties” on page 251.

Using the Account Limitation Builder

Before you can use the Account Limitation Builder, you must have first created the custom property that you want to use to limit the Orion Network Performance Monitor Web Console view. For more information, see “Creating Custom Properties” on page 251. After you have defined custom properties and populated them with data, you may use the Account Limitations Builder as directed in the following procedure.

Creating an Account Limitation

The following steps create an account limitation.

To create an account limitation:

1. Click **Start > All Programs > SolarWinds Orion > Grouping and Access Control > Account Limitation Builder**.
2. Click **Start** on the splash screen.
3. Click **Edit > Add Limitation**.

4. Select a **Custom Property**.

Notes:

- If **Custom Property** is empty, you need to define a custom property. For more information, see “Creating Custom Properties” on page 251.
- The remaining boxes are populated automatically, based upon your selection.

5. Choose a **Selection Method**.

Note: This is the selection format that will appear when you are choosing values for the account limitation through the web Account Manager. For more information, see “Setting Account Limitations” on page 93.

6. If you want to include your own description of your account limitation, type your description over the default text provided in the **Description** field.
7. Click **OK**.

Your newly defined account limitation is added to the top of the table view. You may now use the new limitation in the Orion Web Console Account Manager. For more information, see “Setting Account Limitations” on page 93.

Deleting an Account Limitation

The following steps delete an account limitation using the Account Limitation Builder utility.

To delete an account limitation:

1. Click **Start > All Programs > SolarWinds Orion > Grouping and Access Control > Account Limitation Builder**.
2. Click **Start** on the splash screen.
3. Click the row of the limitation that you want to delete.

Note: Use **Shift+click** to highlight multiple consecutive rows or **Ctrl+Click** to highlight multiple non-consecutive rows.

4. Click **Edit > Delete Selected Limitations**.

Note: Although Orion NPM deletes the selected limitations from the table, ensuring that they will no longer be available through the web Account Manager, if you delete a limitation using the Account Limitation Builder, all accounts that have been assigned that limitation will remain limited. Deleting a limitation simply makes it unavailable for future use in the Orion Web Console.

Chapter 20

Using Orion System Manager

Orion System Manager provides a limited ability to configure, customize, and manage Orion NPM. Though the Orion Web Console is the primary Orion interface, Orion System Manager can display data and statistics that are collected by the Network Performance Monitor Service and stored in a SQL database in accordance with the configurations that you have set in the Orion Web Console. Specifically, Orion System Manager allows you to add and delete nodes and add new elements to your network monitoring profile. As a result, System Manager can be used to view much of the same information about nodes and interfaces that is available in the Orion Web Console.

Starting System Manager

System Manager is the administrative interface for the Orion Network Performance Monitor Service. It can be used to add devices and establish custom alerts.

To start System Manager:

1. Click **Start > All Programs > SolarWinds Orion > System Manager**.
2. *If System Manager detects multiple Orion polling engines*, select the server you want to manage.
3. Click **Connect to Polling Engine**.

Finding Nodes in the Node Tree

When monitoring a large number of nodes it can be difficult to find specific nodes. Use the following procedure to quickly find individual nodes.

To find individual nodes:

1. Click **Nodes > Find Node**.
2. Select a **Lookup Field**.
3. Select a **Lookup Criteria**.

Note: Nodes that match your criteria appear in the **Found Nodes** field.

Grouping Nodes in the Node Tree

When monitoring a large number of nodes it can become difficult to quickly find specific nodes, but defining node groups can help. The following procedure groups nodes into a collapsible tree structure.

To group nodes in the node tree:

1. Click **Nodes > Refresh Node Tree**.
2. Select a criterion for node grouping from the menu above the Node Tree.

Note: You can also create custom properties for defining node groups. For more information, see “Creating Custom Properties” on page 251.

Viewing Network Details

Orion NPM provides a broad range of options for viewing tables of the network data and statistics that it collects. There are over 20 predefined views, and you can customize as many other views as you need. You can rearrange the columns by dragging column headings left or right to the position you want. Clicking in the column header will make the data in that column the sort-order basis for all displayed data. Clicking in the column header again reverses the order. The following procedure generates predefined and custom views of data and statistics for your network.

To view network details:

1. **If you want to generate a predefined view**, click **View > Display View**, and then select the network view that you want to see.
2. **If you want to generate a custom view**, complete the following procedure:
 - a. Click **View > New View**.
 - b. Enter a name for your custom view in the **View name** field.
 - c. Select the items that you would like to view, and then click **OK**.

Network Performance Monitor Settings

Network Performance Monitor Settings specify how Orion NPM presents network data and statistics within System Manager. The following aspects of System Manager are configured from the Network Performance Monitor Settings window:

- Chart properties
- Node Tree properties

The following sections provide procedures to configure System Manager chart and node tree settings.

Charts Settings

Settings on the Charts tab affect the appearance of printed charts. The following steps configure settings for charts in Orion NPM.

To configure chart settings:

1. Click **File > Orion Network Performance Monitor Settings**.
2. Click **Charts** to view chart settings.
3. Select **Color** or **Monochrome with symbols** in the **Print Charts in** area.
Note: If you are printing to a monochrome printer, instead of converting each chart to black and white with symbols before printing, you can select **Monochrome with symbols** and System Manager will convert the charts to black and white each time one is printed.
4. Select **Large**, **Medium**, or **Small** in the **Default Font Size** area.
Note: Default font size is adjusted globally. System Manager will also dynamically adjust the font size for each chart as the chart window is resized.
5. Select **Enable Auto-Refresh** or **Disable Auto-Refresh**.
Note: Performance charts can refresh automatically. This setting affects the display of charts in System Manager only and not in the Orion Web Console.
6. *If you have selected **Enable Auto-Refresh***, set the refresh frequency with the slider.

Node Tree Settings

System Manager displays the Node Tree as a representation of all monitored resources in your network. Each resource in your network is identified with either a Type icon or a Status icon. On the Node Tree tab you can select the kind of icons that the Node Tree uses to represent your network nodes, interfaces, and volumes, as shown in the following procedure.

To select Node Tree icons:

1. Click **File > Orion Network Performance Monitor Settings**.
2. Click **Node Tree** to view the Node Tree icon settings.
3. Select **Display Machine Type Icons** or **Display Node Status Icons** in the **Network Nodes** area.
4. Select **Display Type Icons** or **Display Status Icons** in the **Interfaces and Volumes** area.

Creating XML Snapshots

Orion System Manager provides the option of periodically generating XML files including network data collected by Orion NPM. These XML Snapshots may then be used by other programs, most commonly web applications, for the purpose of displaying information about your network. The following procedure generates an XML Snapshot of the current condition of your network.

Notes:

- XML Snapshot generation is a CPU-intensive activity. Leave this option checked only as long as you actually want to create XML Snapshots.
- Snapshots are saved in the same folder as `OrionNetPerfMon.exe`, by default: `<volume:>\Program Files\Solarwinds\Orion`. The file name used is `NetPerfMon-NetObjects.Snapshot`.

To create XML Snapshots:

1. Click **Start > All Programs > SolarWinds Orion > System Manager**.
2. Click **File > Advanced Settings**.
3. Click the XML Snapshots tab.
4. Check **Generate XML Snapshots**.
5. Click **Yes** to confirm your selection to enable XML Snapshot generation.
6. Use the slider to set an appropriate interval for generating your XML Snapshots, and then click **OK**.

Viewing Alerts in System Manager

Although the Alerts view in the Orion Web Console is more flexible, it is possible to view both basic and advanced alerts in Orion System Manager.

To view alerts in Orion System Manager:

1. Click **Start > All Programs > SolarWinds Orion > System Manager**.
2. Click **Alerts** in the toolbar.
3. **If you want to view advanced alerts**, click **Advanced Alerts** in the Active Alerts window. For more information, see “Viewing Advanced Alerts” on page 263.
4. **If you want to view basic alerts**, click **Basic Alerts** in the Active Alerts window. For more information, see “Viewing Basic Alerts” on page 263.

Viewing Basic Alerts in System Manager

Orion provides basic alerts as a limited way to create alerts for simple network conditions. For more information about configuring basic alerts, see “Configuring Basic Alerts” on page 135.

To view basic alerts in Orion System Manager:

1. Click **Start > All Programs > SolarWinds Orion > System Manager**.
2. Click **Alerts** in the toolbar.
3. Click **Basic Alerts** in the Active Alerts window.
4. *If you want to globally disable alert actions as you acknowledge alerts*, check **Temporarily Disable all Actions for All Basic Alerts** to the left, above the alert list.
5. Select the alert sorting criterion from the **Group By** menu to the right, above the alert list.

Currently active basic alerts are listed on the Basic Alerts tab of the Active Alerts window. Expand any listed alert to review the following information:

Note: Click **Refresh** above the Basic and Advanced Alerts tabs to update all listed alert information.

- The **Alert Time** field provides the date and time the alert was triggered.
- The **Network Object** field provides the local network name of the device that triggered the viewed alert.
- **Current Value** provides the value of the object property monitored to trigger the listed alert.
- The **Message** field provides the message configured to describe the condition triggering the listed alert.

Viewing Advanced Alerts in System Manager

Advanced alerts provide a more powerful way to create alert notifications for an unlimited variety of conditional network events.. For more information about configuring advanced alerts, see “Creating and Configuring Advanced Alerts” on page 145.

To view advanced alerts in Orion System Manager:

1. Click **Start > All Programs > SolarWinds Orion > System Manager**.
2. Click **Alerts** in the toolbar.
3. Click **Advanced Alerts** in the Active Alerts window.

4. **If you want to globally disable alert actions as you acknowledge alerts**, check **Disable all Actions for All Advanced Alerts** to the left, above the alert list.
5. Select the alert sorting criterion from the **Group By** menu to the right, above the alert list.

Currently active advanced alerts are listed on the Advanced Alerts tab of the Active Alerts window. Expand any alert to review the following information:

Note: Click **Refresh** above the Basic and Advanced Alerts tabs to update all listed alert information.

- An **Acknowledged** checkbox allows you to acknowledge alert receipt.
- The **Alert Name** is stated again.
- The **Alert State** value and icon are translated as indicated in the following table.

Alert State Value	Alert State Name	Alert State Description
1	Trigger Pending	Conditions triggering an alert exist, but they have not existed for the full period of an applied delay condition.
2	Triggered	Conditions triggering an alert exist, and they have existed for the full period of any applied delay condition.
3	Reset Pending	Conditions triggering an alert reset exist, but they have not existed for the full period of an applied delay condition.
4	Reset	Conditions triggering an alert reset exist, and they have existed for the full period of any applied delay condition.

- The **Object Name** is the local network name of the device that triggered the viewed alert.
- The **Triggered Time** field provides the date and time the alert was triggered.
- If the alert has been acknowledged, the **Acknowledged By** field indicates the name and logged-in location of the acknowledging user.
- The **Acknowledge Time** field provides the date and time the viewed alert was acknowledged.
- Click **X** in the **Clear** field to remove the viewed alert from the current view.

Viewing Charts

System Manager provides substantial means for viewing information about your network. Expanding the Node Tree in the left pane of the System Manager reveals a number of charts for viewing statistics about Nodes and Interfaces. These charts can dynamically redraw themselves as the windows containing them are resized, and their scales adjust for maximum readability and detail.

You can analyze a chart in more detail by drawing a bounding box around an area of interest, effectively “zooming in” on the selected area. When you drill into a chart, you must begin dragging with your cursor within the bounds of the graph itself. When you zoom-in completely, all data remains available, but you may need to scroll to see data at the bottom of the chart.

Predefined Charts in Orion System Manager

The following sections describe charts that are predefined and available in Orion System Manager. The list of available charts may be expanded in the object tree in the left pane of Orion System Manager.

Network Wide Summary Charts

All of the following network wide charts are customizable. For more information about customizing charts, see “Customizing Charts” on page 268.

Network Wide Percent Utilization Chart

Presents, in the same view, both average receive and average transmit utilization for all interfaces on all nodes on your network, as measured over a customizable period of time.

Network Wide Frame Relay Percent Utilization Chart

Presents the average frame relay utilization of all nodes on your network, as measured over a customizable period of time.

Average Response Time of all Nodes Chart

Presents the average response time of all nodes on your network, as measured over a customizable period of time.

Network Wide Availability Chart

Presents the average availability of all nodes on your network, as measured over a customizable period of time.

Network Wide Availability and Response Time Chart

Presents, in the same view, both network availability and average response time, as measured over a customizable period of time.

Min/Max and Average Response Time for all Nodes on the Network Chart

Presents the minimum, maximum, and average response times for all nodes on your network, simultaneously, as measured over a custom period of time.

Note: The minimum response time may be reported as 0ms. In this case, the minimum response time bar may not display on the chart.

Total Bytes Transferred over Entire Network Chart

Presents a measure of the total bytes transferred over all interfaces on all network nodes, as measured over a custom period of time.

The displayed time period for all Network Wide Summary charts may be changed by clicking any of the following options displayed beneath each chart:

- **Today** creates a chart of averaged hourly values of the selected statistic over the current day.
- **This Week** creates a chart of averaged hourly values of the selected statistic over the last 7 days.
- **This Month** creates a chart of averaged daily values of the selected statistic over all days in the current month.
- **Last 30 Days** creates a chart of averaged daily values of the selected statistic over the last 30 days.
- **Last 3 Months** creates a chart of averaged daily values of the selected statistic over the last 3 months.
- **Last 12 Months** creates a chart of averaged daily values of the selected statistic over the last 12 months.
- **This Year** creates a chart of averaged daily values of the selected statistic over all days in the current year.
- **Custom Period** creates a custom chart of the selected statistic over a period from the **Start Date / Time** to the **Ending Date / Time** that you type. Data points are plotted on the interval selected in the **Generate Sample** field.

Top XX Summary Charts

All of the following Network Wide charts are fully customizable. For more information about customizing charts, see “Customizing Charts” on page 268.

Current Response Time

Presents the Top XX monitored network nodes by Percent Loss and Response Time at the time the chart is selected from the chart tree. Nodes are listed in decreasing order of percent packet loss, followed by decreasing order of response time.

Average Response Time

Presents the Top XX monitored network nodes by Average Percent Loss and Average Response Time since the Orion NPM database began collecting network data. Nodes are listed in decreasing order of percent packet loss, followed by decreasing order of response time.

Current In/Out bps

Presents the Top XX monitored network interfaces by receive or transmit rate at the time the chart is selected from the chart tree. Interfaces are listed by decreasing rate of receive or transmit traffic.

Peak Traffic Load Today

Presents the Top XX monitored network interfaces by peak receive or transmit rate over the current day. Interfaces are listed by decreasing peak rate of receive or transmit traffic.

Current Percent Utilization

Presents the Top XX monitored network interfaces by receive or transmit percent utilization at the time the chart is selected from the chart tree. Interfaces are listed by decreasing receive or transmit percent utilization.

Current CPU Utilization

Presents the Top XX monitored network nodes by percent utilization of CPU capacity at the time the chart is selected from the chart tree. Nodes are listed by decreasing CPU percent utilization.

Current Memory Utilization

Presents the Top XX monitored network nodes by percent utilization of available memory at the time the chart is selected from the chart tree. Nodes are listed by decreasing percent utilization of available memory.

Current Volume Utilization

Presents the Top XX monitored volumes by percent utilization of available memory at the time the chart is selected from the chart tree. Nodes are listed by decreasing percent utilization of available volume memory.

Errors Today

Presents the top XX monitored network interfaces in terms of the total number of receive and transmit errors and discards experienced over the current day. Interfaces are identified with their parent nodes by concatenation in the form *Node_Name-Interface_Name*.

Customizing Charts

Orion NPM offers a number of options for customizing generated charts. The following procedure presents available options for customizing chart views.

To customize chart views:

1. Expand a Chart subgroup of the Node/Interface Tree in the left pane of Orion System Manager.
2. Click a chart.
3. Click **Charts > Customize Chart**.
4. Specify your preferred settings on each of the following tabs to customize your chart view:
 - The General tab presents options relating to chart titles, borders, colors, gridlines, font size, numeric precision, and graph type.
 - The Plot tab configures chart axes and plot styles, including a 3D option.
 - The Subsets tab allows you to break out data subsets, if they are defined and available, in your chart view.
 - The Points tab gives you the option to further specify the data points that are charted.
 - The Axis tab presents more options relating to chart axes.
 - The Font tab allows you to set the appearance of chart labels.
 - The Color tab gives you a wide array of options to set chart and background colors.
 - The Style tab sets the point and line types for chart data subsets.

For more information about other available Chart Settings, see “Charts Settings” on page 261.

Chapter 21

Managing the Orion NPM Database

Orion Network Performance Monitor uses a Microsoft SQL Server database to store collected network performance data and web console settings. The following tools are packaged with Orion NPM as SolarWinds Orion Database Utilities to help you manage your Orion database.

Database Manager

Allows you to perform queries, edit database values, export data, and perform database repair and compaction.

Database Maintenance

Allows you to summarize, clean, and compact your Orion NPM database.

Using Database Manager

The Database Manager can be used to perform queries, view database and table details, export data, and edit database values. You may also repair, compact, restore, or backup the database from the Database Manager application. The following procedures present some of the basic database management operations that are available with Database Manager.

Adding a Server

If you have not already designated a database for use with Orion NPM as a backup or supplement, use the following steps to add a SQL server to the Database Manager. Once added, your selected server and associated databases display in the tree structure in the left pane of Database Manager.

To add a SQL server to Database Manager:

1. Click **Start > All Programs > SolarWinds Orion > Advanced Features > Database Manager**.
2. Click **File > Add Server**.
3. Select from the **SQL Server** list or enter the IP address of the SQL server.
4. Select the login style.

Note: You may choose to **Log in using Windows NT Integrated Security** to automatically pass the Windows user ID and password to the SQL server, or select **Log in using an SQL Server userid and password** to use a separate login. Upon selecting the latter option, the window changes to

provide fields to enter the separate SQL Server **User Name** and **Password** that you want to use.

5. Click **Connect to Database Server**.

Creating Database Backups

You should periodically back-up your Orion Network Performance Monitor databases. For more information about scheduling regular database backups, see “Creating a Database Maintenance Plan” on page 275. The following procedure is used to back-up your databases in Database Manager.

To back-up a database in Database Manager:

1. Click **Start > All Programs > SolarWinds Orion > Advanced Features > Database Manager**.
2. *If the SQL Server hosting your Orion database is not listed in the left pane*, you must add the SQL Server hosting your Orion database. For more information, see “Adding a Server” on page 269.
3. Click **+** in the left pane to expand the SQL Server hosting your Orion database..

Note: `NetPerfMon` is the default name of the Orion database.

4. Right-click the name of the database you want to back-up.
5. Click **Backup Database**.
6. Enter a **Description** of the database backup, and then specify a path for the **Backup Filename** either by either navigating to the location after clicking **Browse (...)** or by entering the path directly.

Note: Typically, the default backup location for an Orion NPM database is designated as `C:\Program Files\SolarWinds\Data\NetPerfMon.BAK`. Ensure that the target location for the database backup has sufficient available disk space.

Restoring a Database

The following steps restore a database that you have backed up.

To restore a database from backup:

1. Click **Start > All Programs > SolarWinds Orion > Advanced Features > Database Manager**.
2. *If the SQL Server hosting your Orion database is not listed in the left pane*, you must add the SQL Server hosting your Orion database. For more information, see “Adding a Server” on page 269.

3. Click **+** in the left pane to expand the SQL Server hosting your Orion database, and then click your Orion database.

Note: `NetPerfMon` is the default name of the Orion database.

4. Click **Database > Restore Database**.
5. Click **Browse (...)** to navigate to the database that you want to restore, or enter a valid SQL backup database name and path.

Note: Typically, the default location for an Orion NPM database backup is `C:\Program Files\SolarWinds\Data\NetPerfMon.BAK`.

6. Click **Verify** to ensure that you have selected a valid SQL database.

Notes:

- When you select a database, the remaining fields are completed for you. The **Database Name** field is populated with the name that SQL Server uses to refer to the specified database. The remaining two fields display the data (`.mdf`) and transaction log (`.ldf`) files for the database. You can change the values provided.
- Database Manager does not create directories. You may only specify a path that already exists.
- You also cannot restore a database that is currently in use.

7. Click **OK** to restore the selected database.

Compacting your Database

Compacting a database shrinks it, reindexes it, and removes whitespace. You can compact a database by performing the following steps.

To compact a database with Database Manager:

1. Click **Start > All Programs > SolarWinds Orion > Advanced Features > Database Manager**.
2. **If the SQL Server hosting your Orion database is not listed in the left pane**, you must add the SQL Server hosting your Orion database. For more information, see “Adding a Server” on page 269.
3. Click **+** in the left pane to expand the SQL Server hosting your Orion database, and then click your Orion database.

Note: `NetPerfMon` is the default name of the Orion database.

4. Click **Database > Compact Database**.

Note: Upon completion, Database Manager displays a window comparing the size of the database before and after compaction. If the sizes are the

same, there may not be enough free space in the database to rearrange data. If you need to free up more space for database compaction to occur, see “Compacting Individual Tables” on page 272.

Compacting Individual Tables

If you are not able to perform a full database compaction due to limited server disk space, you can compact database tables individually, using the Database Manager application, as shown in the following procedure.

To compact individual tables:

1. Click **Start > All Programs > SolarWinds Orion > Advanced Features > Database Manager**.
2. ***If the SQL Server hosting your Orion database is not listed in the left pane***, you must add the SQL Server hosting your Orion database. For more information, see “Adding a Server” on page 269.
3. Click **+** in the left pane to expand the SQL Server hosting your Orion database, and then click your Orion database.
Note: NetPerfMon is the default name of the Orion database.
4. Click a table to compact in the expanded database, and then click **Table > Compact/Rebuild Indexes**.

Viewing Database Details

The Database Details window in Database Manager presents two tabs that display property and tables information about a selected database. The following procedure is a guide to the information that is available in the Database Details window.

To view database details:

1. Click **Start > All Programs > SolarWinds Orion > Advanced Features > Database Manager**.
2. ***If the SQL Server hosting your Orion database is not listed in the left pane***, you must add the SQL Server hosting your Orion database. For more information, see “Adding a Server” on page 269.
3. Click **+** in the left pane to expand the SQL Server hosting your Orion database, and then click your Orion database.
Note: NetPerfMon is the default name of the Orion database.

4. Click **Database > Database Details**.

Notes:

- The Properties tab provides general statistics and descriptions of the selected database.
- The Tables tab shows a list of the tables in the selected database and their respective sizes.

5. ***If the Last Backup field on the Properties tab is blank***, you have not generated a backup of the selected database. For more information about scheduling a recommended regular database backup, see “Creating a Database Maintenance Plan” on page 275.

Viewing Table Details

The Database Manager Table Details window provides property, column, and index information about the selected table. You can also query the selected table directly from the Table Details window., as shown in the following procedure.

To view table details:

1. Click **Start > All Programs > SolarWinds Orion > Advanced Features > Database Manager**.
2. ***If the SQL Server hosting your Orion database is not listed in the left pane***, you must add the SQL Server hosting your Orion database. For more information, see “Adding a Server” on page 269.
3. Click **+** in the left pane to expand the SQL Server hosting your Orion database, and then click **+** to expand your Orion database.

Note: `NetPerfMon` is the default name of the Orion database.

4. Click a table to view in the expanded database.
5. Click **Table > Table Details**.

Note: The Properties tab includes general statistics relating to the table size and creation date; the Columns tab describes the columns in the table, table keys, and field types; and the Indexes tab lists indexes used within the table.

6. If you want to query the open table, click **Query** in the tool bar.

Warning: Special care should be taken while editing database values as you can easily compromise the integrity of your database. For more information, see “Editing Database Fields” on page 274.

Note: A default SQL statement is provided, as well as radio buttons for displaying the data in read or read/write view.

Editing Database Fields

Database fields may be edited within the Database Manager application from the query view. The following procedure directs you in editing database fields in Orion Database Manager.

Warning: Be very careful when you are editing database values, as you can jeopardize the integrity of your database.

To edit database fields with Database Manager:

1. Stop the SolarWinds Network Performance Monitor service as follows:
 - a. Click **Start > All Programs > SolarWinds Orion > Advanced Features > Orion Service Manager**
 - b. Click **SolarWinds Network Performance Monitor** under Services, and then click **Stop**.
2. Click **Start > All Programs > SolarWinds Orion > Advanced Features > Database Manager**.
3. **If the SQL Server hosting your Orion database is not listed in the left pane**, you must add the SQL Server hosting your Orion database. For more information, see “Adding a Server” on page 269.
4. Click **+** in the left pane to expand the SQL Server hosting your Orion database, and then click **+** to expand your Orion database.

Note: `NetPerfMon` is the default name of the Orion database.
5. Click a table to view in the expanded database.
6. Click **Table > Query Table**.
7. Use the provided SQL statement or enter your own in the query field.
8. **If you want to view the query results in table view**, click **Refresh**.
9. **If you want to edit table fields**, select **Read/Write** at the top of the window, and then edit fields as necessary.
10. If you use the same SQL query often, you can save time by making the query a favorite, as follows:
 - a. Enter the query in the query field.
 - b. Click **Add to Favorites**.
 - c. Enter a name for the command, and then click **OK**.

Note: Database Manager saves the command with the name that you have provided. You can now use this command again, directly, by clicking **Paste from Favorites**.

Detaching a Database

Detaching a database removes its reference from the SQL Server, allowing you to safely move files to different locations. Database Manager allows you to detach a database and leave the data files of a database intact, as shown in the following procedure.

Note: SolarWinds does not recommend using the **Detach Database** option to migrate a database from one SQL Server to another. For more information, see “Migrating your Database” on page 279.

To detach a database:

1. Click **Start > All Programs > SolarWinds Orion > Advanced Features > Database Manager**.
2. ***If the SQL Server hosting your Orion database is not listed in the left pane***, you must add the SQL Server hosting your Orion database. For more information, see “Adding a Server” on page 269.
3. Click **+** in the left pane to expand the SQL Server hosting your Orion database, and then click your Orion database.

Note: NetPerfMon is the default name of the Orion database.

4. Click **Database > Detach Database** from the menu.

Creating a Database Maintenance Plan

Using Database Manager, you can create a database maintenance plan that will automatically compact and backup the database on a scheduled basis. As a security and information integrity issue, it is very important to regularly back-up your databases. Database Manager allows you to do this easily, using the following steps.

Note: SQL Server Agent must be running to execute database maintenance.

To create a database maintenance plan for an Orion Network Performance Monitor database:

1. Click **Start > All Programs > SolarWinds Orion > Advanced Features > Database Manager**.
2. ***If the SQL Server hosting your Orion database is not listed in the left pane***, you must add the SQL Server hosting your Orion database. For more information, see “Adding a Server” on page 269.
3. Click **+** in the left pane to expand the SQL Server hosting your Orion database, and then click your Orion database.

Note: NetPerfMon is the default name of the Orion database.

4. Click **Database > Database Backup Schedule**.
5. Select to run the backup either once a **Day** or once a **Week**.
6. *If you to want to run the backup once a week*, choose the **Backup Day**.
7. Set the **Backup Time**.
8. Click **Next**.
9. *If you want to compact and shrink the database before the backup*, check **Compact and Shrink Database before Backup**.
Note: SolarWinds recommends both that you perform database compaction weekly and that you compact and shrink databases before backups.
10. Enter the path to the directory where you would like to place backup files or click **Browse (...)** and then navigate to an appropriate directory.
11. *If you want to keep backup reports*, check **Generate a backup report each time the backup Job runs**, and then enter the path to the directory where you would like to Place Backup reports or click **Browse (...)** and then navigate to an appropriate directory.
12. Click **Finish**.

Using SQL Server Management Studio

If you have a licensed, Standard or Enterprise Edition copy of SQL Server 2005 or 2008 with SQL Server Management Studio installed, you can use it to maintain your Orion NPM database. The following procedure is a basic guide to configuring a daily Orion database maintenance plan in SQL Server Management Studio.

Notes:

- Your specific environment may require additional configuration.
- You may need to contact your database administrator to gain access to SQL Server Management Studio for your Orion database.
- The following procedure clears historical maintenance records and creates a backup of your Orion database. In general, however, SolarWinds recommends that you contact your database administrator and reference the Microsoft documentation provided with SQL Server for instructions on using SQL Server Management Studio to manage your Orion database.

To use SQL Server Management Studio to manage your Orion database:

1. Click **Start > Microsoft SQL Server > SQL Server Management Studio**.
2. Click **View > Object Explorer**.

3. Expand the SQL Server instance containing your Orion database in the Object Explorer pane on the left.
Note: Expand the Databases folder for any instance to confirm included databases. By default, the Orion database is named `NetPerfMon`.
4. Expand the Management folder, right-click the Maintenance Plans folder, and then click **Maintenance Plan Wizard**.
5. Click **Next** to start the SQL Server Maintenance Plan Wizard.
6. Provide an appropriate **Name** and **Description** for your maintenance plan.
7. Click **Browse (...)** next to the **Server** field.
8. Check your *SQL Server\Instance*, and then click **OK**.
Note: If your SQL Server\Instance is not in the list, provide it manually.
9. Select the authentication type that is used to connect to the SQL server, and, if required, provide appropriate **User name** and **Password** credentials.
Note: Use the same authentication type and credentials you provided in the Orion Configuration Wizard to access your Orion database.
10. Check **Clean Up History** and **Back Up Database (Full)**
Note: When a task is clicked, the Maintenance Plan Wizard provides a brief task description.
11. Click **Next**.
12. Set the order of task execution, top to bottom, by selecting tasks and clicking **Move Up** and **Move Down** as needed.
Note: The following steps assume the Clean Up History task precedes the Back Up Database (Full) task.
13. Click **Next** when the task execution order is set.
14. On the Define Cleanup History Task view, check the types of historical data to delete, and then set the threshold age for historical data removal.
15. Click **Next**.
16. On the Database Back Up (Full) view, complete the following steps:
 - a. Click the **Databases** field.
 - b. Select **These databases**.
 - c. Check your Orion database.
17. Click **OK**.
18. Select **Database** in the Backup component area.

19. In the Destination area, complete the following steps:
 - a. Select **Disk**.
 - b. Select **Create a backup file for every database**.
 - c. Click **Browse (...)** to select an appropriate database backup file destination with sufficient free space.
20. Click **Next**.
21. On the Select Plan Properties view, click **Change**.
22. Configure the database maintenance job schedule as follows:
 - a. Provide an appropriate **Name** for the new job schedule.
 - b. Select **Recurring** as the **Schedule type**.
 - c. Check **Enabled**, and then select **Daily** in the **Occurs** field.
 - d. Provide an off-peak network usage time in the **Occurs once at** field.
 - e. Select a **Start date**, and then select **No end date**.
23. Click **OK**.
24. Click **Next**.
25. Check **Write a report to a text file**.
26. Click **Browse (...)** to select an appropriate maintenance report file destination.
27. Review wizard results, and then click **Finish**.
28. When the wizard successfully finishes, click **Close**.

For additional help with using SQL server Management Studio, visit the Microsoft Support Website at <http://support.microsoft.com>.

Database Maintenance

The primary tasks that are available for maintaining a SQL database are data summarization and database compaction. Data summarization occurs automatically as a part of the nightly maintenance program. You can also run database maintenance on demand from the System Manager or from the Windows Start menu.

Running Database Maintenance

Database maintenance performs a series of data summarizations that help you optimize the size of your Orion database. Data summarization consists of gathering all the collected network data for a defined period of time, calculating statistics from the data, and then discarding the data itself while retaining the

statistics. By regularly running database maintenance, you can realize significant space savings and performance improvements.

Database maintenance can either be run directly from the Start menu, or scheduled for a set Archive Time and initiated from the Orion Polling Settings view in the Orion Web Console. In either case, once started, database maintenance normally proceeds without further attention. For more information about setting the Archive Time for database maintenance on the Orion Polling Settings view, see “Orion Polling Settings” on page 101. The following procedure provides the steps to perform Database Maintenance:

Note: Administrative privileges are required to run Database Maintenance.

To run the Database Maintenance utility:

1. ***If you want to run database Maintenance from the Orion Web Console***, complete the following steps:
 - a. Click **Settings** in the top right of the web console.
 - b. Click **Poller Settings** in the Settings group.
 - c. Click **Perform Maintenance Now** in the Database Settings area.
2. ***If you want to run database Maintenance from the Start menu***, click **Start > All Programs > SolarWinds Orion > Advanced Features > Database Maintenance**, and then click **Start**.

Migrating your Database

If you are modifying your Orion NPM implementation to use a different database server, you can migrate data from one Orion NPM database to another. Both the database from which you export data and the database into which you want to import data must be from the same version of Orion NPM.

Warning: You will not lose Web Console customizations when you overwrite your website, unless you have manually overwritten or modified the HTML within the `.asp` pages.

Note: Do not skip tabs or deviate from the tab order. Click **Start**, and then click **Continue** to complete the wizard in order. Completing tabs out of order may adversely affect the install process. For more information, see “Installing SolarWinds Orion Network Performance Monitor” on page 9.

To export data from one Orion NPM database and import it into another:

1. Connect to your database server with Database Manager. For more information, see “Adding a Server” on page 269.
2. Select your database, and then click **Database > Backup Database**.

3. Enter a **Description** of the database backup.
4. Enter a path or click **Browse (...)** and then navigate to a **Backup Filename**.
5. Click **OK**.
6. Copy the newly created backup file to a folder on the new server.
Note: The backup file is named after your Orion NPM database with the `.bak` extension. For example, if you have chosen the default name for your Orion NPM database, `NetPerfMon`, the backup is named `NetPerfMon.bak`.
7. Click **Start > All Programs > SolarWinds Orion > Advanced Features > Database Manager**.
8. Click **Add Server**.
9. Select the name of the SQL instance from the SQL Server list. If your server is not listed, complete the procedure in “Adding a Server” on page 269.
10. Select the appropriate authentication type, and then click **Connect to Database Server**.
11. Select your new server in the list, and then click **Server > Connect to Server**.
12. Click **Server > Restore Database**.
13. Enter the path to the database backup file on the server or click **Browse (...)** and then navigate to the location of the database backup file.
14. Click **OK**.
15. Close the Database Manager.
16. Click **Start > All Programs > SolarWinds Orion > Configuration and Auto-Discovery > Configuration Wizard**.
17. Specify the newly restored database in the Database Setup section of the wizard.
18. When prompted, click **Yes** to use the existing database.

Chapter 22

Monitoring Network Application Data

The Orion Application Performance Monitor (Orion APM) module provides focused application monitoring for network engineers, but it is much more than merely up/down status checks and process monitoring. By allowing you to create and monitor your own custom collection of monitored components, Orion APM provides an open field of opportunity to the network engineer. With Orion APM you can focus monitoring on your core services while easily ensuring application outages do not originate in the network. Orion APM provides the following features to help:

- Network service monitoring
- General TCP port monitoring
- WMI and SNMP process monitoring
- Service monitoring
- User experience monitoring using HTTP or HTTPS content checking

Built on the proven capabilities and solid architecture of Orion Network Performance Monitor, you know your current needs will be met and, as your needs grow, both the Orion platform and the Orion APM module will scale with you.

For more information about monitoring network applications with SolarWinds Orion Application Performance Monitor, see the *SolarWinds Orion Application Monitor Administrator Guide* at www.solarwinds.com.

Chapter 23

Managing IP Addresses

Orion IP Address Manager (Orion IPAM) module IP Address Manager (Orion IPAM) leverages Orion NPM's intuitive point-and-click interface to allow you to easily investigate IP address space issues. By periodically scanning the network for IP address changes, Orion IPAM maintains a dynamic list of IP addresses and allows engineers to plan for network growth, ensure IP space usage meets corporate standards, and reduce IP conflicts. Using Orion IPAM, network engineers can discover non-responsive IP addresses, coordinate team access to your IP space, and track network changes.

Built on the enterprise Orion core, Orion IPAM allows network engineers to create, schedule, and share IP space reports from a single reporting engine. Finally, network engineers can monitor network devices for fault, performance, configuration, and now IP address health indicators.

- Manage your entire IP infrastructure from an intuitive Web-Console
- Consolidate your IP addresses into a single repository
- Keep better records by periodically scanning your network for IP address changes
- Create, schedule and share reports on the IP address space percent utilization
- Keep network devices up by identifying and eliminating IP address conflicts
- Coordinate team access to your address space with role-based access control and track changes
- Identify non-responsive IP addresses to optimize your IP space

For more information about Orion IP Address Manager, see the *SolarWinds Orion IP Address Manager Administrator Guide* at www.solarwinds.com.

Chapter 24

Monitoring NetFlow Traffic Analysis Data

Orion Network Performance Monitor NetFlow Traffic Analyzer provides an easy-to-use, scalable network monitoring solution for IT professionals who are juggling any size Cisco NetFlow-enabled network.

NetFlow-enabled Cisco routers and switches provide a wealth of IP-related traffic information. Orion NetFlow Traffic Analyzer collects this NetFlow data, correlates the data into a useable format, and then provides this data, along with detailed network performance data collected by Orion NPM, as easily read graphs and reports on bandwidth use in and to your network. These reports help you monitor bandwidth, track conversations between internal and external endpoints, analyze traffic, and plan bandwidth capacity needs.

Orion NetFlow Traffic Analyzer also provides the same flow data analysis capabilities for devices using sFlow and J-flow packets.

For more information about Orion NetFlow Traffic Analyzer, see the *SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide* at www.solarwinds.com.

Chapter 25

Managing IP Service Level Agreements

SolarWinds Orion IP Service Level Agreement (IP SLA) Manager offers an easy-to-use, scalable IP SLA network monitoring solution that integrates seamlessly into the Orion Network Performance Monitor Web Console.

Why Install Orion Network Performance Monitor

Internet Protocol Service Level Agreement (IP SLA) technology offers a cost-effective and efficient response to the needs of enterprises of all sizes. As a network manager, you face more than the simple question of whether your network is up or down. You need to know specific quality of service measures for your network, and you need to know them both historically and in realtime. Orion IP SLA Manager gives you the tools to quickly test the fitness of your current network and then determine and track quality of service on your network over time.

Orion IP SLA Manager leverages the proven functionality of Orion NPM, adding a number of IP SLA-specific data collection and presentation tools that enable IP SLA network monitoring and realtime status reporting. Because it is a module of Orion NPM, Orion IP SLA Manager maintains the function of Orion NPM while allowing you to narrow your network management and monitoring focus to the IP SLA-capable devices of your wider network.

What Orion Network Performance Monitor Does

Orion IP SLA Manager provides a full-featured solution that gives you the ability to monitor and report both realtime and historical performance statistics for your IP SLA-capable network. Orion IP SLA Manager offers the following features to help you manage your entire network.

- Quality of Service (QoS) Monitoring with Cisco IP SLA Operations
- Custom Charts and Gauges
- Custom Alerts and Actions
- Custom Reporting
- Call Manager Monitoring

For more information about Orion IP SLA Manager, see the *SolarWinds Orion IP SLA Manager Administrator Guide* at www.solarwinds.com.

Chapter 26

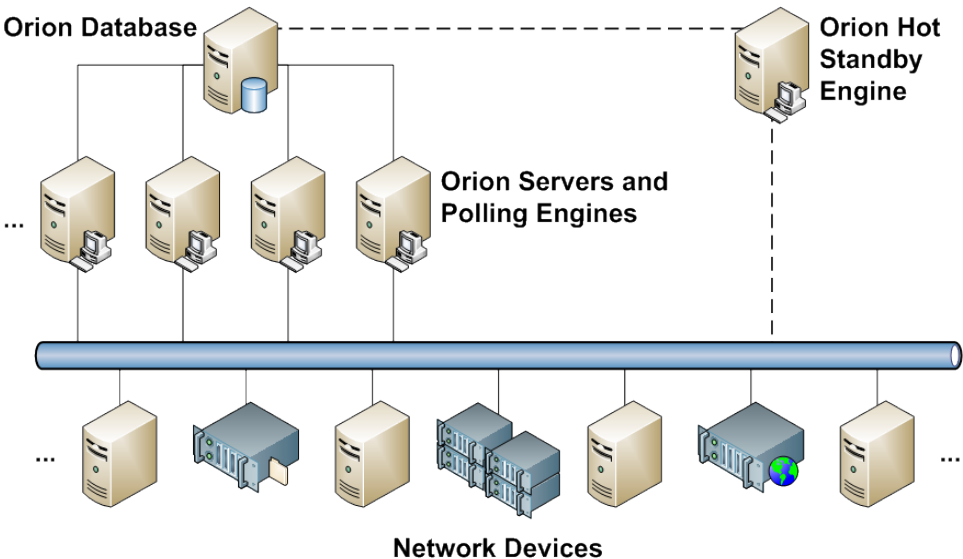
Orion Hot Standby Engine

The Orion Hot Standby Engine is an additional product that provides seamless backup service for other Orion NPM polling engines. In the event of an Orion NPM server failure, the designated hot standby system immediately assumes monitoring, data collection, and basic alerting responsibilities for that server. If the Orion NPM server becomes operational again, the Hot Standby Engine returns monitoring control to the Orion NPM server.

Warning: Orion Hot Standby Engines do not currently provide all the same data to custom pollers and Universal Device Pollers that may have been collected previously from the failed Orion NPM server. Likewise, Orion Hot Standby Engines are not currently capable of collecting data and computing network performance statistics for EnergyWise, VMware ESX, or wireless devices.

Note: A single Hot Standby Engine can serve as failover protection for multiple Orion NPM servers and polling engines simultaneously, but a single Hot Standby Engine can only assume the function of a single failed Orion NPM server at any given time.

The following graphic shows how an Orion Hot Standby Engine assumes the polling duties of any one failed Orion NPM server.



Installing a Hot Standby Engine

Orion Hot Standby Engine installation is nearly identical to the installation of a standard Orion NPM server, as shown in the following procedure.

Notes:

- To ensure optimal performance, your Orion Hot Standby Engine should not be any older than the latest version of any of the Orion NPM servers the Hot Standby Engine is supporting.
- For the same version, hardware and software requirements for both Orion NPM and Orion Hot Standby Server are equivalent. For more information, see “Orion NPM Requirements” on page 10.

To install a Hot Standby Engine:

1. Install and configure an Orion NPM server on your network. For more information about installing and configuring Orion NPM, see “Installing SolarWinds Orion Network Performance Monitor” on page 9.
2. Log on to the server you want to use as the Hot Standby server.
Note: The Hot Standby Engine must be installed on a server other than the primary Orion NPM server.
3. Download or copy the Hot Standby Engine installer to an appropriate location on the server you want to use as the Hot Standby Server.
4. ***If you downloaded the Hot Standby Engine from the SolarWinds website***, navigate to the download executable file, and then launch it.
5. ***If you received Hot Standby Engine on physical media***, browse to the executable file, and then launch the executable.
6. ***If you are prompted to install any required components such as Microsoft .NET Framework 3.5***, click **Install**, and then complete installation of the required additional components.
7. Review the Welcome text, and then click **Next**.
8. Agree to the license agreement, and then click **Next**.
9. Provide an installation destination folder on the Choose Destination Location window, and then click **Next**.
10. Click **Next** on the Start Copying Files window.
11. Provide the appropriate information on the Install Software License Key window, and then click **Continue**.

Note: You need your customer ID and password to successfully install the key. For more information, see “Software License Key” on page 303.

12. Click **Continue** when the license is successfully installed, and then click **Finish** on the Installation Complete window.
13. Click **Next** on the Welcome window of the Configuration Wizard.
14. Select or type the address of your **SQL Server**.
15. *If you are using Windows NT Integrated Security*, select the available option, and then click **Continue**.
16. *If you are using a SQL Server UserID and password*, select the available option, type a username and password, and then click **Continue**.
17. Select **Use an existing database**.
18. Provide the name of the **Existing Database** that your primary Orion NPM server is currently using, and then click **Next**.

Note: The Hot Standby Engine is designed to take the place of a failed server, so both the Orion NPM polling engine and standby polling engines must point to the same database in order to maintain network monitoring.
19. Select **Use an existing account**.
20. Provide an **Existing Account** and **Password** for the polling engine and web site to use to access the database, and then click **Next**.
21. *If you need to specify a particular IP Address for your Orion NPM installation*, provide the IP address of the web server that you want to use for the web console.

Note: SolarWinds recommends that you retain the default IP address setting of **All Unassigned**, unless your environment requires the designation of a specific IP address for your Orion Web Console.
22. Specify both the port through which you want to access the web console and the volume and folder in which you want to install the web console files.

Note: If you specify any port other than 80, you must include that port in the URL used to access the web console. For example, if you specify an IP address of 192.168.0.3 and port 8080, the URL used to access the web console is `http://192.168.0.3:8080`.
23. Click **Next**.
24. *If you are prompted to create a new directory*, click **Yes**.
25. Check the services you want to install on the Hot Standby server, and then click **Next**.

Note: Selecting all available services will ensure that all network monitoring functions are maintained if and when the server fails.
26. Click **Next** to start configuration.

27. When SolarWinds services have been installed, click **Finish**.
28. **If you are prompted to send a request to start the Hot Standby polling service**, click **Yes**.

Note: The configuration wizard stopped all polling engines when you configured the Hot Standby server.

29. Click **Start > All Programs > SolarWinds Orion > Advanced Features > Monitor Polling Engines**.
30. Confirm that both your primary Orion NPM server and the Hot Standby server are listed as **Responding** in the Monitor Polling Engines window.

Note: Click an Orion NPM server to view server information in the lower half of the Monitor Polling Engines window.

Configuring a Hot Standby Engine

The Hot Standby server that you have installed and assigned has the ability to both alert you when it assumes the Orion NPM server role and continue to alert you as long as the original server is stopped. However, the transition from the stopped Orion NPM server to the Hot Standby Engine is not necessarily immediate, as the delay between primary failure and hot standby assumption is variable. The following steps configure the Hot Standby Engine alerts and delays.

To configure a Hot Standby Engine:

1. Click **Start > All Programs > SolarWinds Orion > Advanced Features > Monitor Polling Engines**.
2. Click your Hot-Standby server from the list in the top pane of the Monitor Polling Engines window.

Note: The lower pane provides current information about the selected server.
3. Click **Configure Hot-Standby**.

Note: The default view of the Hot-Standby tab in the Configure Hot-Standby Server window provides a list of the servers for which the currently selected server is a hot standby.
4. Check the Orion NPM server for which you are installing the new Hot Standby Engine.
5. **If you want to enable an alert action for when the hot standby server is employed**, click **Fail-Over Notifications**, and then click **Add New Action**.

Note: For more information about adding alert actions, see “Adding Alert Actions” on page 158.
6. Click **Fail-Over Timing**.

7. Position the top slider to set the delay between the stopping of the Orion NPM server and the starting of your Hot-Standby server.
8. ***If you set an alert action as above and you want it to alert continuously, as long as the Hot-Standby server is enabled,*** complete the following procedure:
 - a. Check **Continuously send Fail-Over notifications...** in the middle of the tab view.
 - b. Position the bottom slider to set the delay between the stopping of the Orion NPM server and the starting of your Hot-Standby server.
9. Once you have completed configuring your Hot Standby Engine, click **OK**.

Testing a Hot Standby Engine

After you have installed, assigned, and configured your Hot Standby Engine, test that it works properly with the following steps.

Warning: Testing a Hot Standby Engine requires you to power off an Orion NPM server on your network. SolarWinds recommends you conduct any testing in off-peak usage periods to minimize potential uptime interruption.

To test a Hot Standby Engine:

1. Confirm that the SQL database you are maintaining with Orion NPM is not on the primary Orion NPM server.
2. Click **Start > All Programs > SolarWinds Orion > Advanced Features > Monitor Polling Engines**.
3. Click **Start > All Programs > SolarWinds Orion > Orion Web Console**.
4. Turn off your Orion NPM server.
5. Confirm that the Hot Standby server has assumed Orion NPM server duties by reviewing results from the Monitor Polling Engines window and the Orion Web Console.

Note: The lower pane of the Monitor Polling Engines window provides a number of helpful entries for determining engine state, including:

- Server Type
- Hot-Standby For...
- Last Fail-Over

Chapter 27

Using Additional Polling Engines

Because larger networks can quickly become too extensive for a single Orion NPM polling engine to adequately monitor, Additional Polling Engines are available to increase the monitoring capacity of your Orion NPM installation by enabling multiple monitoring engines that work in parallel across your network.

Note: Additional Polling Engines only support data collection for EnergyWise, ESX Server, and wireless devices if the primary Orion NPM polling engine is running.

Additional Polling Engine System Requirements

System requirements for an Additional Polling Engine are the same as system requirements for a primary Orion NPM polling engine. For more information about system requirements, see "Orion NPM Requirements" on page 10.

Note: Orion NPM is not able to add nodes to an Additional Polling Engine if DNS cannot resolve the name of the server hosting the Additional Polling Engine.

Installing an Additional Polling Engine

The installation of a new Additional Polling Engine, including initial configuration, follows the same steps required to complete the installation and configuration of a primary Orion NPM polling engine, with the following additional considerations:

- If you are using custom properties to monitor your network, you must copy related schema and configuration files from your primary Orion server to the server hosting your Additional Polling Engine. For more information, see "Custom Properties on Additional Polling Engines" on page 297.
- If you are using any basic alerts to monitor your network, you must make copies of all basic alert definitions in your Orion database, and then assign the copies to your Additional Polling Engine. For more information, see "Copying Basic Alerts to an Additional Polling Engine" on page 297.
- If you want to use any Orion modules for monitoring or managing any devices polled with an Additional Polling Engine, you must install the Additional Polling Engine version of the module you want to use on the server hosting your Additional Polling Engine. For more information, see the SolarWinds documentation for your Orion module.

For more information about completing an Orion NPM installation, see "Installing Orion Network Performance Monitor" on page 15.

Upgrading an Additional Polling Engine

Upgrading an Additional Polling Engine follows the same steps required to upgrade a primary Orion NPM polling engine. For more information, see “Upgrading Orion Network Performance Monitor” on page 20.

Note: If you are upgrading an Additional Polling Engine that is currently in service, the Additional Polling Engine will shutdown temporarily with the result that you may lose some polling data. SolarWinds recommends that you perform any Additional Polling Engine upgrades during off-peak hours of network usage to minimize the impact of temporary polling stoppages.

Configuring an Additional Polling Engine

Configuration typically occurs after an initial installation, but it may also be required when a non-standard configuration change is made or when a module is added to your Additional Polling Engine. In general, the steps to configure an Additional Polling Engine are the same as those required to configure a primary Orion NPM polling engine, with the following additional considerations:

- If you are using custom NPM properties to monitor your network, you must copy related schema and configuration files from your primary Orion server to the server hosting your Additional Polling Engine. For more information, see “Custom Properties on Additional Polling Engines” on page 297.
- If you are using any basic alerts to monitor your network, you must make copies of all basic alert definitions in your Orion database, and then assign the copies to your Additional Polling Engine. For more information, see “Copying Basic Alerts to an Additional Polling Engine” on page 297.
- If you want to use any Orion modules for monitoring or managing any devices polled with an Additional Polling Engine, you must install the Additional Polling Engine version of the module you want to use on the server hosting your Additional Polling Engine. For more information, see the SolarWinds documentation for your Orion module.

For more information about optimizing an additional polling engine configuration to coordinate with other polling engines, including a primary polling engine, see “Managing Orion NPM Polling Engines” on page 99.

Note: During configuration, the Additional Polling Engine will shutdown temporarily with the result that, if you are actively polling, you may lose some data. SolarWinds recommends that you configure polling engines during off-peak hours of network usage to minimize the impact of any temporary polling stoppage.

Custom Properties on Additional Polling Engines

Whenever a custom property is created or deleted, a number of Orion schema and configuration files are also modified. If you have created custom properties for monitoring your network, you must copy these related schema and configuration files from your original Orion NPM server to the server hosting your Additional Polling Engine, as shown in the following procedure.

To copy custom properties to an Additional Polling Engine:

1. Log on to the Orion polling engine on which your custom properties are defined using an account with administrative privileges.
2. Copy the following files from the default location on your primary Orion polling engine `C:\Program Files\SolarWinds\Orion\`:
 - `CustomPropertyEditor.trace`
 - `EnergyWise.schema`
 - `EnergyWiseCurrent.schema`
 - `OrionReportWriter.cfg`
 - `OrionReportWriter.schema`
 - `Wireless.schema`
3. Log on to your new Additional Polling Engine using an account with administrative privileges.
4. Paste the copied files to the same default location on your Additional Polling Engine (`C:\Program Files\SolarWinds\Orion\`).

Copying Basic Alerts to an Additional Polling Engine

Unlike advanced alerts, which are stored in the Orion database with a unique alert definition identifier, basic alert definitions are keyed to polling engines. As a result, if you want to apply a basic alert to nodes you have moved to an Additional Polling Engine, you must make a copy of each basic alert definition and then key it to the new Additional Polling Engine. The following procedure provides the steps required to copy basic alerts from your primary Orion polling engine to an Additional Polling Engine.

To copy basic alerts to an Additional Polling Engine:

1. Using an account with administrative privileges, log on to your primary Orion NPM server.
2. Click **Start > All Programs > SolarWinds Orion > System Manager**.
3. Click **Alerts**, and then click **Configure Basic Alerts**.

4. For each alert you want to apply to devices monitored by your Additional Polling Engine, complete the following steps:

Note: Repeat this procedure for each alert you want to copy to the Additional Polling Engine.

 - a. Check the alert to copy, and then click **Copy Alert**.
 - b. On the General tab, edit the alert name in the **Name of Alert** field to indicate that it is an Additional Polling Engine alert.
 - c. On the Monitored Network Objects tab, confirm that the copied alert is applied to the appropriate network devices.
 - d. Configure other tabs as appropriate, and then click **Done**. For more information, see “Configuring Basic Alerts” on page 135.
5. Click **Start > All Programs > SolarWinds Orion > Advanced Features > Monitor Polling Engines**.
6. Click the icon designating the Additional Polling Engine to which you want to copy your basic alerts.
7. Record the **Engine ID** for your Additional Polling Engine.
8. Click **Start > All Programs > SolarWinds Orion > Advanced Features > Database Manager**.
9. In the left pane, click **+** to expand both your SQL Server and your Orion database.

Notes:

- If your SQL Server and Orion database are not listed, you must add them. For more information about adding a SQL Server and an Orion database, see “Using Database Manager” on page 269.
- `NetPerfMon` is the default name of the Orion database.

10. Click **Alerts** in the expanded list of Orion database tables.
11. Click **Table > Query Table**, and then select **Read-Write (Results can be edited)**.
12. Clear the query field, and then type the following query into the cleared field:

Note: *EngineID* is the value found in the Monitor Polling Engines utility above. `'APE '` is a suggested string to identify alerts on the Additional Polling Engine..

```
UPDATE [NetPerfMon].[dbo].[Alerts]
  SET [EngineID]='EngineID', [AlertName]='APE ' + [AlertName]
  WHERE [AlertName] Like 'Copy%'
```

13. Click **Refresh**.

Chapter 28

Using an Orion Additional Web Server

The Orion Additional Web Server allows you to remotely view the Orion Web Console of your primary Orion NPM server just as you would see it if you were logged in locally on the primary Orion NPM server. The additional web server enables remote users to view the primary Orion Web Console without installing the entire Orion NPM suite or excessively taxing the resources of your primary Orion NPM server. The following procedure installs the Orion Additional Web Server.

To install an Orion Additional Web Server:

1. **If you downloaded the Orion Additional Web Server from the SolarWinds website**, navigate to your download location, and then launch the executable.
2. **If you received the Orion Additional Web Server on physical media**, browse to the executable file, and then launch the executable.
3. Review the Welcome text, and then click **Next**.
4. Accept the terms of the license agreement, and then click **Next**.
5. **If you want to install the Orion Additional Web Server to a folder other than the indicated default**, click **Browse**, and then provide a different destination folder on the Choose Destination Location window.
6. Click **Next** on the Choose Destination Location window.
7. Confirm the settings on the Start Copying Files window, and then click **Next**.
8. Provide the appropriate information on the Install Software License Key window, and then click **Continue**.
Note: You need your customer ID and password to install the key. For more information, see “Software License Key” on page 303.
9. Click **Continue** when the license is successfully installed.
10. Click **Finish** on the Installation Complete window.
11. **If the Configuration Wizard does not start automatically**, click **Start > All Programs > SolarWinds Orion > Configuration and Auto-Discovery > Configuration Wizard**.
12. Click **Start** on the Welcome tab of the Configuration Wizard.

13. Click **Continue** on the Setup Database tab of the Configuration Wizard.
14. Select or type the **SQL Server** used by your primary Orion NPM server.
15. *If you are using Windows NT Integrated Security*, select the available option, and then click **Continue**.
16. *If you are using a SQL Server UserID and password*, complete the following steps:
 - a. Select the available option.
 - b. Provide your **User Name** and **Password**.
 - c. Click **Continue**.
17. Select or type the **Database Name** that is on your Orion NPM server, and then click **Continue**.
18. *If a dialog appears that says that multiple polling engines have been detected*, click **OK** to continue database upgrade/verification.
19. When the database structure validation completes, click **Continue**.
20. Specify a SQL account **User Name** and **Password** for the polling engine and web site to use to access the database, and then click **Continue**.

Note: If you already have a SQL account, you can specify the credentials for that account.
21. To set up the web console, click **Continue** on the Create Website tab, and then complete the following procedure:
 - a. Specify the **IP Address** of the local server on which you are installing the new web-only interface.
 - b. Specify the **TCP Port** through which you want to access the web console.

Note: If you specify any port other than 80, you must specify that port in the URL that is used to access the web console. For example, if you specify an IP address of 192.168.0.3 and port 8080, your URL is `http://192.168.0.3:8080`.
 - c. Specify the volume and folder in which you want to install the web console files, and then click **Continue**.
22. *If you are asked to overwrite an existing website*, click **Yes**.
23. When the new web console has been created, click **Continue**.
24. Click **Start > All Programs > SolarWinds Orion > Orion Web Console**.
25. Enter the local IP address in the Address bar.

26. **If you already have an Admin account and password**, enter them in the respective fields, and then click **Login**.
Note: You can log in without a password using `Admin` as the Account ID.
27. Confirm that the new additional web server displays the same view for the same account, as used both locally and on your primary Orion NPM server.
28. **If you intend to install either Orion NetFlow Traffic Analyzer or Orion Application Performance Monitor on this Orion additional web server**, complete the following steps to install the required additional web console components.
 - a. Using your SolarWinds **Customer ID** and **Password**, log in to the Customer Port at <http://www.solarwinds.com/customerportal/>.
 - b. Click **Additional Components** in the Customer Portal menu on the left.
 - c. Click **Download Orion NPM Components**.
29. **If you intend to use Orion Application Performance Monitor with this Orion additional web server**, complete the following steps.
 - a. Click **Application Performance Monitor Additional Web Console—v2** in the Additional Components – Orion v8 and v9 section.
 - b. Click **Save**.
 - c. Browse to an appropriate location, and then click **Save**.
 - d. When the download completes, click **Open**.
 - e. Launch the executable, and then complete the configuration wizard.
30. **If you intend to use Orion NetFlow Traffic Analyzer with this Orion additional web server**, complete the following steps.
 - a. Click **Application NetFlow Traffic Analyzer Additional Web Console—v3** in the Additional Components – Orion v8 and v9 section.
 - b. Click **Save**.
 - c. Browse to an appropriate location, and then click **Save**.
 - d. When the download completes, click **Open**.
 - e. Launch the executable, and then complete the configuration wizard.

Appendix A

Software License Key

During installation, you may be prompted with the Install Software License Key window requesting that you supply your name, e-mail address, phone number, customer ID, and password. If this is the case, follow the instructions below to enable a software license key.

To enable a software license key:

1. ***If the computer on which you are installing Orion Network Performance Monitor is connected to the Internet***, enter the requested information on the Install Software License Key window, and then click **Continue**.

Note: The SolarWinds license registration server will immediately issue a license key that will allow Orion Network Performance Monitor to operate.

2. ***If the computer on which you are installing Orion Network Performance Monitor is not connected to the Internet***, your server cannot authenticate to the SolarWinds license registration server, so you must complete the following procedure:
 - a. Click **Skip This and Enter Software License Key Now** on the Install Software License Key window.
 - b. Using another computer that is connected to the Internet, log in to the customer area of the SolarWinds website at www.solarwinds.com/keys.
 - c. Click **Software Keys** from the Customer Area menu.
 - d. Click the product for which you need a key.
 - e. Provide the requested information, including the Computer Name and Program Serial Number.
 - f. Click **Generate Key**.
 - g. Copy the generated key.
 - h. Enter the key in the **Enter Software License Key** text box.
3. Click **Continue** to complete your Software License Key installation.

Appendix B


















Status Icons and Identifiers

Orion NPM and Orion modules use a number of different icons as status indicators in System Manager and Web Console resources. In the case of alerts and events, further information is provided with the icon within the resource.

Status Indicators

The following table lists Orion NPM icons with associated status indications, status types, and numerical status identifiers, proceeding from the worst.

Note: Status levels of type Ignore are not displayed in any status rollup mode.

Icon	Status Indication	Type	ID
	Node or Interface is Down (Polling request timed-out)	Error	2
	Shutdown	Error	4
	Lower Layer Down	Error	8
	Unreachable	Error	12
 	Node is in a Warning state (dropped packets or down interface)	Warning	3
	Critical	Warning	14
	Mixed Availability	Warning	15
	Misconfigured	Warning	16
	Could Not Poll	Warning	17
	Unconfirmed	Warning	19
	Polling Engine Shutdown, Monitoring Stopped, System Error, or Fail Over	Warning	--
	System Warning; Node, Interface, or Volume Changed; Interface Reappeared; Network Baseline Started/Completed	Warning	--
	Node or Interface is Up	OK	1
	Dormant	OK	6
	Active	OK	22
	Inactive	OK	24
	Expired	OK	25


Icon	Status Indication	Type	ID
	Unknown	Ignore	0
	Node or Interface is Unmanaged	Ignore	9
	Interface is Unplugged but not Down	Ignore	10
	Node is defined as External (Node is not monitored by Orion NPM, but an application on the node may be monitored by Orion Application Performance Monitor.)	Ignore	11
	Monitoring Disabled	Ignore	26
	Disabled	Ignore	27
	Not Licensed	Ignore	28
	Informational Volume Reappeared	N/A	--
	Monitoring Started, NPM Service Started, or Fail Back	N/A	--
	Node, Interface, or Volume Removed Interface Shutdown	N/A	--
	Node Added Interface or Volume Added (System Manager)	N/A	--
	Interface or Volume Added (Web Console)	N/A	--
	Node Rebooted	N/A	--
	Interface Enabled	N/A	--
	Interface Remapped	N/A	--
	Volume Remapped	N/A	--
	Interface or Volume Disappeared	N/A	--











Status Rollup Mode

In the Orion Web Console, the Status Rollup Mode designates how the availability status of a collection of nodes on the node tree or on a map is displayed in the web console. Two options are available for the case when there are nodes or applications with different status levels in the selected group:

- **Show Worst Status** ensures that the worst status in a group of objects is displayed for the whole group. The following table indicates how the **Show Worst Status** option operates:

Object States	Group Status
(Up, Warning, Down)	(Down)
(Warning, Down)	(Warning)
(Warning, Down, Unknown)	(Down)

- Mixed Status shows Warning** ensures that the status of a group displays the worst warning-type state in the group. If there are no warning-type states, but the group contains a mix of up and down states, then a Mixed Availability () warning status is displayed for the whole group. The following table indicates how the **Mixed Status shows Warning** option operates:

Object States	Group Status
 	 (Critical)
  	 (Critical)
 	 (Mixed Availability)

Appendix C

Alert Variables and Examples

Orion NPM alert engines can use variables within the messages that are sent when an alert is triggered or reset. These variables are dynamic, and they parse when the alert is triggered or reset. For example, using the basic alert engine, the variable `${InPercentUtil}` will parse with the current inbound percent utilization of the interface that is triggering the alert.

Notes:

- In some cases, the table name may be required for alert variables, as in `${CustomPollers.Description}`.
- In earlier versions of Orion NPM, variables were referred to as *macros*.

Variable Modifiers

The variables in the following sections can be modified by appending any of the variable modifiers in the following table.

Variable Modifier	Description
-Raw	Displays the raw value for the statistic. For example, if Transmit Bandwidth is set to 10 Mbps, then the raw value would be "10000000". The cooked value would be "10 Mbps".
-Previous	Displays the previous value for the statistic before the Alert was triggered
-Cooked	Displays the cooked value for the statistic. For example, if Transmit Bandwidth is set to 10 Mbps, then the raw value would be "10000000" and cooked value would be "10 Mbps".
-PreviousCooked	Displays the previous cooked value for the statistic before the Alert was triggered

Basic Alert Engine Variables

The following variables can be used in alert messages within Orion NPM. Each variable must be enclosed in braces and begin with a dollar sign, like `${NodeID}`

Buffer Errors

Buffer Error Variable	Description
<code>\$(BufferNoMemThisHour)</code>	Buffer errors caused by low memory during the current hour
<code>\$(BufferNoMemToday)</code>	Buffer errors caused by low memory during the current day
<code>\$(BufferSmMissThisHour)</code>	Small buffer misses during this hour

Buffer Error Variable	Description
#{BufferSmMissToday}	Small buffer misses during the current day
#{BufferMdMissThisHour}	Medium buffer misses during this hour
#{BufferMdMissToday}	Medium buffer misses during the current day
#{BufferBgMissThisHour}	Big buffer misses during this hour
#{BufferBgMissToday}	Big buffer misses during the current day
#{BufferLgMissThisHour}	Large buffer misses during this hour
#{BufferLgMissToday}	Large buffer misses during the current day
#{BufferHgMissThisHour}	Huge buffer misses during this hour
#{BufferHgMissToday}	Huge buffer misses during the current day

Interfaces

Interface Variable	Description
#{Caption}	Description of the interface.
#{InterfaceID}	Unique ID of the interface. Network Performance Monitor assigns a unique ID to every network object.
#{InterfaceCaption}	User-assigned name for this interface
#{Index}	Index of the interface within the network node.
#{InterfaceType}	Numerical type of the interface. This information is collected by Orion NPM when discovering the network node.
#{MAC}	Physical address (MAC Address) of the interface
#{MTU}	Maximum Transmission Unit
#{InterfaceSpeed}	Speed of the Interface discovered by Network Performance Monitor when scanning the network node
#{InterfaceName}	Name of the interface discovered from the node
#{InterfaceIcon}	Icon depicting the type of interface (Ethernet, Frame-Relay, ATM, Token Ring, wireless, etc).
#{NodeID}	ID of the Node to which this interface belongs. Orion NPM assigns a unique ID to every network object.
#{InterfaceTypeName}	Type of interface. Discovered from ifType.
#{FullName}	Full name of the interface including the name of the network node it is in
#{Counter64}	Interface supports IF-MIB high-capacity counters

Interface Errors

Interface Error Variable	Description
#{InDiscardsToday}	Cumulative number of receive discards for this interface today
#{InErrorsToday}	Cumulative number of receive errors for this interface today
#{OutErrorsToday}	Cumulative number of transmit errors for this interface today
#{OutDiscardsToday}	Cumulative number of transmit discards for this interface today
#{InDiscardsThisHour}	Cumulative number of receive discards for this in

Interface Error Variable	Description
<code>#{InErrorsThisHour}</code>	Cumulative number of receive errors for this interface this hour (this counter resets at the top of the hour)
<code>#{OutErrorsThisHour}</code>	Cumulative number of transmit errors for this interface this hour (this counter resets at the top of the hour)
<code>#{OutDiscardsThisHour}</code>	Cumulative number of transmit discards for this interface this hour (this counter resets at the top of the hour)

Interface Status

Interface Status Variable	Description
<code>#{AdminStatus}</code>	Administrative status of the interface (enabled or disabled)
<code>#{AdminStatusLED}</code>	LED showing current administrative status of the interface (enabled or disabled)
<code>#{InterfaceLastChange}</code>	Last date and time the interface changed operational status
<code>#{OperStatus}</code>	Operational status of the interface
<code>#{OperStatusLED}</code>	LED showing current operational status of the interface
<code>#{Status}</code>	Current status of the interface (up, down, shutdown, etc.)
<code>#{StatusLED}</code>	Current status of the interface (up, down, shutdown, etc.)

Interface Polling

Interface Polling Variable	Description
<code>#{PollInterval}</code>	How often the interface should be polled (seconds)
<code>#{RediscoveryInterval}</code>	How often the node/interface should be rediscovered (minutes)
<code>#{NextRediscovery}</code>	Scheduled time for the next complete discovery of this interface
<code>#{NextPoll}</code>	Scheduled time for next poll of this interface
<code>#{StatCollection}</code>	Frequency of statistics collection

Interface Traffic

Interface Traffic Variable	Description
<code>#{OutBandwidth}</code>	User-defined transmit bandwidth of the Interface. The Transmit and Receive bandwidth can each be set independently in order to accurately monitor asymmetric circuits.
<code>#{OutBps}</code>	Current amount of traffic being transmitted by the interface
<code>#{InBps}</code>	Current amount of traffic being received by the interface
<code>#{OutPps}</code>	Current rate of transmitted packets per second by the interface
<code>#{InPps}</code>	Current rate of received packets per second by the interface
<code>#{InPktSize}</code>	Average packet size of the packets currently being received by the interface

Interface Traffic Variable	Description
#{OutUcastPps}	Current rate of transmitted unicast packets per second
#{OutMcastPps}	Current rate of transmitted multicast packets per second
#{InUcastPps}	Current rate of received unicast packets per second
#{InMcastPps}	Current rate of received multicast packets per second
#{OutPktSize}	Average packet size of the packets currently being transmitted by the interface
#{InPercentUtil}	Current percentage of utilization on the receive side of the interface
#{OutPercentUtil}	Current percentage of utilization on the transmit side of the interface
#{MaxInBpsToday}	Peak received bps today for the interface
#{MaxOutBpsToday}	Peak transmitted bps today for the interface
#{MaxInBpsTime}	Time (today) of the peak bps received
#{MaxOutBpsTime}	Time (today) of the peak bps transmitted
#{InBandwidth}	User-defined receive bandwidth of the Interface. The Transmit and Receive Bandwidth can each be set independently in order to accurately monitor asymmetric circuits.

Nodes

Node Variable	Description
#{NodeID}	Unique ID automatically assigned to each node
#{IP_Address}	IP Address of the node. This is the IP address that is used for all management functions.
#{NodeName}	User assigned name for this node
#{SysName}	System name of the node
#{DNS}	DNS name determined using a reverse DNS lookup. The DNS entry is checked during rediscovery of the network node.
#{SysObjectID}	Unique identifier assigned to this node by the manufacture
#{Vendor}	The manufacture of the network node
#{Location}	Location retrieved from the system MIB
#{Contact}	System Contact. This information is collected by Network Performance Monitor when discovering the network node.
#{Description}	System description of the node. This information is collected by Network Performance Monitor when discovering the network node.
#{LastBoot}	Date and time the machine last booted
#{Community}	SNMP community string used to communicate with this node
#{VendorIcon}	Icon depicting the type of machine
#{IOSImage}	Cisco IOS image family type
#{IOSVersion}	Cisco IOS version
#{MachineType}	The machine type or manufacture of the network node

Node Polling

Node Polling Variable	Description
<code>#{RediscoveryInterval}</code>	How often the node should be rediscovered (in minutes)
<code>#{NextRediscovery}</code>	Date and time of next rediscovery
<code>#{PollInterval}</code>	How often the node/interface should be polled. (in seconds)
<code>#{NextPoll}</code>	Scheduled time for the next poll of the node/interface
<code>#{StatCollection}</code>	Frequency of statistics collection

Node Statistics

Node Statistics Variable	Description
<code>#{ResponseTime}</code>	Current response time of the node in milliseconds
<code>#{PercentLoss}</code>	Percent packet loss over the last few minutes. Packet loss is calculated from the number of ICMP packets that are dropped when polling the node.
<code>#{AvgResponseTime}</code>	Average response time for the node over the last few minutes
<code>#{MinResponseTime}</code>	Shortest response time over the last few minutes
<code>#{MaxResponseTime}</code>	Longest response time over the last few minutes
<code>#{CPULoad}</code>	Percentage of CPU usage
<code>#{TotalMemory}</code>	Total RAM reported in node
<code>#{MemoryUsed}</code>	Total RAM in allocated in node
<code>#{PercentMemoryUsed}</code>	Percentage of used RAM to total RAM

Node Status

Node Status Variable	Description
<code>#{Status}</code>	Current status of the node. (up, down, warning, etc)
<code>#{StatusLED}</code>	Current status icon of the node
<code>#{GroupStatus}</code>	Current status icon of the Node and all its interfaces (Up, Down, Warning, etc)
<code>#{StatusDescription}</code>	Current status of the Node and its interfaces.
<code>#{Severity}</code>	Severity Status of the Node and its Interfaces

Object Types

Object Types Variable	Description
<code>#{ObjectType}</code>	Type of network object
<code>#{ObjectSubtype}</code>	Subtype of the network object

Volumes

Volume Variable	Description
\$(NodeID)	ID of the network node to which this volume belongs. Network Performance Monitor assigns a unique ID to every network object.
\$(VolumeID)	Unique ID of the volume. Network Performance Monitor assigns a unique ID to every network object.
\$(Caption)	User-assigned name for this volume
\$(VolumeIndex)	Index of the volume within the Network Node
\$(VolumeType)	Type of volume. Discovered from hrStorageType
\$(VolumeDescription)	Description of the volume
\$(FullName)	Full name of the volume including the name of the Network Node it is in.

Volume Polling

Volume Polling Variable	Description
\$(PollInterval)	How often the volume should be polled
\$(StatCollection)	Frequency of statistics collection
\$(NextPoll)	Scheduled time for next poll of this volume
\$(RediscoveryInterval)	Rediscovery Interval of this Volume
\$(NextRediscovery)	Scheduled time for the next complete discovery of this volume.

Volume Statistics

Volume Statistics Variable	Description
\$(VolumeSize)	Volume size in bytes
\$(VolumeSpaceUsed)	Total bytes used on volume
\$(VolumePercentUsed)	Percentage of volume used as discovered by SNMP
\$(VolumeAllocationFailuresThisHour)	Number of volume allocation errors this hour
\$(VolumeAllocationFailuresToday)	Number of volume allocation errors today

Volume Status

Volume Status Variable	Description
\$(Status)	Current status of the volume (up, down, shutdown, etc.)
\$(StatusLED)	Current status of the volume (up, down, shutdown, etc.)
\$(VolumeResponding)	Indicates whether or not the volume is currently responding to SNMP queries

Date/Time

Date/Time Variable	Description
`\${DateTime}`	Current date and time. (Windows control panel defined "Short Date" and "Short Time" format)
`\${Date}`	Current date. (Short Date format)
`\${LongDate}`	Current date. (Long Date format)
`\${MediumDate}`	Current date. (Medium Date format)
`\${Time}`	Current Time. (Short Time format)
`\${DayOfWeek}`	Current day of the week.
`\${D}`	Current day of the month
`\${DD}`	Current day of the month (two digit number, zero padded)
`\${AbbreviatedDOW}`	Current day of the week. Three character abbreviation.
`\${LocalDOW}`	Current day of the week. Localized language format.
`\${M}`	Current numeric month
`\${MM}`	Current month. Two digit number, zero padded.
`\${MMM}`	Current month. Three character abbreviation.
`\${MMMM}`	Full name of the current month
`\${LocalMonthName}`	Current month name in the local language.
`\${DayOfYear}`	Numeric day of the year
`\${Year2}`	Two digit year
`\${Year}`	Four digit year
`\${H}`	Current hour
`\${HH}`	Current hour. Two digit format, zero padded.
`\${Minute}`	Current minute. Two digit format, zero padded.
`\${S}`	Current second.
`\${Second}`	Current second. Two digit format, zero padded.
`\${AMPM}`	AM/PM indicator

Alert-specific

Alert-specific Variable	Description
`\${AlertName}`	Name of the Alert
`\${Property}`	Property that this Alert is monitoring
`\${TriggerTime}`	Date and time of the last event for this Alert. (Windows control panel defined "Short Date" and "Short Time")
`\${LastResetTime}`	Date and time of the last event for this Alert. (Windows control panel defined "Short Date" and "Short Time")
`\${LongTriggerTime}`	Date and time of the last event for this Alert. (Windows control panel defined "Medium Date" and "Medium Time")
`\${LongLastResetTime}`	Date and time of the last event for this Alert. (Windows control panel defined "Medium Date" and "Medium Time")

Alert-specific Variable	Description
`\${TriggeredValue}`	Value that triggered the Alert
`\${AlertStartTime}`	Time of day that the Alert is active and can be Triggered/Reset
`\${AlertEndTime}`	Time of day that the Alert is active and can be Triggered/Reset

Example Messages Using Variables

The following examples illustrate some of the uses of variables.

- Interface `\${FullName}` has changed from `\${Status-Previous}` to `\${Status}`. `\${FullName}` rebooted at `\${LastBoot}`.
- Previous reboot was at `\${LastBoot-Previous}`.
- Interface `\${Caption}` on `\${NodeName}` is `\${Status}`. This indicates a problem with this network segment that should be investigated. This problem was identified at `\${DateTime}`.
- Alert: `\${NodeName}` has exceptionally high response time. Average Response Time is `\${AvgResponseTime}` and is varying from `\${MinResponseTime}` to `\${MaxResponseTime}`.
- Alert: Percent Utilization of `\${FullName}` is above `\${OutPercentUtil}`. Current traffic load on this interface is `\${InBps}` Received and `\${OutBps}` Transmitted.
- Current packet loss for `\${NodeName}` is `\${%Loss}`. Average Response time is `\${AvgResponseTime}` and is varying from `\${MinResponseTime}` to `\${MaxResponseTime}`.
- Alert: The SNMP Community string used to query `\${NodeName}` has been changed from `\${Community-Previous}` to `\${Community}`.
- Orion NPM uses the new Community String to query `\${NodeName}`.

Basic Alert Engine Suppression Examples

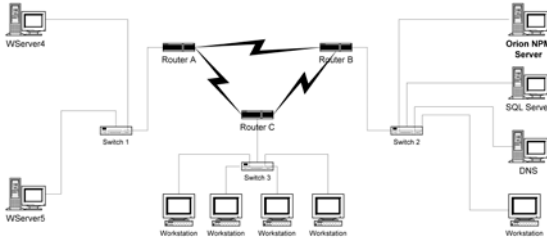
Many error conditions can occur in a network to trigger multiple alerts from a single event. There are also conditions that may not need to trigger an alert by themselves but that should trigger alerts if they occur with other conditions. Alert Suppression allows you to set up conditions to analyze alert situations and give you the information you need to determine the root cause of the problem.

By default, alert suppression is not enabled for Orion NPM alerts. When using the basic alert engine, you may specify alert suppression either when any of one or more conditions exist, or if all of two or more conditions exist.

Note: Proceed with extreme care when configuring the alert suppressions, as it is possible to suppress alerts containing important information about your network.. SolarWinds suggests you carefully consider any alert suppression

scheme, develop a diagram of your network, and then extensively test any scenario in which you intend to apply alert suppression.

Examples of situations for which you might want to create alert suppressions are illustrated in the following diagram.



Note: The Orion NPM server is located on Switch 2, at the top right.

Failure of redundant servers

In the diagram, both WServers are identical to provide failover, redundancy, and load balancing. If WServer4 fails but WServer5 is still functioning, you may want to be alerted immediately if the failure occurs during business hours, though it might not justify a pager alert in the middle of the night. In this case, you would configure the alert for the failure of one WServer to be suppressed unless the other also fails.

Apparent failure of dependent nodes downstream of a failed router (or switch, or circuit)

In the diagram, there are dependencies among devices. For instance, if Router C fails, the Orion NPM server cannot reach Switch 3 or any of the four workstations. You will want to know if and when the workstations have failed, but only if Router C and Switch 3 have not failed. You would configure the alerts such that a failure alert for the workstations is dependent on Router C and Switch 3 being operational.

Failure of a network link when a redundant link is still functional

In some cases, you may only want to know of the failure of the link between Routers B and C if the alternative link through Router A is also down.

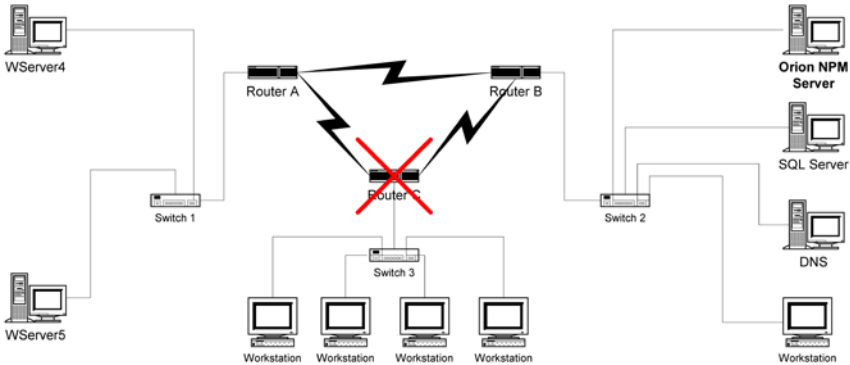
Failure of load balancing between devices

You may have configured your network to balance traffic across your web servers. In this case, you could configure an alert that notifies you of very high CPU utilization on any one of the servers but only if one or more is experiencing much lower usage.

Note: Alert suppression does not preclude knowledge of critical events. Network events are logged in the database whether alert suppression is enabled or not.

Dependent Node Alert Suppression Example

Suppose you configure an alert to notify you when nodes on a subnet go down. In this case, the nodes are on a segment of your network on the other side of a particular router, and you only want alerts if the router is still operational.



Note: For this example, the router should not be included in the group of monitored objects, since its failure is the trigger for suppressing the alert. To be notified of router failure, you must set up another alert.

To configure a dependant node alert suppression:

1. Click **Start > All Programs > SolarWinds Orion > System Manager**.
 2. Click **Alerts > Configure Basic Alerts**.
 3. Click **New Alert**.
 4. Click General, enter a name for your alert, and then check **Enable this Alert**.
 5. Click Property to Monitor.
 6. Check **Node Status > Status**.
- Note:** Select only one property from those that are available.
7. Click Monitored Network Objects, and then select the workstations that are on the segment of your network that is on the other side of the router.
 8. Click Alert Trigger.
 9. Check **Trigger Alert when Status is > Unknown, Down, and Warning**.
 10. Check **Reset Alert when Status is > Up**.
 11. Click Alert Suppression, and then select **Suppress this alert if ANY of the selected suppressions are active**.

Note: The window opens to display a list of current suppressions, if any exist, and buttons that you can use to add, edit, and delete conditions.

12. Click **Add**.
13. Click Property to Monitor, and then select **Node Status > Status**.

Note: Select only one property from those that are available.
14. Click Network Object.
15. Select the router that stands between Orion NPM and the subnet for which you have configured the node down alert.

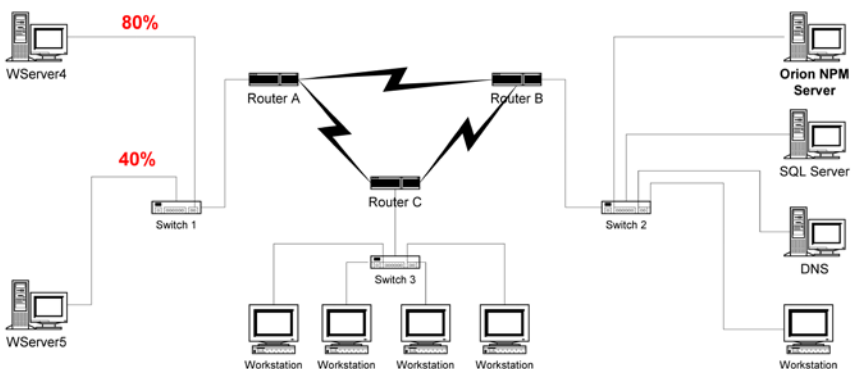
Note: The type of objects available for monitoring depends upon the choice that you made in the Properties to Monitor tab. If you had chosen to monitor an interface-related property, you would see a list of available interfaces. Since you've chosen a node-related property, you will see a list of nodes.
16. Click Suppression Trigger.
17. Check **Down**, **Warning**, and **Unknown** on the tab, and then click **OK**.

Note: For status conditions, you may specify more than one condition.
18. Check the suppressions that you want to apply in order to enable them.

Note: By default, suppressions are not turned on.
19. **If you want to add more conditions**, repeat this procedure, by clicking **Add** to begin again.

Failure of Load Balancing Alert

If you have multiple servers configured to share the load on your website, you will want to know if one of them is not performing as it should. For the purposes of this example, we'll assume that you want to be alerted when the CPU load on two servers exceeds 80 percent, but only if one shows a CPU load of 40 percent or less. In other words, the alert is suppressed if the second server reports greater than 40 percent utilization, as shown in the diagram.



You will need to configure two alerts, one for each server. They will be identical, except for the server that each alert monitors. Proceed to follow these steps to configure these alerts. For more information, see “Creating and Managing Alerts” on page 133.

To configure a load balancing failure alert:

1. Click **Start > All Programs > SolarWinds Orion > System Manager**.
2. Click **Alerts > Configure Basic Alerts**.
3. Click **New Alert**.
4. Click **General**.
5. Enter a name for your alert, and then check **Enable this Alert**.
6. Click **Property to Monitor**.
7. Check **Node Statistics > % CPU Utilization**.
8. Click **Monitored Network Objects**, and then check the server that you want to monitor.
9. Click **Alert Trigger**.
10. Select a condition to **Trigger Alert when % CPU Utilization**, and then enter the trigger value: **Trigger Value 80%** for our example.
11. Select a condition to **Reset Alert when % CPU Utilization**, and then enter the reset value: **Reset Value 80%** for our example.
12. *If you want to set timeframe parameters*, use the **Time of Day** tab.
13. Click **Alert Suppression**.
14. Select **Suppress this alert if ANY of the selected suppressions are active**.
Note: Any previously configured alerts will be listed, unchecked.
15. Click **Add**.
16. Click **Property to Monitor**.
17. Check **Node Statistics > % CPU Utilization**.
18. Click **Network Object**.
19. Check the second server of the pair whose load should be balanced.
20. Click **Suppression Trigger**.
21. Select **Greater Than**.
22. Type **40** in the text-entry field, and then click **OK**.

23. Check the suppression that you just defined to activate it.
24. Repeat the procedure, reversing the server choices made for alerting and suppression.

Advanced Alert Engine Variables

The following variables can be used in alert messages within Orion NPM and Orion Modules. You must begin each variable with a dollar sign and enclose each variable identifier in braces as, for example, `${ObjectName}`.

General

The following are valid, general advanced alert variables.

General Variable	Description
<code>\${Acknowledged}</code>	Acknowledged status
<code>\${AcknowledgedBy}</code>	Who the alert was acknowledged by
<code>\${AcknowledgedTime}</code>	Time the alert was acknowledged
<code>\${AlertTriggerCount}</code>	Count of triggers
<code>\${AlertTriggerTime}</code>	Date and time of the last event for this Alert. (Windows control panel defined "Short Date" and "Short Time")
<code>\${Application}</code>	SolarWinds application information
<code>\${CR}</code>	Line Feed – Carriage Return
<code>\${Copyright}</code>	Copyright information
<code>\${ObjectName}</code>	Description/Name of the object in the alert
<code>\${Release}</code>	Release information
<code>\${Version}</code>	Version of the SolarWinds software package

Universal Device Poller

The following are valid Universal Device Poller variables.

Universal Device Poller Variable	Description
<code>\${DateTime}</code>	Date/Time
<code>\${Description}</code>	Description of the Universal Device Poller
<code>\${Enabled}</code>	Enabled status of the Universal Device Poller
<code>\${MIB}</code>	MIB
<code>\${OID}</code>	OID
<code>\${Rate}</code>	Rate
<code>\${Status}</code>	Status
<code>\${Total}</code>	Total
<code>\${UniqueName}</code>	Name of the Universal Device Poller

Date/Time

The following are valid date and time variables.

Date/Time Variable	Description
#{AMPM}	AM/PM indicator
#{AbbreviatedDOW}	Current day of the week. Three character abbreviation.
#{D}	Current day of the month
#{DD}	Current day of the month (two digit number, zero padded)
#{Date}	Current date. (Short Date format)
#{DateTime}	Current date and time. (Windows control panel defined "Long Date" and "Long Time" format)
#{DayOfWeek}	Current day of the week.
#{DayOfYear}	Numeric day of the year
#{H}	Current hour
#{HH}	Current hour. Two digit format, zero padded.
#{Last2Hours}	Last two hours
#{Last24Hours}	Last 24 hours
#{Last7Days}	Last seven days (Short Date format)
#{LastHour}	Last hour
#{LocalDOW}	Current day of the week. Localized language format.
#{LocalMonthName}	Current month name in the local language.
#{LongDate}	Current date. (Long Date format)
#{M}	Current numeric month
#{MM}	Current month. Two digit number, zero padded.
#{MMM}	Current month. Three character abbreviation.
#{MMMM}	Full name of the current month
#{MediumDate}	Current date. (Medium Date format)
#{Minute}	Current minute. Two digit format, zero padded.
#{S}	Current second.
#{Second}	Current second. Two digit format, zero padded.
#{Time}	Current Time. (Short Time format)
#{Today}	Today (Short Date format)
#{Year}	Four digit year
#{Year2}	Two digit year
#{Yesterday}	Yesterday (Short Date format)

SQL Query

Any value you can collect from the database can be generated, formatted, or calculated using a SQL query as a variable. To use a SQL query as a variable in Orion NPM, use ``${SQL:{query}}`` as shown in the following example that returns the results of the SQL query `Select Count(*) From Nodes:`

```
`${SQL:Select Count(*) From Nodes}
```

Node Status Variables

When using the ``${Status}`` variable with a node, status values are returned. The following table provides a description for each status value.

Status Value	Description
0	Unknown
1	Up
2	Down
3	Warning
4	Shutdown
5	Testing
6	Dormant
7	Not Present
8	Lower Layer Down
9	Unmanaged
10	Unplugged
11	External
12	Unreachable
14	Critical
15	Mixed Availability
16	Misconfigured
17	Could Not Poll
19	Unconfirmed
22	Active
24	Inactive
25	Expired
26	Monitoring Disabled
27	Disabled
28	Not Licensed

Interface Poller Variables

The following are valid interface poller variables.

Note: At least one of the `CustomPollerStatus` variables from the tables below must be included in the trigger condition of all interface poller alerts.

Interface Poller Assignment Variable	Description
<code>\${AssignmentName}</code>	User friendly name of a specific assignment in the form: <code><PollerName> - <NodeName> - <InterfaceName></code> . Interface name is '0' if this is a node poller.
<code>\${CustomPollerAssignmentID}</code>	Internal unique ID (as guid) of specific assignment of a poller to a node or interface.
<code>\${InterfaceID}</code>	Internal unique ID of interface (as integer) in this assignment. '0' if this is a node poller.
<code>\${NodeID}</code>	Internal unique ID of node (as integer) in this assignment.
<code>\${PollerID}</code>	Internal unique ID of poller (as guid) in this specific assignment

Interface Poller Status Variable	Description
<code>\${CustomPollerAssignmentID}</code>	Internal unique ID (as guid) of the specific assignment of a poller to a node or interface.
<code>\${DateTime}</code>	Date and time statistic was last collected for this assignment.
<code>\${DateTimeUTC}</code>	Date and time statistics were last collected for this assignment (universal time)
<code>\${Rate}</code>	For a poller with a MIB value type of 'Rate', this field contains numeric data collected from the OID. For a poller with a MIB value type of 'Counter', this field contains the change in the previous value as normalized to the polling interval. For a poller with a MIB value of 'Raw Value' this field is null.
<code>\${RawStatus}</code>	For poller with a MIB value type 'Rate' or 'Counter', this field is null. For a poller with MIB value 'Raw Value' and an OID response value that is numeric, this field contains the numeric value. For a poller with MIB value 'Raw Value' and an OID response value that is not numeric, this field is null. For enumerations this field contains the actual numeric value returned from the OID instead of the user friendly text. Status comparisons that are numeric (greater than and less than) should use this field. Status values that are text descriptions should use the 'Status' field.
<code>\${Status}</code>	For a poller with a MIB value type of 'Rate' or 'Counter', this field is null. For a poller with a MIB value of 'Raw Value' this field contains the value from the OID 'cooked' according to its sub-type. Enumerations contain user friendly text instead of a numeric value returned from the OID.

Interface Poller Status Variable	Description
\$(Total)	For a poller with a MIB value type of 'Rate', this field is null. For a poller with a MIB value type of 'Counter' this field contains the change in the previously collected value. For a poller with a MIB value of 'Raw Value' this field is null.

Note: Rate pollers only write to the 'Rate' field; counter pollers only write to the 'Total' and 'Rate' fields; and status pollers only write to the 'Status' field, unless they can be successfully converted to a numeric value, in which case the numeric value is also written to the 'RawStatus' field.

Interface Poller Variable	Description
\$(DefaultDisplayTimeUnitID)	Internal unique ID of time units as represented by UI
\$(Description)	Poller description
\$(Enabled)	(1) indicates poller currently up and collecting, otherwise (0)
\$(Format)	Currently unused
\$(GroupName)	User friendly name of group to which this poller belongs
\$(IncludeHistoricStatistics)	(1) indicates that every statistic collection is inserted as a new record. (0) indicates that this statistic is updated so that it only has one statistic record.
\$(LastChange)	Date and time that poller record last changed
\$(LastChangeUTC)	Date and time that poller record last changed (universal time)
\$(MIB)	Generally recognized OID name
\$(NetObjectPrefix)	(N) if this is a node poller. (I) if this is an interface poller
\$(OID)	OID used to gather information
\$(ParserID)	Internal unique ID of the parser (sub-type) of this poller, where 1=None, 2=text, 3=enum, 4=macAddress, 5=counter, 6=gauge, 10=TrueFalse, 11=FalseTrue, 12=CleanMac, 14=TimeTicks, 15=HighBandwidth, 16=AdminStatus, 17=OperationalStatus
\$(PollerID)	Poller unique ID (guid)
\$(PollerType)	(R) for rate poller, (C) for counter poller, (S) for status poller
\$(SNMPGetType)	SNMP request type (Get or GetNext)
\$(TimeUnitID)	Internal unique ID of time unit (msec/sec/min/hr/days) to which poller is normalizing
\$(TimeUnitQuantity)	Number of time units to which poller is normalizing
\$(UniqueName)	Poller user friendly name
\$(Unit)	User-entered description of unit collected (bytes/degrees/dbs)

Node Poller Variables

The following are valid node poller variables.

Note: At least one of the `CustomPollerStatus` alerts from the table below must be included in the trigger condition of any and all Node Poller alerts.

Node Poller Assignment Variable	Description
<code>\${AssignmentName}</code>	User friendly name of a specific assignment in the form: <code><PollerName> - <NodeName> - <InterfaceName></code> . Interface name is '0' if this is a node poller
<code>\${CustomPollerAssignmentID}</code>	Internal unique ID (as guid) of specific assignment of a poller to a node or interface.
<code>\${InterfaceID}</code>	Internal unique ID of interface (as integer) in this assignment. '0' if this is a node poller
<code>\${NodeID}</code>	Internal unique ID of node (as integer) in this assignment
<code>\${PollerID}</code>	Internal unique ID of poller (as guid) in this specific assignment

Node Poller Status Variable	Description
<code>\${CustomPollerAssignmentID}</code>	Internal unique ID (as guid) of the specific assignment of a poller to a node or interface.
<code>\${DateTime}</code>	Date and time statistic was last collected for this assignment
<code>\${DateTimeUTC}</code>	Date and time statistics were last collected for this assignment (universal time)
<code>\${Rate}</code>	For a poller with a MIB value type of 'Rate', this field contains numeric data collected from the OID. For a poller with a MIB value type of 'Counter', this field contains the change in the previous value as normalized to the polling interval. For a poller with a MIB value of 'Raw Value' this field is null.
<code>\${RawStatus}</code>	For poller with a MIB value type 'Rate' or 'Counter', this field is null. For poller with MIB value 'Raw Value' and an OID response value that is numeric, this field contains the numeric value. For a poller with MIB value 'Raw Value' and an OID response value that is not numeric, this field is null. For enumerations this field contains the actual numeric value returned from the OID instead of the user friendly text. Status comparisons that are numeric (greater than and less than) should use this field. Status values that are text descriptions should use the 'Status' field.
<code>\${Status}</code>	For a poller with a MIB value type of 'Rate' or 'Counter', this field is null. For a poller with a MIB value of 'Raw Value' this field contains the value from the OID 'cooked' according to its sub-type. Enumerations contain user friendly text instead of a numeric value returned from the OID.

Node Poller Status Variable	Description
\$(Total)	For a poller with a MIB value type of 'Rate', this field is null. For a poller with a MIB value type of 'Counter' this field contains the change in the previously collected value. For a poller with a MIB value of 'Raw Value' this field is null.

Note: Rate pollers only write to the 'Rate' field; counter pollers only write to the 'Total' and 'Rate' fields; and status pollers only write to the 'Status' field, unless they can be successfully converted to a numeric value, in which case the numeric value is also written to the 'RawStatus' field.

Node Poller Variable	Description
\$(DefaultDisplayTimeUnitID)	Internal unique ID of time units as represented by UI
\$(Description)	Poller description
\$(Enabled)	(1) indicates poller currently up and collecting, otherwise (0)
\$(Format)	Currently unused
\$(GroupName)	User friendly name of group to which this poller belongs
\$(IncludeHistoricStatistics)	(1) indicates that every statistic collection is inserted as a new record. (0) indicates that this statistic is updated so that it only has one statistic record.
\$(LastChange)	Date and time that poller record last changed
\$(LastChangeUTC)	Date and time that poller record last changed (universal time)
\$(MIB)	Generally recognized OID name
\$(NetObjectPrefix)	(N) if this is a node poller. (I) if this is an interface poller
\$(OID)	OID used to gather information
\$(ParserID)	Internal unique ID of the parser (sub-type) of this poller, where 1=None, 2=text, 3=enum, 4=macAddress, 5=counter, 6=gauge, 10=TrueFalse, 11=FalseTrue, 12=CleanMac, 14=TimeTicks, 15=HighBandwidth, 16=AdminStatus, 17=OperationalStatus
\$(PollerID)	Poller unique ID (guid)
\$(PollerType)	(R) for rate poller, (C) for counter poller, (S) for status poller
\$(SNMPGetType)	SNMP request type (Get or GetNext)
\$(TimeUnitID)	Internal unique ID of time unit (msec/sec/min/hr/days) to which poller is normalizing
\$(TimeUnitQuantity)	Number of time units to which poller is normalizing
\$(UniqueName)	Poller user friendly name
\$(Unit)	User-entered description of unit collected (bytes/degrees/dbs)

Interface Variables

The following are valid interface variables.

Interface Variable	Description
`\${AdminStatus}`	Numeric administrative status of interface. For more information, see “Node Status Variables” on page 323.
`\${AdminStatusLED}`	Filename of current interface administrative status icon
`\${Caption}`	User friendly description of interface combining name with other identifying information
`\${Counter64}`	States if interface supports IF-MIB high capacity counters
`\${CustomBandwidth}`	Indicates if transmit and receive bandwidth fields are user-controlled (1) or controlled by automated detection via ifSpeed MIB (0)
`\${CustomPollerLastStatisticsPoll}`	Day, date, and time that this interface was last polled by the current poller
`\${FullName}`	User friendly name combining captions of parent node and interface
`\${IfName}`	Internal name discovered for this interface with the ifName OID
`\${InterfaceID}`	Internal unique identifier of selected interface
`\${InBandwidth}`	Incoming bandwidth of interface
`\${Inbps}`	Current incoming traffic, in bps, to interface
`\${InDiscardsThisHour}`	Number of incoming packets discarded by interface in last hour
`\${InDiscardsToday}`	Number of incoming packets discarded by interface in current day
`\${InErrorsThisHour}`	Number of interface receive errors in last hour
`\${InErrorsToday}`	Number of interface receive errors in current day
`\${InMcastPps}`	Current incoming multicast traffic, in packets per second, to interface
`\${InPercentUtil}`	Current percent utilization of interface receive
`\${InPktSize}`	Average size of incoming packets to interface
`\${InPps}`	Current incoming traffic, in packets per second, to interface
`\${InterfaceAlias}`	Alias or description of interface discovered from parent node
`\${InterfaceIcon}`	Filename of the icon used to represent the interface type
`\${InterfaceIndex}`	Index of selected interface on parent node
`\${InterfaceLastChange}`	sysUpTime value when the interface entered current operational state
`\${InterfaceMTU}`	Interface Maximum Transfer Unit: the largest packet the interface can handle
`\${InterfaceName}`	User friendly name

Interface Variable	Description
<code>#{InterfaceSpeed}</code>	Interface bandwidth
<code>#{InterfaceType}</code>	IANA type of selected interface
<code>#{InterfaceTypeDescription}</code>	User friendly description of interface type
<code>#{InterfaceTypeName}</code>	User friendly name of interface IANA type
<code>#{InUcastPps}</code>	Current incoming unicast traffic, in packets per second, to interface
<code>#{LastSync}</code>	Time and date of last interface database and memory synchronization
<code>#{NextPoll}</code>	Day, date and time of next scheduled interface polling
<code>#{NextRediscovery}</code>	Next interface rediscovery time
<code>#{NodeID}</code>	Internal unique identifier of node that is parent to the selected interface
<code>#{ObjectSubType}</code>	States if parent node supports SNMP or is ICMP only
<code>#{OperStatusLED}</code>	Filename of current interface operational status icon
<code>#{OutBandwidth}</code>	Outgoing bandwidth of interface
<code>#{Outbps}</code>	Current outgoing traffic, in bps, from interface
<code>#{OutDiscardsThisHour}</code>	Number of outgoing packets discarded by interface in last hour
<code>#{OutDiscardsToday}</code>	Number of outgoing packets discarded by interface in current day
<code>#{OutErrorsThisHour}</code>	Number of interface transmit errors in last hour
<code>#{OutErrorsToday}</code>	Number of interface transmit errors in current day
<code>#{OutMcastPps}</code>	Current outgoing multicast traffic, in packets per second, from interface
<code>#{OutPercentUtil}</code>	Current percent utilization of interface transmit
<code>#{OutPktSize}</code>	Average size of outgoing packets from interface
<code>#{OutPps}</code>	Current outgoing traffic, from interface, in pps
<code>#{OutUcastPps}</code>	Current outgoing unicast traffic, in packets per second, from interface
<code>#{PhysicalAddress}</code>	Physical address of interface
<code>#{PollInterval}</code>	Interval, in seconds, between polling attempts for interface
<code>#{RediscoveryInterval}</code>	Interval, in minutes, between rediscovery attempts for interface
<code>#{Severity}</code>	A network health score providing 1 point for an interface in a warning state, 1000 points for a down interface, and 1 million points for a down node
<code>#{StatCollection}</code>	Interface statistics collection frequency, in minutes
<code>#{Status}</code>	Numeric interface status. For more information, see "Node Status Variables" on page 323.
<code>#{StatusLED}</code>	Filename of current interface status icon

Node Variables

The following are valid node variables.

Node Variable	Description
`\${AgentPort}`	Node SNMP port number
`\${Allow64BitCounters}`	Node allows 64-bit counters (1), or not (0)
`\${AvgResponseTime}`	Average node response time , in msec, to ICMP requests
`\${BlockUntil}`	Day, date, and time until which node polling is blocked
`\${BufferBgMissThisHour}`	Device-dependent count of big buffer misses on node in current hour, queried with MIB 1.3.6.1.4.9.2.1.30
`\${BufferBgMissToday}`	Device-dependent count of big buffer misses on node in current day, queried with MIB 1.3.6.1.4.9.2.1.30
`\${BufferHgMissThisHour}`	Device-dependent count of huge buffer misses on node in current hour, queried with MIB 1.3.6.1.4.9.2.1.62
`\${BufferHgMissToday}`	Device-dependent count of huge buffer misses on node in current day, queried with MIB 1.3.6.1.4.9.2.1.62
`\${BufferLgMissThisHour}`	Device-dependent count of large buffer misses on node in current hour, queried with MIB 1.3.6.1.4.9.2.1.38
`\${BufferLgMissToday}`	Device-dependent count of large buffer misses on node in current day, queried with MIB 1.3.6.1.4.9.2.1.38
`\${BufferMdMissThisHour}`	Device-dependent count of medium buffer misses on node in current hour, queried with MIB 1.3.6.1.4.9.2.1.22
`\${BufferMdMissToday}`	Device-dependent count of medium buffer misses on node in current day, queried with MIB 1.3.6.1.4.9.2.1.22
`\${BufferNoMemThisHour}`	Count of buffer errors due to low memory on node in current hour
`\${BufferNoMemToday}`	Count of buffer errors due to low memory on node in current day
`\${BufferSmMissThisHour}`	Device-dependent count of small buffer misses on node in current hour, queried with MIB 1.3.6.1.4.9.2.1.14
`\${BufferSmMissToday}`	Device-dependent count of small buffer misses on node in current day, queried with MIB 1.3.6.1.4.9.2.1.14
`\${Caption}`	User friendly node name
`\${Community}`	Node community string

Node Variable	Description
#{Contact}	Contact information for person or group responsible for node
#{CPULoad}	Node CPU utilization rate at last poll
#{CustomPollerLastStatisticsPoll}	Day, date, and time of last poll attempt on node
#{CustomPollerLastStatisticsPollSuccess}	Day, date, and time that node was last successfully polled
#{Description}	Node hardware and software
#{DNS}	Fully qualified node name
#{DynamicIP}	If node supports dynamic IP address assignment via BOOTP or DHCP (1); static IP address return (0)
#{EngineID}	Internal unique identifier of the polling engine to which node is assigned
#{GroupStatus}	Filename of status icon for node and its interfaces
#{IOSImage}	Family name of Cisco IOS on node
#{IOSVersion}	Cisco IOS version on node
#{IP_Address}	Node IP address
#{LastBoot}	Day, date and time of last node boot
#{LastSync}	Time and date of last node database and memory synchronization
#{Location}	Physical location of node
#{MachineType}	Node manufacturer or distributor and family or version information
#{MaxResponseTime}	Maximum node response time , in msec, to ICMP requests
#{MemoryUsed}	Total node memory used over polling interval
#{MinResponseTime}	Minimum node response time , in msec, to ICMP requests
#{NextPoll}	Day, date and time of next scheduled node polling
#{NextRediscovery}	Time of next node rediscovery
#{NodeID }	Internal unique identifier of node
#{ObjectSubType}	States if node supports SNMP or is ICMP-only
#{PercentLoss}	ICMP packet loss percentage when node last polled
#{PercentMemoryUsed}	Percentage of total node memory used over polling interval
#{PollInterval}	Node polling interval, in seconds
#{RediscoveryInterval}	Node rediscovery interval, in minutes
#{ResponseTime}	Node response time, in milliseconds, to last ICMP request

Node Variable	Description
#{RWCommunity}	Node read/write community string; acts as security code for read/write SNMP access
#{RWSNMPV3AuthKey}	SNMPv3 read/write credential authentication key
#{RWSNMPV3AuthKeyIsPwd}	States if the SNMPv3 read/write credential authentication key is the password
#{RWSNMPV3AuthMethod}	SNMPv3 read/write credential authentication method
#{RWSNMPV3Context}	SNMPv3 read/write security context information
#{RWSNMPV3PrivKey}	SNMPv3 read/write credential key
#{RWSNMPV3PrivKeyIsPwd}	States if the SNMPv3 read/write credential privacy key is the password
#{RWSNMPV3PrivMethod}	SNMPv3 read/write credential privacy encryption method
#{RWSNMPV3Username}	User friendly name for SNMPv3 read/write credential
#{Severity}	A network health score providing 1 point for an interface in a warning state, 1000 points for a down interface, and 1 million points for a down node.
#{SNMPV2Only}	States if node only supports SNMPv1 or SNMPv2
#{SNMPV3AuthKey}	SNMPv3 authentication key
#{SNMPV3AuthKeyIsPwd}	States if node SNMPv3 authentication key is password
#{SNMPV3AuthMethod}	SNMPv3 authentication type
#{SNMPV3Context}	Group or domain of user with SNMPv3 access to node
#{SNMPV3PrivKey}	SNMPv3 credential key
#{SNMPV3PrivKeyIsPwd}	States if node SNMPv3 credential key is the password
#{SNMPV3PrivMethod}	SNMPv3 credential key type
#{SNMPV3Username}	User friendly name for SNMPv3 credential
#{SNMPVersion}	States the version of SNMP used by the node
#{StatCollection}	Statistics collection frequency, in minutes
#{Status}	Numerical node status. For more information, see "Node Status Variables" on page 323.
#{StatusDescription}	User friendly node status
#{StatusLED}	Filename of node status icon
#{SysName}	String reply to SNMP SYS_NAME OID request
#{SysObjectID}	Vendor ID of the network management subsystem in OID form. Clearly determines the type of node.

Node Variable	Description
`\${SystemUpTime}`	Time, in hundredths of a second, since network monitoring started
`\${TotalMemory}`	Total node memory available
`\${UnManaged}`	States if node is currently unmanaged
`\${UnManageFrom}`	Day, date, and time when node is set to "Unmanaged"
`\${UnManageUntil}`	Day, date, and time when node is scheduled to be managed
`\${Vendor}`	Node manufacturer or distributor
`\${VendorIcon}`	Filename of node vendor logo

Volume Variables

The following are valid volume variables.

Volume Variable	Description
`\${Caption}`	User friendly volume name
`\${FullName}`	User friendly volume name including captions of parent node and interface
`\${LastSync}`	Time and date volume last synchronized in database and memory models
`\${NextPoll}`	Day, date and time of next scheduled volume polling
`\${NextRediscovery}`	Scheduled time of next volume rediscovery
`\${NodeID}`	Internal unique identifier of parent node
`\${PollInterval}`	Volume status polling interval, in seconds
`\${RediscoveryInterval}`	Volume rediscovery interval, in minutes
`\${StatCollection}`	Statistics collection frequency, in minutes
`\${Status}`	Numerical volume status: (0="Unknown", 1="Up", 2="Shutdown", 3="Testing")
`\${StatusLED}`	Filename of volume status icon
`\${VolumeAllocationFailuresThisHour}`	Number of volume allocation errors for this volume in last hour
`\${VolumeAllocationFailuresToday}`	Number of volume allocation errors for this volume in current day
`\${VolumeDescription}`	User friendly volume description
`\${VolumeID}`	Internal unique identifier of volume
`\${VolumeIndex}`	Unique index of this volume within the parent node
`\${VolumePercentUsed}`	Percentage of volume currently in use
`\${VolumeResponding}`	(Y) = volume is currently responding to SNMP queries
`\${VolumeSize}`	Size of volume, in bytes
`\${VolumeSpaceAvailable}`	Total space available on volume, in bytes
`\${VolumeSpaceUsed}`	Total space used on volume, in bytes

Volume Variable	Description
#{VolumeType}	Volume type, as reported by hrStorageType OID (Removable Disk/Fixed Disk/Compact Disc/Virtual Memory/RAM/etc)
#{VolumeTypeIcon}	Filename of icon for volume type

Wireless Node Variables

The following are valid wireless node variables.

Wireless Node Variable	Description
#{WirelessAP}	States if node is being polled by the wireless poller (1) or not (0)
#{WirelessLastStatPoll}	Date and time node last polled by wireless poller
#{WirelessPollInterval}	Interval, in minutes, between wireless polling attempts on node
#{WirelessStatBlockUntil}	Date and time node may be polled again by wireless poller

Syslog Alert Variables

The following variables can be used in Syslog alert messages within Orion Network Performance Monitor applications. You must begin each variable with a dollar sign and enclose each variable identifier in curly braces as, for example, #{ObjectName}.

Syslog Date/Time Variables

Syslog Date/Time Variable	Description
#{AbbreviatedDOW}	Current day of the week. Three character abbreviation.
#{AMPM}	AM or PM corresponding to current time (before or after noon)
#{D}	Current day of the month
#{DD}	Current day of the month (two digit number, zero padded)
#{Date}	Current date. (Short Date format)
#{DateTime}	Current date and time. (Windows control panel defined "Short Date" and "Short Time" format)
#{DayOfWeek}	Current day of the week.
#{DayOfYear}	Numeric day of the year
#{H}	Current hour
#{HH}	Current hour. Two digit format, zero padded.
#{Hour}	Current hour. 24-hour format
#{LocalDOW}	Current day of the week. Localized language format.
#{LongDate}	Current date. (Long Date format)
#{LocalMonthName}	Current month name in the local language.
#{LongTime}	Current Time. (Long Time format)

Syslog Date/Time Variable	Description
#{M}	Current numeric month
#{MM}	Current month. Two digit number, zero padded.
#{MMM}	Current month. Three character abbreviation.
#{MediumDate}	Current date. (Medium Date format)
#{Minute}	Current minute. Two digit format, zero padded.
#{Month}	Full name of the current month
#{N}	Current month and day
#{S}	Current second.
#{Second}	Current second. Two digit format, zero padded.
#{Time}	Current Time. (Short Time format)
#{Year2}	Two digit year
#{Year}	Four digit year

Other Syslog Variables

Syslog Variable	Description
#{Application}	SolarWinds application information
#{Copyright}	Copyright information
#{DNS}	Fully qualified node name
#{IP_Address}	IP address of device triggering alert
#{Message}	Status of device triggering alert
#{MessageType}	Assigned alert name
#{Release}	Release information
#{Severity}	A network health score providing 1 point for an interface in a warning state, 1000 points for a down interface, and 1 million points for a down node.
#{Version}	Version of the SolarWinds software package

Trap Alert Variables

The following variables can be used in trap alert messages within Orion Network Performance Monitor applications. You must begin each variable with a dollar sign and enclose each variable identifier in curly braces as, for example, `#{ObjectName}`.

Trap Date/Time Variables

Trap Date/Time Variable	Description
#{AbbreviatedDOW}	Current day of the week. Three character abbreviation.
#{AbbreviatedMonth}	Current month of the year. Three character abbreviation.

Trap Date/Time Variable	Description
\${AMPM}	AM or PM corresponding to current time (before or after noon)
\${D}	Current day of the month
\${DD}	Current day of the month (two digit number, zero padded)
\${Date}	Current date. (MM/DD/YYYY format)
\${DateTime}	Current date and time. (MM/DD/YYYY HH:MM format)
\${Day}	Current day of the month
\${DayOfWeek}	Current day of the week.
\${DayOfYear}	Numeric day of the year
\${H}	Current hour
\${HH}	Current hour. Two digit format, zero padded.
\${Hour}	Current hour. 24-hour format
\${LocalDOW}	Current day of the week. Localized language format.
\${LongDate}	Current date. (DAY NAME, MONTH DAY, YEAR format)
\${LongTime}	Current Time. (HH:MM:SS AM/PM format)
\${M}	Current numeric month
\${MM}	Current month. Two digit number, zero padded.
\${MMM}	Current month. Three character abbreviation.
\${MMMM}	Full name of the current month
\${MediumDate}	Current date. (DD-MMM-YY format)
\${MediumTime}	Current time. (HH:MM AM/PM format)
\${Minute}	Current minute. Two digit format, zero padded.
\${MonthName}	Full name of the current month
\${S}	Current second.
\${Second}	Current second. Two digit format, zero padded.
\${Time}	Current Time. (HH:MM format)
\${Year}	Four digit year
\${Year2}	Two digit year

Other Trap Variables

Trap Variable	Description
\${Application}	SolarWinds application information
\${Community}	Node community string
\${Copyright}	Copyright information
\${DNS}	Fully qualified node name
\${Hostname}	Host name of the device triggering the trap
\${IP}	IP address of device triggering alert
\${IP_Address}	IP address of device triggering alert

Trap Variable	Description
\${Message}	Message sent with triggered trap and displayed in Trap Details field of Trap Viewer
\${MessageType}	Name or type of trap triggered
\${Raw}	Raw numerical values for properties sent in the corresponding incoming trap
\${RawValue}	Raw numerical values for properties sent in the corresponding incoming trap. The same as \${Raw}

Appendix D

95th Percentile Calculations

Calculation of the 95th percentile, a well-known statistical standard used to discard maximum spikes, is based on 5 minute data samples. The calculation gathers these values every 5 minutes for however long you select, throws away the top 5%, yielding the 95th percentile value at the beginning of the list.

Consider the following example of how the 95th percentile is calculated for a 10 hour work day from 8am to 6pm (600 minutes):

1. Over the 10 hours, the following 120 values were collected for inbound traffic (Mb/s):

```
0.149 0.623 0.281 0.136 0.024 0.042 0.097 0.185 0.198 0.243 0.274 0.390
0.971 0.633 0.238 0.142 0.119 0.176 0.131 0.127 0.169 0.223 0.291 0.236
0.124 0.072 0.197 0.105 0.138 0.233 0.374 0.290 0.871 0.433 0.248 0.242
0.169 0.116 0.121 0.427 0.249 0.223 0.231 0.336 0.014 0.442 0.197 0.125
0.108 0.244 0.264 0.190 0.471 0.033 0.228 0.942 0.219 0.076 0.331 0.227
0.849 0.323 0.221 0.196 0.223 0.642 0.197 0.385 0.098 0.263 0.174 0.690
0.571 0.233 0.208 0.242 0.139 0.186 0.331 0.124 0.249 0.643 0.481 0.936
0.124 0.742 0.497 0.085 0.398 0.643 0.074 0.590 0.771 0.833 0.438 0.242
0.092 0.376 0.231 0.627 0.249 0.663 0.181 0.636 0.224 0.342 0.697 0.285
0.108 0.211 0.074 0.490 0.271 0.133 0.338 0.242 0.519 0.376 0.331 0.227
```

2. When reordered from high to low:

```
0.971 0.942 0.936 0.871 0.849 0.833 0.771 0.742 0.697 0.690 0.663 0.643
0.643 0.642 0.636 0.633 0.627 0.623 0.590 0.571 0.519 0.497 0.490 0.481
0.471 0.442 0.438 0.433 0.427 0.398 0.390 0.385 0.376 0.376 0.374 0.342
0.338 0.336 0.331 0.331 0.331 0.323 0.291 0.290 0.285 0.281 0.274 0.271
0.264 0.263 0.249 0.249 0.249 0.248 0.244 0.243 0.242 0.242 0.242 0.242
0.238 0.236 0.233 0.233 0.231 0.231 0.228 0.227 0.227 0.224 0.223 0.223
0.223 0.221 0.219 0.211 0.208 0.198 0.197 0.197 0.197 0.196 0.190 0.186
0.185 0.181 0.176 0.174 0.169 0.169 0.149 0.142 0.139 0.138 0.136 0.133
0.131 0.127 0.125 0.124 0.124 0.124 0.121 0.119 0.116 0.108 0.108 0.105
0.098 0.097 0.092 0.085 0.076 0.074 0.074 0.072 0.042 0.033 0.024 0.014
```

3. Drop the first 6, as these equal the top 5% of the values:

```
0.771 0.742 0.697 0.690 0.663 0.643 0.643 0.642 0.636 0.633 0.627 0.623
0.590 0.571 0.519 0.497 0.490 0.481 0.471 0.442 0.438 0.433 0.427 0.398
0.390 0.385 0.376 0.376 0.374 0.342 0.338 0.336 0.331 0.331 0.331 0.323
0.291 0.290 0.285 0.281 0.274 0.271 0.264 0.263 0.249 0.249 0.249 0.248
0.244 0.243 0.242 0.242 0.242 0.238 0.236 0.233 0.233 0.231 0.231
```

0.228 0.227 0.227 0.224 0.223 0.223 0.223 0.221 0.219 0.211 0.208 0.198
0.197 0.197 0.197 0.196 0.190 0.186 0.185 0.181 0.176 0.174 0.169 0.169
0.149 0.142 0.139 0.138 0.136 0.133 0.131 0.127 0.125 0.124 0.124 0.124
0.121 0.119 0.116 0.108 0.108 0.105 0.098 0.097 0.092 0.085 0.076 0.074
0.074 0.072 0.042 0.033 0.024 0.014

- 4. The 95th percentile is **0.771**.

Appendix E

Configuring Automatic Login

The Orion Network Performance Monitor Web Console allows you to log in automatically, using Windows Pass-through Security, DirectLink, or URL Pass-through.

If you choose to employ Windows Pass-through Security, Orion NPM users can be authenticated through Windows Security, with no need to log in using a separate Orion NPM Account or User ID and Password. With the presence of the DirectLink account, any URL that refers directly to an Orion Network Performance Monitor web page will bypass the Orion Network Performance Monitor Login Page by logging the user into the DirectLink account.

Note: When authenticating users with Windows Security, ensure your Orion server uses the NetBIOS domain name and not the fully qualified domain name.

Orion NPM prioritizes user login in the following manner:

1. The Account or User ID and Password passed on the URL.
2. The Account or User ID and Password entered on the login.aspx page.
3. The Windows User if IIS NT Security is enabled, logging the user in using NT Security.
4. The Windows Domain to which the User belongs, for example, `Development\Everyone`.
5. The presence of a DirectLink Account.

Passing Login Information Using URL Parameters

The user ID and password can be passed as parameters within the URL. This allows you to create a favorite or bookmark within a browser, or on your desktop. Create a favorite with a link in the following form to pass the login information:

```
http://DOMAIN/Orion/Login.aspx?AccountID=USER&Password=PASSWORD
```

Provide the hostname or IP address of your Orion server as the `DOMAIN`. Provide your Orion User ID as the `USER`, and then provide your Orion user account password as the `PASSWORD`.

Warning: HTTP requests are not encrypted, so User IDs and Passwords sent in HTTP requests are not secure. For more information about enabling HTTPS on your Orion server, consult www.microsoft.com.

Using Windows Pass-through Security

You may take advantage of the Windows Pass-through Security functionality when IIS NT Security is enabled. Orion NPM users can be authenticated through Windows Security, with no need to log in using a separate Orion NPM account or User Id and Password. Pass-through Security can be configured to employ either Domain or Local computer security. Both may also be used at the same time. The Orion Network Performance Monitor Account or User ID and Passwords must then be set up to match the Account or User ID and Passwords that are used for the Domain and/or Local computer security. Use the following procedure to enable IIS NT Security for logging in to the Orion Web Console with Windows Pass-through Security.

Notes:

- Select **Logout** from the Orion NPM menu bar and log in as the other user.
- When authenticating users with Windows Security, ensure your Orion server uses the NetBIOS domain name, instead of the fully qualified domain name.

To enable IIS NT security for Windows Pass-through Security:

1. ***If you are using NT Domain Authentication Format for pass-through accounts***, create these accounts in the Orion Web Console Account Manager using *Domain\UserID* as the **User Name**, as follows:

- Washington\Edward
- StLouis\Everyone

Note: Currently, the only domain group supported by the Orion Web Console is the 'Everyone' group. For more information about creating accounts using the Orion Web Console Account Manager, see "Creating New Accounts" on page 91.

2. ***If you are using Local Computer Authentication Format for pass-through accounts***, create these accounts in the Orion Web Console Account Manager using *Computer\UserID* as the **User Name**, as follows:

- SolarWindsS2\Edward
- Server3\JonesR

Note: For more information about creating accounts using the Orion Web Console Account Manager, see "Creating New Accounts" on page 91.

3. Click **Start > Control Panel > Administrative Tools > Internet Information Services (IIS) Manager**.

4. **If you are using Windows Server 2003**, complete the following steps:
 - a. Expand **Internet Information Services** > *Local Computer* > **Web Sites** in the left pane.
 - b. Select **SolarWinds NetPerfMon**.
 - c. Click **Action** > **Properties**.
 - d. Click the Directory Security tab.
 - e. Click **Edit** within the **Authentication and access control** area.
 - f. Clear **Enable anonymous access**.
 - g. Check **Integrated Windows authentication** in the Authenticated access group.
 - h. Click **OK** to close the Authentication Methods window.
 - i. Click **Apply**, if available, and then click **OK** to close the SolarWinds NetPerfMon Properties window.
 - j. Collapse **Internet Information Services** > *Local Computer* > **Web Sites**.
 - k. Collapse **Internet Information Services** > *Local Computer* in the left pane.
 - l. Click **Action** > **All Tasks** > **Restart IIS**.
 - m. Confirm that **Restart Internet Services on Local Computer** is selected, and then click **OK**.
 - n. Close the IIS Manager.
5. **If you are using Windows Server 2008**, complete the following steps:
 - a. Click **Start** > **Administrative Tools** > **Server Manager**.
 - b. Expand **Roles**.
 - c. Click **Web Server (IIS)**.
 - d. In the Role Services area, confirm that Web Server > Security > Windows Authentication is installed.
 - e. **If Windows Authentication is not installed**, click **Add Role Services**, check **Web Server > Security > Windows Authentication**, click **Next**, and then complete the service installation.
 - f. Click **Start** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.
 - g. Select your Orion server in the left pane.
 - h. Click **Authentication** in the IIS group of the main pane.

- i. Right-click **Anonymous Authentication**, and then click **Disable**.
 - j. Right-click **Windows Authentication**, and then click **Enable**.
 - k. Click your Orion server, and then click **Restart** in the Actions pane.
6. Close the IIS Manager.
7. Log in to the Orion Web Console using the Windows account credentials you have already established.

Using the DirectLink Account

Enabling a DirectLink account allows you to make direct hyperlinks to specific web console views available to individuals who do not already have Orion Web Console user accounts. Any URL referring directly to an Orion NPM web page bypasses the login screen, logging the user into the DirectLink account. The DirectLink account is created like any other account, and it can include custom views and account limitations. For more information web console accounts, see “Creating New Accounts” on page 91.

To enable a DirectLink account for Orion NPM:

1. Log in to the Orion Web Console as an administrator.
2. Click **Settings** in the top right of the web console.
3. Click **Account Manager** in the Accounts grouping of the Orion Website Administration page.
4. Click **Add**.
5. Type `DirectLink` as the new **User Name**.
6. Type a **Password**, confirm it, and then click **Submit**.
7. Edit DirectLink account options, as necessary, for your installation of Orion Network Performance Monitor. For more information about editing account options, see “Editing User Accounts” on page 92.
8. Create a custom view to be used as the home page of the DirectLink account. For more information, see “Creating New Views” on page 43.
9. Specify the new DirectLink view as a default view in Account Manger. For more information, see “Editing User Accounts” on page 92.
10. ***If you would like to limit the DirectLink account to specific devices or device types***, see “Setting Account Limitations” on page 93.

Appendix F

Regular Expression Pattern Matching

When editing comparison criteria, the following regular expressions can be used for pattern matching. Examples are provided at the end of this section.

Characters

Character	Description	Example
Any character except [, \, ^, \$, ., , ?, *, +, (,),	All characters except the listed special characters match a single instance of themselves.	a matches a
\ (backslash) followed by any of [, \, ^, \$, ., , ?, *, +, (,),	A backslash escapes special characters to suppress their special meaning.	\+ matches +
\xFF where FF are 2 hexadecimal digits	Matches the character with the specified ASCII/ANSI value, which depends on the code page used. Can be used in character classes.	\xA9 matches © when using the Latin-1 code page.
\n, \r and \t	Match an LF character, CR character and a tab character respectively. Can be used in character classes.	\r\n matches a DOS/Windows CRLF line break.

Character Classes or Character Sets [abc]

Character Classes or Sets	Description	Example
[(opening square bracket)	Starts a character class. A character class matches a single character out of all of the possibilities offered by the character class. Inside a character class, different rules apply. The rules in this section are only valid inside character classes. The rules outside this section are not valid in character classes, except \n, \r, \t and \xFF	
Any character except ^, -,], \ add that character to the possible matches for the character class.	All characters except the listed special characters.	[abc] matches a, b or c
\ (backslash) followed by any of ^, -,], \	A backslash escapes special characters to suppress their special meaning.	[^\]] matches ^ or]
- (hyphen) except immediately after the opening [Specifies a range of characters. (Specifies a hyphen if placed immediately after the opening [)	[a-zA-Z0-9] matches any letter or digit

Character Classes or Sets	Description	Example
<code>^</code> (caret) immediately after the opening <code>[</code>	Negates the character class, causing it to match a single character not listed in the character class. (Specifies a caret if placed anywhere except after the opening <code>[</code>)	<code>[^a-d]</code> matches <code>x</code> (any character except <code>a</code> , <code>b</code> , <code>c</code> or <code>d</code>)
<code>\d</code> , <code>\w</code> and <code>\s</code>	Shorthand character classes matching digits 0-9, word characters (letters and digits) and whitespace respectively. Can be used inside and outside character classes	<code>[\d\s]</code> matches a character that is a digit or whitespace

Anchors

Anchors	Description	Example
<code>^</code> (caret)	Matches at the start of the string to which the regular expression pattern is applied. Matches a position rather than a character. Most regular expression flavors have an option to make the caret match after line breaks (i.e. at the start of a line in a file) as well.	<code>^.</code> matches <code>a</code> in <code>abc\ndef</code> . Also matches <code>d</code> in "multi-line" mode.
<code>\$</code> (dollar)	Matches at the end of the string to which the regular expression pattern is applied. Matches a position rather than a character. Most regular expression flavors have an option to make the dollar match before line breaks (i.e. at the end of a line in a file) as well. Also matches before the very last line break if the string ends with a line break.	<code>.\$</code> matches <code>f</code> in <code>abc\ndef</code> . Also matches <code>c</code> in "multi-line" mode.
<code>\A</code>	Matches at the start of the string to which the regular expression pattern is applied to. Matches a position rather than a character. Never matches after line breaks.	<code>\A.</code> matches <code>a</code> in <code>abc</code>
<code>\Z</code>	Matches at the end of the string to which the regular expression pattern is applied. Matches a position rather than a character. Never matches before line breaks, except for the very last line break if the string ends with a line break.	<code>.\Z</code> matches <code>f</code> in <code>abc\ndef</code>
<code>\z</code>	Matches at the end of the string to which the regular expression pattern is applied. Matches a position rather than a character. Never matches before line breaks.	<code>.\z</code> matches <code>f</code> in <code>abc\ndef</code>

Quantifiers

Quantifiers	Description	Example
? (question mark)	Makes the preceding item optional. The optional item is included in the match, if possible.	abc? matches ab or abc
??	Makes the preceding item optional. The optional item is excluded in the match, if possible. This construct is often excluded from documentation due to its limited use.	abc?? matches ab or abc
* (star)	Repeats the previous item zero or more times. As many items as possible will be matched before trying permutations with fewer matches of the preceding item, up to the point where the preceding item is not matched at all.	. * matches "def" "ghi" in abc "def" "ghi" jkl
*? (lazy star)	Repeats the previous item zero or more times. The engine first attempts to skip the previous item before trying permutations with ever increasing matches of the preceding item.	. *? matches "def" in abc "def" "ghi" jkl
#NAME?	Repeats the previous item once or more. As many items as possible will be matched before trying permutations with fewer matches of the preceding item, up to the point where the preceding item is matched only once.	.+ matches "def" "ghi" in abc "def" "ghi" jkl
+? (lazy plus)	Repeats the previous item once or more. The engine first matches the previous item only once, before trying permutations with ever increasing matches of the preceding item.	.+? matches "def" in abc "def" "ghi" jkl
{ <i>n</i> } where <i>n</i> is an integer ≥ 1	Repeats the previous item exactly <i>n</i> times.	a{3} matches aaa
{ <i>n,m</i> } where $n \geq 1$ and $m \geq n$	Repeats the previous item between <i>n</i> and <i>m</i> times. Will try to repeat <i>m</i> times before reducing the repetition to <i>n</i> times.	a{2,4} matches aa, aaa or aaaa
{ <i>n,m</i> ?} where $n \geq 1$ and $m \geq n$	Repeats the previous item between <i>n</i> and <i>m</i> times. Will try to repeat <i>n</i> times before increasing the repetition to <i>m</i> times.	a{2,4}? matches aaaa, aaa or aa
{ <i>n</i> ,} where $n \geq 1$	Repeats the previous item at least <i>n</i> times. Will try to match as many items as possible before trying permutations with fewer matches of the preceding item, up to the point where the preceding item is matched only <i>m</i> times.	a{2,} matches aaaaa in aaaaa
{ <i>n</i> ,}? where $n \geq 1$	Repeats the previous item between <i>n</i> and <i>m</i> times. The engine first matches the previous item <i>n</i> times before trying permutations with ever increasing matches of the preceding item.	a{2,}? matches aa in aaaaa

Dot

Dot Character	Description	Example
. (dot)	Matches any single character except line break characters \r and \n.	. matches x or most any other character

Word Boundaries

Word Boundary	Description	Example
\b	Matches at the position between a word character (anything matched by \w) and a non-word character (anything matched by [^\w] or \W) as well as at the start and/or end of the string if the first and/or last characters in the string are word characters.	.\b matches c in abc
\B	Matches at the position between two word characters (i.e the position between \w\w) as well as at the position between two non-word characters (i.e. \W\W).	\B.\B matches b in abc

Alternation

Alternation Character	Description	Example
(vertical bar or "pipe")	Causes the regular expression engine to match either the part on the left side or the part on the right side. Can be strung together into a series of options.	abc def xyz matches abc, def or xyz
(vertical bar or "pipe")	The vertical bar has the lowest precedence of all operators. Use grouping to alternate only part of the regular expression.	abc(def xyz) matches abcdef or abcxyz

Regular Expression Pattern Matching Examples

The following examples illustrate uses of regular expression pattern matching.

```
snmp-server community public
```

Finds any line that includes the text `snmp-server community public`. There can be text before and/or after the string on the same line.

```
service tcp-keepalives-in.*\n(.*)*.service tcp-keepalives-out
```

Finds the first line `service tcp-keepalives-in` and then looks for `service tcp-keepalives-out` on any line after that. The regular expression string `.*\n(.*)*.service tcp-keepalives-out` is used to search any number of lines between strings.


```
access-list 105 deny.*tcp any any eq 139 log
```

Finds the line with `access-list 105 deny`, followed by any number of characters of any type, followed by `tcp any any eq 139 log` on the same line. The regular expression string `.*` finds any character and any number of characters on the same line. This expression can be used to find spaces, tabs, numbers, letters, or special characters.

```
ntp clock-period \d*
```

Finds any line that includes `ntp clock-period`, followed by any number. The regular expression string `\d*` will find any number at any length, such as 3, 48, or 2394887.

```
user \x2a
```

Finds any line that includes `user *`. The regular expression string `\x`, followed by a hexadecimal value, specifies an individual character. In this example, `\x2a` represents the asterisk character, which has a hexadecimal value of `2a`.

Appendix G

Troubleshooting

If you have problems with Orion Network Performance Monitor, the causes are usually related to an incorrect configuration or corrupted files. The following suggestions can often clear up these problems.

Back Up Your Data

As a first step in any troubleshooting procedure, you should back up your Orion Network Performance Monitor database. For more information, see “Creating Database Backups” on page 270.

Verify Program Operation

Orion NPM must run several components at the same time to deliver information. Check to see that the following components are running:

- SolarWinds Network Performance Monitor Service (NPM)
- SQL Server
- Internet Information Service (IIS)

Stop and Restart

Many problems disappear when programs are restarted. Stopping and restarting Internet Information Service (IIS) may eliminate web page problems. Problems with polling or data gathering may be eliminated by stopping and restarting the SolarWinds Network Performance Monitor Service using the available shutdown tool that you can locate as follows:

Click **Start > All Programs > SolarWinds Orion > Advanced Features > Orion Service Manager**.

For a complete refresh of the system, reboot the computer.

Run the Configuration Wizard

Running the Configuration Wizard, which refreshes files on the web server and performs checks on the structure of your database, may solve many problems.

Note: Before you run the Configuration Wizard, you should close all open applications and stop the SolarWinds Network Performance Monitor Service in

the Windows Services Control Panel. It will be restarted by the Wizard at the end of its process.

Adjusting Interface Transfer Rates

Orion NPM monitors the actual transfer rates on the interfaces and calculates the percent utilization in realtime, as it's requested in reports or within the user interface. Usually when you see interface utilization over 100% it is because the *Transmit* and *Receive* bandwidth values for this interface in Orion NPM are incorrect.

To update interface transfer rates:

1. Click **Start > All Programs > SolarWinds Orion > System Manager**.
2. Drill into the node that contains the interface you want to update, and then click **Interfaces > Interface Details**.
3. Edit the values in the **Transmit Bandwidth** and **Receive Bandwidth** fields, and then click **Apply Changes**.

Using Full Variable Names

If you are having difficulty acquiring expected values from a selected variable, using the `${VariableName}` format, it may be helpful to include the database table name within the variable name, as in `${Nodes.IP_Address}`.

Working with Temporary Directories

The following sections provide procedures for moving Windows and SQL Server temporary directories to optimize Orion server performance and resources.

Moving the SQL Server Temporary Directory

The SQL Server temporary directory, `tempdb`, where temporary database objects generated during table creation and sorting are stored, is typically created in the same location on your Orion database server as the `master`, `model`, and `msdb` databases. Moving the `tempdb` database to a physical drive separate from your Orion NPM database can significantly improve overall system performance.

For more information about moving the SQL Server 2005 temporary directory, `tempdb`, for see "Moving System Databases – Example A: Moving the tempdb Database".

For more information about moving the SQL Server 2008 temporary directory, `tempdb`, for see "Moving System Databases – Example A: Moving the tempdb Database".

Redefining Windows System Temporary Directories

Following established Windows standards, the Orion NPM installer may use Windows User and System TEMP and TMP variable directories as temporary scratch spaces for file expansion and execution. If you do not have the required scratch space available in the default User or System TEMP and TMP directories, use the following procedure to redefine your default locations.

Note: Regardless of where you actually install Orion NPM, some common files may be installed where the operating system of your Orion server are located.

To redefine default system temporary directories:

1. Log on to your Orion server as a user with administrative rights.
2. Right-click **My Computer**, and then click **Properties**.
3. Click **Advanced**, and then click **Environment Variables**.
4. Select the variable name representing the directory you want to redefine, click **Edit**, and then provide a new path as the **Variable value** for the selected temporary directory variable.

Index

Index

6

- 64-bit counters 42

9

- 95th percentile calculations
 - configuration 63
 - definition 339

A

- account limitations 93
 - creating 257
 - deleting 258
 - introduction 257
 - pattern 94
 - removing 258
 - viewing reports 208
- Account Manager 39
- accounts
 - editing users 92
 - new user 91
 - Web Console 39
- acknowledging
 - events in System Manager 131
 - events in the Web Console 130
 - Syslog messages in Syslog Viewer 214
 - Syslog messages in the Web Console 214

- logging alerts to Windows Event Log 164, 219

- logging traps to a file 230

- logging traps to Windows Event Log 230

- modifying Syslog message 219

- playing a sound 161, 219, 231

- send email/page 158, 220, 231

- send SNMP trap 176, 219

- send Windows Net messages 175, 220, 231

- sending syslog messages 166, 219

- sending traps 230

- tag message 219

- tag trap 230

- text-to-speech 174, 219, 231

- traps 230

- visual basic scripts 231

- Visual Basic scripts 170, 219

- adding

- alert actions 158

- database servers 269

- devices in the Web Console 78

- additional pollers

- introduction 295

- adjusting interface transfer rates 352

- Advanced Alert Manager

- Active Alerts 156

- creating alerts 145, 146

- Current Events 155

- escalation 153

- monitoring period 150

- overview 154

- reset actions 152

- reset conditions 148

- settings 157

- suppressions 149

- time of day 150

- trigger actions 151
- trigger conditions 146
- advanced alerts
 - acknowledging (System Manager) 178
 - acknowledging (Web Console) 177
 - actions 158
 - adding actions 158
 - alert trigger 146
 - configuration 145
 - creating 145, 146
 - disabling actions 263
 - escalated 178
 - escalation 153
 - monitoring period 150
 - reset actions 152
 - reset conditions 148
 - suppressions 149
 - time of day 150
 - trigger actions 151
 - trigger conditions 146
 - viewing in System Manager 263
- advanced customization
 - Web Console settings 63
- alert actions
 - change custom property 173
 - discard message 218
 - discard trap 230
 - email a web page 171
 - executing an external program 169, 219, 231
 - flagging traps 230
 - GET/POST 177
 - logging alerts to a file 162, 219
 - logging alerts to Windows Event Log 164, 219
 - logging traps to a file 230
 - logging traps to Windows Event Log 230
 - modifying Syslog message 219
 - playing a sound 161, 219, 231
 - send email/page 158, 220, 231
 - send SNMP trap 176, 219
 - send Windows Net messages 175, 220, 231
 - sending Syslog messages 166, 219
 - sending traps 230
 - tagging message 219
 - tagging traps 230
 - text-to-speech 174, 219, 231
 - visual basic scripts 231
 - Visual Basic scripts 170, 219
- alert suppressions
 - advanced 149
 - basic 138
- alert trigger
 - advanced alerts 146
 - basic alerts 138
- alert variables
 - advanced alert engine 321
 - alert-specific (basic) 315
 - basic alert engine 309
 - buffer errors (basic) 309
 - Date/Time (advanced) 322
 - date/time (basic) 315
 - date/time (Syslog) 334
 - date/time (traps) 335
 - examples (basic) 316
 - general (advanced) 321
 - interface (advanced) 328
 - interface errors (basic) 310
 - interface poller (advanced) 324
 - interface polling (basic) 311
 - interface status (basic) 311
 - interface traffic (basic) 311
 - interfaces (basic) 310
 - modifiers 309
 - node (advanced) 330
 - node poller (advanced) 326
 - node polling (basic) 313
 - node statistics (basic) 313
 - node status (advanced) 323
 - node status (basic) 313
 - nodes (basic) 312
 - object types (basic) 313
 - other (Syslog) 335
 - other (traps) 336
 - SQL query (advanced) 323
 - Syslog 221, 334
 - Syslog (date/time) 221

- Syslog (other) 222
- traps 231, 335
- traps (date/time) 232
- traps (other) 232
- Universal Device Poller
 - (advanced) 321
 - volume (advanced) 333
 - volume polling (basic) 314
 - volume statistics (basic) 314
 - volume status (basic) 314
 - volumes (basic) 314
 - wireless node (advanced) 334
- alerts
 - actions 158
 - adding actions 158
 - audible web 97
 - condition groups 153
 - dependent node alert
 - suppression example 318
 - escalated 178
 - escalation example 178
 - executing an external program
 - 169, 219, 231
 - introduction 133
 - load balancing failure example
 - 319
 - log files 162, 219
 - logging to Windows Event Log
 - 164, 219
 - playing a sound 231
 - suppression examples (basic)
 - 316
 - Universal Device Pollers 249
 - viewing in System Manager 134, 262
 - viewing in the Web Console 134
 - visual basic scripts 231
 - Visual Basic scripts 170, 219
- allocation failures
 - charts 70

- Application Performance Monitor
 - 281, 283
 - architecture 7
 - assigning pollers 87
 - audible web alerts 97
 - automatic login
 - DirectLink 344
 - introduction 341
 - URL pass-through 341
 - Windows pass-through 342
- availability
 - calculation 105
 - charts 69
- average response time charts
 - in System Manager 267

B

- bandwidth 352
- banner
 - configuration 61
- baseline calculation 105
- basic alerts
 - actions 139, 158
 - adding actions 158
 - alert trigger 138
 - configuring 135
 - copying 141
 - creating 136
 - deleting 144
 - disabling actions 263
 - editing names 136
 - monitored network objects 137
 - properties to monitor 137
 - suppressions 138
 - testing 140
 - time of day 138
 - trigger conditions 138
 - viewing in System Manager 263
- benefits of Orion NPM 2
- breadcrumbs 36, 37

C

- calculating
 - availability 105
 - baseline 105
- calculation
 - availability 104
 - baseline 104

- call managers
 - monitoring 287
- capabilities of Orion NPM 1
- charts
 - allocation failures 70
 - aspect ratio 63
 - availability 69
 - cache timeout 63
 - CPU load 69
 - custom 66
 - custom chart view 71
 - custom interface 68
 - custom node 69
 - custom volume 70
 - customizing in System Manager 268
 - data export options 72
 - discards 68
 - disk usage 70
 - errors 68
 - font size 72
 - in the web console 66
 - interfaces 68
 - memory usage 69
 - multicast traffic 68
 - nodes 69
 - packet loss 70
 - percent loss 70
 - percent utilization 68
 - predefined in System Manager 265
 - printing options 71
 - response time 70
 - sample intervals 71
 - settings in System Manager 261
 - settings in the Web Console 63
 - size 71
 - SLA line 58
 - time periods 71
 - titles 71
 - traffic 68
 - viewing in System Manager 265
 - volume sizes 70
 - volumes 70
- Cisco buffer misses threshold 44
- clearing events
 - in System Manager 131
- color scheme 61
- compacting
 - database tables 272
 - databases in Database Manager 271
- components of Orion NPM 7
- concepts 5
- condition groups 153
 - all 153
 - any 154
 - none 154
 - not all 154
- configuration
 - web console resources 49
- Configuration Wizard 18
- configurations
 - Web Console 75
- configuring
 - advanced alerts 145
 - audible web alerts 97
 - basic alerts 135
 - Hot Standby Engine 292
 - Orion NPM 18
 - reports folders 96
 - web-only interface 299
- copying basic alerts 141
- counter rollover 104
- counter rollovers 42
- CPU load
 - charts 69
 - threshold 43
- creating
 - account limitations 257
 - alerts 136
 - alerts, advanced 145, 146
 - backup databases 270
 - custom properties 251
 - custom properties filters 253
 - escalated alerts 179
 - user accounts 91
- credentials
 - VMware ESX 126

- current CPU utilization charts
 - in System Manager 267
- current in/out bps charts
 - in System Manager 267
- current memory utilization charts
 - in System Manager 267
- current percent utilization charts
 - in System Manager 267
- current response time charts
 - in System Manager 266
- current volume utilization charts
 - in System Manager 267
- custom properties
 - creating a property 251
 - creating filters 253
 - Custom Property Editor 251
 - Custom Property Editor settings 256
 - deleting 252
 - deleting filters 254
 - editing 253
 - filters 253
 - importing data 255
 - introduction 251
 - removing 252
 - removing filters 254
 - settings 256
- customize
 - Web Console 39
- customizing charts
 - in System Manager 268

D

- data
 - export charts 72
 - security 41, 101
- database
 - maintenance 101
- database details
 - in Database Manager 272
 - in the Web Console 41
- database maintenance 278
 - introduction 278
 - migrating a database 279
- Database Manager
 - adding a server 269
 - backup databases 270

- compacting a database 271
- compacting database tables 272
- database details 272
- detaching a database 275
- editing fields 274
- introduction 269
- maintenance plan 275
- restoring a database 270
- table details 273
- database settings 102
- definition
 - account limitation 257
 - availability 105
 - baseline 105
 - custom property 251
 - EnergyWise 111
 - ICMP 5
 - interfaces 9
 - MIB 7
 - nodes 9
 - Orion NPM 1
 - SNMP 6
 - SNMP credentials 6
 - volumes 9
- deleting
 - account limitations 258
 - basic alerts 144
 - custom properties 252
 - custom properties filters 254
 - devices from the Web Console 81
 - wireless devices 128
- detaching a database 275
- devices
 - adding in the Web Console 78
 - deleting from the Web Console 81
 - poll now 88
 - rediscover 88
- DirectLink automatic login 344
- directories
 - temporary 352
- disabling actions
 - advanced alerts 263
 - basic alerts 263

- discarding
 - syslog messages 218
 - traps 230
- discards
 - charts 68
- discovery 25
 - removable volumes 63
 - results 30
 - scheduled results 32
 - seed files 31
- Discovery Ignore List 33
- discovery settings 63
- disk usage
 - charts 70
- disk usage threshold 43
- documentation iv
- domain 111
- E**
- editing
 - custom properties 253
- editing alert names
 - basic 136
- editing device properties
 - in the web console 83
- editing user accounts 92
- element 13
- email a web page 171
- enabling a software license key 303
- Enabling SNMP
 - ESX Server version 3.5 121
 - ESX Server version 4.0 123
 - ESXi 120
- EnergyWise 111
 - domain 111
 - entity 111
 - entity power levels 117
 - importance 111
 - keywords 112
 - monitoring devices 113
 - name 112
 - neighbor 112
 - policy level 113
 - power level 113
 - reports 188
 - resources 113
 - Summary view 114
 - terminology 111
- EnergyWise Level 113
- EnergyWise Summary view 117
- Engineer's Toolset 72
- entity 111
 - power levels 117
- errors
 - charts 68
- errors charts
 - in System Manager 267
- escalated alerts 178
 - creation 179
 - example 178
- escalation
 - advanced alerts 153
- estimating maximum polls/sec 107, 108
- ESX API
 - polling
 - settings 103
- ESX Server
 - enabling SNMP on version 3.5 121
 - enabling SNMP on version 4.0 123
- ESX Servers 119
 - adding 126
 - creating credentials 125
 - managing credentials 126
 - monitoring requirements 119
 - polling methods 119
- ESXi 119
 - enabling SNMP 120
 - monitoring requirements 119
 - polling methods 119
- event details
 - in System Manager 130
- event summary
 - adding to web console 52
- events
 - acknowledging in the Web Console 130
 - in System Manager 131
 - viewing in the Web Console 129

- Events view 129
- EW Level 113
- exporting databases 279
- external websites 59
- F**
- facility 222
- features 2
- fields
 - editing in Database Manager 274
- filtering
 - custom properties 253
- filtering a node list resource 56
- finding nodes in System Manager 259
- font size 63
 - charts 72
- functional overview 7
- G**
- GET
 - alerts 177
- grouping nodes
 - in System Manager 260
- grouping nodes in a resource 57
- H**
- help server 63
- Home tab 36
- Hot Standby Engine
 - configuration 292
 - installation 290
 - introduction 289
 - testing 293
- HTTP 74
- HTTPS
 - scheduled reports 207
- I**
- ICMP 5
 - monitoring 7
 - promoting to SNMP 84
 - settings 103
- icons
 - status 305
- ignored devices 33
- IIS
 - on Windows Server 2003 14
 - on Windows Server 2008 14
 - on Windows Vista 14
 - on Windows XP 14
- importance 111
- importing
 - custom properties data 255
 - databases 279
- installing
 - Hot Standby Engine 290
 - Orion NPM 15
 - web-only interface 299
- integrated remote desktop 74
- interface
 - errors and discards threshold 45
 - percent utilization threshold 45
 - status rollup 63
 - transfer rates 352
- interfaces
 - adding in the Web Console 78
 - adding multiple 25
 - custom charts 68
 - definition 9
 - deleting from the Web Console 81
 - discovery 25
 - editing properties in the web console 83
 - management 88
 - poll now 88
 - polling intervals 101
 - polling statistics intervals 102
 - remote shut down 88
 - remotely enable 88
 - unpluggable 83
 - viewing resources in the web console 85
- introduction 1
- IPAM
 - introduction 283
- L**
- license
 - deactivating 22
 - details 41
 - key 303
 - maintenance 22
 - sizing 9

- License Manager 22
 - installing 22
 - using 22
- licensing 9
- limitations
 - account 93
 - pattern 94
- List Resources 85
- load balancing 108
- logging
 - alerts to a file 162, 219
 - alerts to Windows Event Log 164, 219
 - traps to a file 230
 - traps to Windows Event Log 230
- M**
- maintaining a database 278
- maintenance plan 275
- manage nodes 86
- Management Studio 276
- map cache timeout 63
- maps 183
 - adding to web console 49
 - list resource 51
 - objects list resource 50
- memory swapping 89
- memory usage
 - charts 69
- menu bars
 - account defaults 95
 - custom 59
- MIB 7
- migrating
 - databases 279
- modifying syslog messages 219
- modules
 - Application Performance Monitor 281, 283
 - NetFlow Traffic Analyzer 285
 - VoIP Monitor 287
- monitored network objects
 - basic alerts 137
- monitoring
 - applications 281, 283
 - call managers 287
 - capabilities 1
 - memory 89
 - NetFlow 285
 - period (advanced alerts) 150
 - QoS 287
 - traffic 285
 - VoIP networks 287
 - wireless networks 127
- monitoring requirements 12
- multicast traffic
 - charts 68
- N**
- neighbor 112
- Net messages 175, 220, 231
- NetFlow
 - monitoring 7
- NetFlow Traffic Analyzer 285
- NetPerfMon Engine status 99
- network
 - details (System Manager) 260
- Network Atlas 183
- Network Discovery
 - getting started 25
 - ignored results 33
 - introduction 25
 - results 30
 - scheduled results 32
 - seed files 31
- Network Overview 77
- network settings 103
- Network tab 36
- networking
 - concepts 5
 - terminology 5
- network-wide charts
 - in System Manager 265
- node
 - status rollup 63
- node groups
 - System Manager 260
- node maintenance mode 89
- node management
 - enable interfaces 88
 - in the Web Console 77
 - poll now 88
 - rediscover 88
 - shut down interfaces 88

- states 86
- Web Console administration 38
- node tree
 - System Manager 259
- node tree settings
 - System Manager 261
- node warning interval 106
- nodes
 - adding in the Web Console 78
 - adding multiple 25
 - availability 105
 - custom charts 69
 - definition 9
 - deleting from the Web Console 81
 - discovery 25
 - editing properties in the web console 83
 - filtering a resource list 56
 - finding in System Manager 259
 - grouping in a resource 57
 - grouping in System Manager 260
 - poll now 88
 - polling intervals 101
 - polling statistics intervals 102
 - reassigning to polling engines 108
 - rediscover 88
 - viewing resources in the web console 85
- notification bar 35

O**Orion**

- Application Performance Monitor 281, 283
- NetFlow Traffic Analyzer 285
- Network Atlas 183
- VoIP Monitor 287
- Wireless 127
- Orion NPM
 - License Manager 22
 - System Manager 259
 - thwack.com integration 2

- Orion Polling Settings 101
- Orion Report Scheduler 206
- Orion Web Console 35
- Orion Website Accounts 39
- overview
 - functional 7

P

- packet loss
 - calculation 44
 - charts 70
- packet queues 100
- page refresh 63
- pattern limitations 94
- peak traffic charts
 - in System Manager 267
- percent loss
 - charts 70
- percent memory used threshold 43
- percent packet loss threshold 44
- percent utilization
 - charts 68
- playing a sound 161, 219, 231
- policy level 113
- poll now 88
- pollers
 - configuration 101
 - settings 101
- polling engine
 - status 99
- polling engines
 - configuration 101
 - details 41
 - estimating maximum polls/sec 107
 - load balancer 108
 - management 99
 - reassigning nodes 108
 - setting maximum polls/sec 108
 - settings 101
 - tuning 106
- polling intervals
 - response time 101
 - status 101
- polling statistics intervals 102
- POST
 - alerts 177

- power levels 117
- predefined charts
 - in System Manager 265
- printing
 - charts 71
- product updates
 - downloading 62
 - viewing 62
- promoting nodes from ICMP to SNMP 84
- property to monitor
 - basic alerts 137
- R**
- realtime change detection 219, 231
- rediscovery 88
- regular expressions
 - alternation 348
 - anchors 346
 - character sets/classes 345
 - characters 345
 - dot 348
 - examples 348
 - pattern matching 345
 - quantifiers 347
 - word boundaries 348
- remote access
 - HTTP 74
 - SSH 74
 - Telnet 74
- remote desktop 74
- removable volumes
 - discovery: 63
- removing
 - account limitations 258
 - custom properties 252
 - custom properties filters 254
 - wireless devices 128
- report cache timeout 63
- reports
 - access points 196
 - account limitations 208
 - adding to web console 54
 - alerts 191
 - availability 186, 188
 - buffer misses 192
 - Cisco buffer 192
 - clients 196
 - CPU 192
 - creating a report 199
 - design mode 199
 - device types 195
 - disk space 195
 - down events 191
 - down interfaces 187
 - down nodes 187
 - energy consumption 188
 - EnergyWise 188
 - events 191
 - example 204
 - exporting 203
 - field formatting options 203
 - field options 200
 - filter results options 201
 - folder 96
 - footers 203
 - formats 203
 - general options 199
 - getting started 198
 - grouping options 202
 - headers 203
 - interface bandwidth 195
 - interface response time 187
 - interface status 187
 - interface types 195
 - inventory 195
 - IOS versions 195
 - last 250 events 191
 - list resource 55
 - modifying a report 199
 - network traffic 193
 - node response time 187
 - node status 187
 - predefined 186
 - preview mode 198
 - response time 192
 - rogues 196
 - scheduling 206
 - SQL query 204
 - summarization options 202
 - time frame options 202
 - top XX records options 201
 - total bytes transferred 193

- traffic rates 193
- virtual machine CPU utilization
 - 194
- virtual machine memory
 - utilization 194
- virtual machine running time 194
- virtual machine traffic 194
- VMware ESX Server 194
- volume status 188
- volume usage 195
- volumes 195
- wireless 196
- Reports
 - view 185
- requirements 10
 - monitored devices 12
 - Orion database server 11
 - Orion NPM server 10
 - SNMP monitoring 12
 - virtual machines 12
 - virtual servers 12
 - VMware Servers 12
- reset
 - actions (advanced alerts) 152
 - conditions (advanced alerts) 148
- resources
 - configuration 49
 - custom HTML 53
 - custom text 53
 - EnergyWise 113
 - event summary 52
 - map objects list 50
 - maps 49
 - maps list 51
 - reports 54
 - reports list 55
 - Syslog 212
 - user-defined links 52
- response
 - calculation 44
- response time
 - charts 70
 - threshold 44
- restoring databases 270
- rollover 42
- S**
- sample intervals
 - adjust 71
- scheduled discovery
 - ignored results 33
 - managing results 32
- scheduling node maintenance 89
- secure sockets layer 23
- security of data 41, 101
- seed files 31
- sending
 - email/page 158, 220, 231
 - SNMP trap 176, 219
 - syslog messages 166, 219
 - traps 230
- server
 - requirements 13
 - sizing 13
- service level agreement
 - chart line 58
- services 7
- session timeout 63
- setting
 - account defaults 95
 - account limitations 93
 - pattern account limitations 94
- settings
 - charts 63
 - discovery 63
 - System Manager 260
 - Web Console 40
 - website 63
- severity 223
- site login text 63
- site logo
 - configuration 61
 - URL 63
- sizing
 - database 9
 - network 9
- SNMP
 - monitoring requirements 12
- SNMP 6
 - monitoring 7

- SNMP
 - settings 103
- SNMP credentials 6
- snmp traps See traps
- software license key 303
- spoofing network packets 220
- SQL
 - query as a variable 323
 - Server Management Studio 276
 - variables 323
- SQL Server
 - tempdb 352
- SSH 74
- SSL 23
- statistics pollers 100
- status icons 305
- status pollers 100
- status rollup 63
- summarization 278
- suppression
 - advanced alerts 149
- suppression examples
 - basic alerts 316
 - dependent node alert 318
 - load balancing failure alert 319
- suppressions
 - basic alerts 138
- Syslog
 - acknowledging messages in
 - Syslog Viewer 214
 - acknowledging messages in the
 - Web Console 211, 214
 - alert actions 218
 - alert variables 221, 334
 - alerts 166, 216, 219
 - daemons 222
 - facility 222
 - filters 216
 - forwarding messages 220
 - messages in the Web Console
 - 211
 - monitoring 7, 211
 - priority value 222
 - processes 222
 - resources 212
 - searching messages 215
 - server settings 215
 - severity 223
 - view 213
 - viewing messages in Syslog
 - Viewer 214
 - viewing messages in the Web
 - Console 213
- System Manager
 - acknowledging advanced alerts
 - 178
 - availability calculation 105
 - average response time charts
 - 267
 - baseline calculation 105
 - charts 265
 - charts settings 261
 - creating basic alerts 136
 - current CPU utilization charts 267
 - current in/out bps charts 267
 - current memory utilization charts
 - 267
 - current percent utilization charts
 - 267
 - current response time charts 266
 - current volume utilization charts
 - 267
 - customizing charts 268
 - errors charts 267
 - event details 130
 - events 131
 - finding nodes 259
 - grouping nodes 260
 - network wide charts 265
 - node groups 260
 - node maintenance 89
 - node tree 259
 - node tree settings 261
 - node warning interval 106
 - peak traffic charts 267
 - polling engine status 99
 - predefined charts 265
 - settings 260
 - starting 259
 - top XX charts 266
 - using 259
 - viewing alerts 134

- viewing network details 260

T

- tables

- compacting 272
 - details 273

- tabs 36

- tagging

- syslog messages 219
 - traps 230

- Telnet 74

- TEMP 353

- tempdb 352

- terminology 5

- EnergyWise 111
 - EnergyWise domain 111
 - EnergyWise entity 111
 - EnergyWise importance 111
 - EnergyWise keywords 112
 - EnergyWise name 112
 - EnergyWise neighbor 112
 - EnergyWise policy level 113
 - EnergyWise power level 113

- testing

- basic alerts 140
 - Hot Standby Engine 293

- text-to-speech 174, 219, 231

- thresholds 43, 104

- Cisco buffer misses 44
 - configuration 45
 - CPU load 43
 - disk usage 43
 - interface errors and discards 45
 - interface percent utilization 45
 - percent memory used 43
 - percent packet loss 44
 - response time 44

- thumbnail aspect ratio 63

- thwack.com 2

- time of day

- advanced alerts 150
 - basic alerts 138

- time periods

- charts 71

- TMP 353

- Toolset integration 72

- adding programs 73

- configuration 72

- top XX charts

- in System Manager 266

- traffic

- charts 68

- Trap Viewer 226

- settings 227

- traps

- alert actions 228
 - alert actions 176, 219
 - alert variables 231, 335
 - alerts 228, 230
 - alerts actions 230
 - community string 228
 - conditions 228
 - defined 225
 - DNS hostname 228
 - email/page 231
 - executing an external program 231

- filters 228

- log files 230

- logging to Windows Event Log 230

- playing a sound 231

- port 226

- protocol 225

- searching 227

- text-to-speech 231

- time of day 228

- Trap Viewer configuration 226

- Trap Viewer settings 227

- trigger thresholds 228

- viewing 226

- viewing in the Web Console 225

- visual basic scripts 231

- Traps

- view 225

- trigger actions

- advanced alerts 151

- trigger conditions

- advanced alerts 146

- basic alerts 138

- troubleshooting 351

- temporary directories 352

- variables 352

tuning polling engines 106

U

Universal Device Pollers

adding resources to the Web

Console 249

alerts 249

assigning devices 240

assigning to devices 87

copying 242

creating a poller 236

creating transformations 245

disabling 241

duplicating 242

exporting 243

importing 242

introduction 235

suspending 241

transformations 244

transforming 244

viewing statistics 249

unmanage nodes 86

unplugged interfaces 83

upgrading Orion NPM 20

URL pass-through automatic login

341

user accounts

access settings 92

creating 91

editing 92

limitations 93

menu bars 95

pattern limitations 94

reports folder 96

views 95

user-defined links 52

V

variables

advanced alerts 321

alert-specific (basic alerts) 315

basic alerts 309

buffer errors (basic alerts) 309

Date/Time (advanced alerts) 322

date/time (basic alerts) 315

date/time (Syslog alerts) 334

date/time (trap alerts) 335

examples (basic alerts) 316

full names 352

general (advanced alerts) 321

interface (advanced alerts) 328

interface errors (basic alerts) 310

interface poller (advanced alerts)
324

interface polling (basic alerts) 311

interface status (basic alerts) 311

interface traffic (basic alerts) 311

interfaces (basic alerts) 310

introduction 309

node (advanced alerts) 330

node poller (advanced alerts) 326

node polling (basic alerts) 313

node statistics (basic alerts) 313

node status (advanced alerts)
323

node status (basic alerts) 313

nodes (basic alerts) 312

object types (basic alerts) 313

other (Syslog alerts) 335

other (trap alerts) 336

SQL query (advanced alerts) 323

Syslog alerts 221, 334

Syslog alerts (date/time) 221

Syslog alerts (other) 222

trap alerts 231, 335

trap alerts (date/time) 232

trap alerts (other) 232

Universal Device Poller

(advanced alerts) 321

volume (advanced alerts) 333

volume polling (basic alerts) 314

volume statistics (basic alerts)
314

volume status (basic alerts) 314

volumes (basic alerts) 314

wireless node (advanced alerts)
334

viewing

advanced alerts (System
Manager) 263

alerts (System Manager) 134,
262

alerts (Web Console) 134

- basic alerts (System Manager) 263
- charts (System Manager) 265
- device resources (Web Console) 85
- event details (System Manager) 130
- events (Web Console) 129
- predefined charts (System Manager) 265
- Syslog messages (Web Console) 213
- traps (Web Console) 225
- views
 - account defaults 95
 - adding EnergyWise Summary 117
 - Alerts 134
 - by device type 49
 - copying 48
 - creating 46
 - customizing 46
 - deleting 49
 - editing 46
 - EnergyWise Summary 114
 - in System Manager 260
 - menu bars 59
 - Network Overview 77
 - Orion Poller Settings 101
 - Orion Website Accounts 39
 - product updates 62
 - Reports 185
 - Syslog 213
 - Traps 225
 - Web Console 40
- visual basic scripts 231
- Visual Basic scripts 170, 219
- VMware
 - adding ESX Servers 126
 - ESX Servers 119
 - ESXi 119
 - managing credentials 126
 - monitoring requirements 12

- VMware Tools 12
- VoIP Monitor 287
- volume
 - status rollup 63
- volumes
 - adding in the Web Console 78
 - adding multiple 25
 - custom charts 70
 - definition 9
 - deleting from the Web Console 81
 - discovery 25
 - polling intervals 101
 - polling statistics intervals 102
 - size charts 70
 - viewing resources in the web console 85

W

- web console 35
 - breadcrumbs 37
 - configuring resources 49
 - navigation 36
 - notification bar 35
 - tabs 36
- Web Console
 - Account Manager 39
 - accounts 39
 - acknowledging advanced alerts 177
 - adding a map 49
 - adding an SLA chart line 58
 - adding devices 78
 - adding interfaces 78
 - adding nodes 78
 - adding volumes 78
 - Admin login 35
 - administration 38
 - Alerts view 134
 - banner 61
 - changing passwords 38
 - charts 66
 - clearing configurations 76
 - color scheme 61
 - configurations 75
 - configuring product updates 62
 - copying views 48

- creating accounts 91
 - creating configuration backups 75
 - creating views 46
 - custom HTML 53
 - custom text 53
 - customization 39
 - customizing 59
 - data security 41, 101
 - database details 41
 - deleting devices 81
 - deleting interfaces 81
 - deleting nodes 81
 - deleting views 49
 - deleting volumes 81
 - downloading product updates 62
 - editing accounts 92
 - editing device properties 83
 - editing views 46
 - event summary resource 52
 - Events view 129
 - external websites 59
 - filtering a node list resource 56
 - grouping nodes in a resource 57
 - icons 305
 - interface management 88
 - interface tooltips 82
 - license details 41
 - login 35
 - map objects list resource 50
 - maps list resource 51
 - menu bars 59
 - Network Overview 77
 - node management 38, 77
 - node management states 86
 - node tooltips 82
 - poll now 88
 - polling engines details 41
 - promoting nodes from ICMP to SNMP 84
 - rediscover 88
 - Reports 185
 - reports list resource 55
 - reports resource 54
 - restoring configuration backups 76
 - settings 40, 63
 - site logo 61
 - Syslog 211
 - thresholds 43
 - Toolset integration 72
 - Traps 225
 - Universal Device Poller
 - assignment 87
 - Universal Device Poller resources 249
 - user-defined links resource 52
 - view customization 46
 - viewing alerts 134
 - viewing device resources 85
 - viewing poller statistics 249
 - views 40
 - Views by Device Type 49
 - web node management 77
 - web-only interface
 - configuration 299
 - installation 299
 - introduction 299
 - website settings 63
 - Windows
 - Event Log alerts 164, 219, 230
 - memory 89
 - Net messages 175, 220, 231
 - pass-through automatic login 342
 - Wireless Networks
 - getting started 127
 - introduction 127
 - migrating historical data 127
 - removing devices 128
 - viewing data 127
- X**
- XML snapshots 262