

SolarWinds

Network Performance Monitor

Version 12.0

Administrator Guide

© 2016 SolarWinds Worldwide, LLC. All rights reserved.

This document may not 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 prior 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 respective licensors.

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, NOR 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.

The SolarWinds and other SolarWinds marks, identified on the SolarWinds website, as updated from SolarWinds from time to time and incorporated herein, are registered with the U.S. Patent and Trademark Office and may be registered or pending registration in other countries. All other SolarWinds trademarks may be common law marks or registered or pending registration in the United States or in other countries. All other trademarks or registered trademarks contained and/or mentioned herein are used for identification purposes only and may be trademarks or registered trademarks of their respective companies.

Table of Contents

Prepare a SolarWinds Orion Platform installation	24
SolarWinds Orion Platform requirements	24
SolarWinds Orion server software requirements	24
Server port requirements	26
SolarWinds Orion server hardware requirements	26
Server sizing recommendations	27
Recommendations	27
SolarWinds Orion database server (SQL Server) requirements	28
SQL Server configuration best practices	30
Virtual machines and servers requirements	33
Requirements for monitoring Microsoft Hyper-V, VMware ESXi, and ESX Servers	34
Security enhancements and exceptions for SolarWinds Orion Platform products	35
Enable secure channels with SSL	35
Configure the Orion Web Console for SSL	36
Configure the Orion Web Console to require SSL	36
Enable FIPS	37
Antivirus directory exclusions	38
Uninstall SolarWinds NPM	39
SolarWinds Orion Platform products licensing	39
Activate your SolarWinds license	40
Activate licenses with Internet access	40
Activate licenses offline	41
License Manager requirements	41
Install License Manager	42
Activate licenses with the License Manager	42
Deactivate and reactive licenses	43

Deactivate, move, and assign licenses online	43
Deactivate, move, and assign licenses offline	44
Upgrade and synchronize licenses	44
Synchronize licenses to the Customer Portal	44
How Orion Platform products work	46
Discover and add network devices	47
Discover your network with the Discovery Wizard	47
Add nodes using Active Directory	51
Credentials for Active Directory discovery	52
Automatically add discovered nodes	52
Add discovered devices to SolarWinds NPM	54
Add a single node for monitoring	57
Import nodes from a list of IP addresses	59
Manage scheduled discovery results	60
Minimize SNMP processing load during discoveries using the Discovery Ignore List	60
Add ignored devices back to discovery	60
Choose the polling method to use	60
External Node (No Status)	60
Status Only: ICMP	61
Most Devices: SNMP & ICMP	61
Windows Servers: WMI and ICMP	61
Windows Servers: Agent	62
Manage devices in the Orion Web Console	62
Edit node properties	62
Edit the node name, web address, and which view opens when you double-click the node	63
Edit polling settings	63
Edit dependencies or custom properties	64
Add what additional data you want to poll on the node	64
Customize alerting thresholds	64

Suspend collecting data for monitored nodes	65
Resume data collection for nodes	65
Poll and rediscover devices immediately	65
Stop monitoring devices	66
Change the polling method for a node	66
Change polling engine node assignments	66
Assign Universal Device Pollers (UnDPs) to monitored devices	67
View interface status and details about downtime periods	67
Change the time period for checking interface status	68
Edit the title and subtitle	68
Change how long the interface downtime history is retained	68
Disable interface downtime monitoring	68
Detect and predict possible duplex mismatches	68
How do I resolve mismatches?	69
Troubleshooting	69
Edit interface properties	70
Suspend and resume collecting data for interfaces, or show interface as Unplugged instead of Down	71
Suspend collecting data for interfaces	71
Resume collecting statistics for interfaces	71
Set the interface status as Unpluggable	71
Remotely manage monitored interfaces	71
Access nodes using HTTP, SSH, and Telnet	72
Group objects and mirror network dependencies in the Orion Web Console	72
Group monitored objects	72
Create groups	73
Edit group properties or change the group members	73
Add or remove group members	74
Delete groups	74

Set the group status based on the status of the group members	74
Mirror network object dependencies in the Orion Web Console	75
Create a dependency between network objects	75
Edit a dependency between network objects	76
Delete a dependency between network objects	77
View active alerts on child objects when the parent object is down	78
Monitor devices in the Orion Web Console	79
View events, alerts, traps, and syslogs in the Orion Web Console Message Center	79
View properties of all monitored nodes and interfaces in the Network Overview	79
View the resources and statistics monitored on a node	80
View network events in the Web Console	80
Filter the displayed logged events in the Web Console	80
Remove events from the Web Console	80
View notifications	81
Monitor hardware health	81
Monitored Hardware Sensors	82
Enable hardware health monitoring	82
Enable monitoring from the Add Node wizard	82
Enable hardware health monitoring on a node	82
Enable, disable, or adjust hardware health sensors	83
Update hardware health statistics	83
Enable hardware sensors	83
Disable hardware sensors	83
Edit hardware health thresholds	84
Change the MIB used for polling hardware health statistics	84
Change the MIB tree used for polling hardware health globally	84
Change the MIB for polling hardware health statistics on a specific node	85
Change hardware health temperature units	85
Monitor virtual infrastructure in the Orion Web Console	85

Prerequisites to monitoring virtual infrastructure	86
Create ESX server credentials for SolarWinds Orion products	86
Add virtual servers for monitoring	86
Assess the status of the virtual environment	87
View ESX host details	88
Assign credentials to virtual servers	88
Assign credentials to Hyper-V servers	88
Assign credentials to VMware servers	88
Change VMware credentials in the Orion Web Console	89
Poll ESX hosts controlled by vCenter servers directly	89
Monitor Quality of Experience metrics	90
How SolarWinds Packet Analysis Sensors work	91
Network Packet Analysis Sensor (NPAS)	91
Server Packet Analysis Sensor (SPAS)	91
Limitations to Packet Analysis Sensors	91
Common Packet Analysis Sensor deployment scenarios	92
Aggregation per application	93
Aggregation per site	94
Aggregation per computer	96
Monitor traffic to and from a port mirror, SPAN, or network tap	98
Monitor traffic to and from a specific node	100
Remove a sensor	101
Monitor QoE applications and nodes	101
Manage global QoE settings	101
Monitor applications for QoE	103
Monitor nodes with a network sensor	104
Ignore traffic from applications or nodes	105
Define custom HTTP applications	106
Advanced sensor configuration	107

Configure which interface to monitor for traffic	107
Set the number of CPU cores and the amount of memory QoE can use	108
Configure QoE thresholds	108
Packet Analysis Sensor agents	109
Monitor devices with SolarWinds Orion agents	109
Agent requirements	109
Agent resource consumption	110
Agent port requirements	111
Agent settings	111
Navigate to the Agent Settings page	111
Adjust the Global Agent Settings	111
Quality of Experience requirements	112
Network Packet Analysis Sensors (NPAS)	112
Server Packet Analysis Sensors (SPAS)	113
Remote computer port requirements	113
Server-initiated communication	113
Agent-initiated communication	114
Windows agent deployment	114
Deploy Windows agent software through a server push	115
Deploy the Windows agent manually	116
Mass deploy a Windows agent	116
Deploy with a Gold Master Image	117
Deploy a Windows agent with Patch Manager	118
Deploy on Windows Core Servers	122
Deploy Windows agents in the cloud	122
Certificates and the agent	124
Agent management	125
Manage Agents toolbar options	125
Manage Agents table columns	126

Edit agent settings	127
Track your polling method	127
View the status of agent plug-ins	128
Edit agent settings in the Windows Control Panel	129
Connect to a previously installed agent	129
Change the agent communication mode	130
Change the agent port	131
Agent polling method	131
Check nodes polling with agents for changes	131
Agent performance counters	132
SolarWinds: Agent Service	132
SolarWinds: Agent Management Service	132
Monitor Syslog messages	133
Before you begin	133
Configure the SolarWinds Orion server to use the correct syslog port	134
Syslog message priorities	134
Syslog facilities	134
Syslog severities	135
View Syslog messages in the Orion Web Console	136
Define the number of messages displayed, message retention, and the displayed columns in the Syslog Viewer	137
Clear Syslog messages in the Orion Web Console	137
View and clear Syslog messages in the Syslog Viewer	138
Search for Syslog messages in the Syslog Viewer	138
Trigger alerts when receiving specific Syslog messages	138
Forward syslog messages	140
Monitor SNMP traps	140
Before you begin	141
View SNMP traps in the Orion Web Console	141

View current traps in the Trap Viewer	141
Define how many traps to display, if you want to refresh the traps view, trap retention, and the information displayed in the Trap Viewer	142
Search for traps in the Trap Viewer	142
Configure Trap Viewer filters and alerts	142
What is a Trap Template?	144
Monitor capacity usage trends on the network and forecast capacity issues	144
Forecast capacity for nodes, interfaces, or volumes	145
Locate pending capacity problems	145
View capacity usage trends and forecast in graphs	145
View capacity usage trends and forecast in tables	145
Change capacity forecasting settings globally	146
Change calculation method and thresholds for nodes or volumes	146
Change calculation method and thresholds for interfaces	146
Customize capacity forecasting settings for single nodes, interfaces, or volumes	147
Monitor fibre channel devices and virtual storage area networks (VSANs)	148
Monitor custom statistics based on MIBs and OIDs with Universal Device Pollers	148
Define a custom statistic to monitor	149
Troubleshooting failed tests	150
Select nodes or interfaces to poll a custom statistic	151
Transform poller results	151
Create pollers by duplicating and adjusting pollers	153
Import UnDP pollers	153
Export UnDP pollers	154
Temporarily suspend collecting statistics for pollers	155
Define UnDP Warning and Critical thresholds	155
View Universal Device Poller statistics in the Orion Web Console	156
Define resources with UnDP results for Orion Web Console views	156
View UnDP status on maps	157

Cannot find OIDs? Update the SolarWinds MIB Database	157
Manage pollers using Device Studio	158
Manage unique devices on the network	158
Device Studio technologies	159
Data sources used in Device Studio	160
Create pollers in Device Studio	160
Define object identifiers (OIDs) that do not exist in the SolarWinds MIB database	162
What is the SNMP Get Type?	163
What is a formula?	163
Formulas used for transforming Device Studio poller results	163
Test Device Studio pollers	165
Monitor devices using thwack community pollers	165
Test thwack Device pollers	165
Import Device pollers from thwack	166
Import thwack community pollers to an environment without Internet connection	166
Export Device Studio pollers to the thwack community	166
Why can't I connect to thwack?	166
Assign Device Studio pollers to monitored devices	166
Scan monitored objects to verify if the OIDs match	167
Monitor F5 BIG-IP devices	167
Network Insight for F5® BIG-IP® load balancers	167
Set up Network Insight for F5® BIG-IP® load balancers	168
Requirements	168
Add F5 devices and enable iControl	168
Enable iControl on F5 load balancers	169
Monitor services delivered by F5® BIG-IP® load balancers	170
Status of F5 devices	172
F5 device status mapping to Orion status	173
F5 status in Orion	173

F5 high availability	174
F5 health monitors	176
Events, alerts, and reports for Network Insight for F5® BIG-IP® load balancers	177
Out-of-the-box alerts for F5 load balancers	177
Out-of-the-box reports	177
Take an F5 pool member out of rotation	178
Why shouldn't I start maintenance immediately after I take a pool member out of rotation?	178
Take a pool member out of rotation	178
Monitor wireless networks	179
Migrate data from the Wireless Networks Module	180
View wireless data in the Orion Web Console	180
Monitor EnergyWise devices	181
Add the EnergyWise Summary View to the Orion Web Console menu bar	181
Temporarily reset the current power level of a monitored EnergyWise interface	181
Set up and monitor Cisco Unified Computing Systems (UCS)	182
Monitor Cisco® SwitchStack®	183
View stack members and rings	183
View the health of stack members	184
Cisco SwitchStack events	185
Out-of-the-box alerts for SwitchStack	185
Create alerts based on SwitchStack events	185
Discover your network paths	187
Key features of NetPath™	187
How does NetPath™ work?	187
NetPath requirements	188
Probe computer	188
Orion integration	188
Ports	188
Database storage	189

Cloud environment	190
Scalability	190
Create a service	191
Create a new service	191
Probing interval	192
Create a probe	192
Create a probe	193
Assign additional probes	193
Probe troubleshooting	193
View a network path	193
Path layout	194
Path history	196
Troubleshoot a service with external path data	197
Troubleshoot my network with Orion path data	199
Orion integration with NetPath	201
NPM integration	201
NTA integration	201
NCM integration	202
View monitored objects on maps	203
Display nodes in the Worldwide Map of Orion Nodes resource	203
Place nodes automatically on the Worldwide Map	204
In what format should the location on a Cisco device be configured?	205
Place objects into the map using custom properties	205
Network Atlas	207
What can you see on maps?	207
What customization options are there?	207
Install Network Atlas	207
Network Atlas Requirements	207
Install Network Atlas on a remote computer	208

Start Network Atlas	208
Create network maps	209
Add objects on a map	209
Connect objects on maps automatically with ConnectNow	210
Connect objects on maps manually	211
Reshape map links	211
Configure display of connections on maps	211
Add a background	213
Save maps	215
Open maps	215
Create wireless heat maps	215
Disable the wireless heat map poller	216
Set a floor plan as the background	217
Set the wireless heat map scale	217
Add wireless access points	218
Improve the accuracy of wireless heat maps by taking samples of the signal strength on real devices	218
Troubleshoot wireless heat maps	220
Advanced mapping techniques	220
Zoom in and out of a map	221
Create nested maps	221
Display the status of child objects on maps, and change metric thresholds	222
Add independent map objects and floating labels	222
Change the appearance of map objects	222
Customize the width, color, and line styles of network links in maps	225
Customize labels	225
Customize the page that opens when you click on a map object	226
Link or embed maps in web pages using the map URL	226
Customize map tooltips	226

Set when a map is displayed as Up on parent maps using the Up status threshold	226
Display restricted nodes for users with account limitations	227
Advanced map layouts	227
Position map objects	227
Display grid	228
Align map objects	228
Distribute map objects	228
Arrange map objects according to a layout style	229
Display Network Atlas maps in the Orion Web Console	229
Display wireless heat maps in the Orion Web Console	230
Change the time and frequency for regenerating the map	230
View the location of clients connected to access points in maps	230
Limit the number of clients displayed on the map	231
Use alerts to monitor your environment	232
Alert preconfiguration tasks	232
Configure the default information in the email action	233
Best practices and tips for alerting	233
Navigate to the Alert Manager	234
Create new alerts to monitor your environment	234
Set alert properties	234
Define the conditions that must exist to trigger an alert	235
Define the conditions that must exist to reset an alert	237
Schedule when an alert monitors your environment	238
Define what happens when an alert is triggered	239
Add actions to alerts	239
Add what happens when an alert is not acknowledged	240
Define what happens when the alert is reset	241
Review the alert's configuration	242
Commonly created alerts	242

Alert me when a server goes down	242
Discover network device failures	243
Alert on custom properties	244
View triggered alerts in the Orion Web Console	245
Remove alerts from the Active Alerts list	245
Test alert triggers and actions	245
Test trigger conditions	245
Test alert actions while creating or editing an alert	245
Test alert actions in the Action Manager	246
Modify multiple alerts or share alerts	246
Add actions to alerts without opening the Alert Wizard	246
Share alerts with others	247
Build complex conditions	247
Wait for multiple objects to meet the trigger condition	247
Evaluate multiple condition blocks	248
Evaluate multiple object types	248
Manage alert actions	249
Assign an action to an alert	249
Enable and Disable Alerts	249
Available alert actions	249
Change a custom property	249
Dial a paging or SMS service	250
Email a web page to users	250
Create a dynamic URL	250
Execute an external batch file	251
Execute an external Visual Basic script	251
Log the alert message to a file	252
Log the alert to the NPM event log	252
Change the resource allocation of a virtual machine	253

Delete a snapshot of a virtual machine	254
Move a virtual machine to a different host	254
Move a virtual machine to a different storage	255
Pause a virtual machine	256
Power off a virtual machine	256
Power on a virtual machine	257
Restart a virtual machine	258
Suspend a virtual machine	258
Take a snapshot of a virtual machine	259
Play a sound when an alert is triggered	259
Send a Windows Net message	260
Restart IIS sites or application pools	261
Send an SNMP trap	261
Send a GET or POST request	262
Send a syslog message	263
Send an email or page	263
Manually set a custom status	264
Use the speech synthesizer to read alerts	265
Log an alert to the Windows Event Log on a specific server	265
Create a ServiceNow incident	266
Changes in the alerting engine	267
Changed or removed functionality	267
Database changes	267
Macro or variable changes	268
Alert migration to the web	268
Migration issues	268
Limitations to migrated alerts	268
Share alerts with other SolarWinds products	269
Configure ServiceNow	269

Integrate an Orion Platform product with ServiceNow	269
Before you begin	269
Install and configure the SolarWinds Alert Integration application in ServiceNow	270
Create a ServiceNow integration user with Web service access only	270
Configure an Orion Platform product with ServiceNow	270
Configure web proxy settings	271
How conditions are evaluated	271
General alert variables	272
Defunct alert variables	273
Manage the Orion Web Console	275
Log in to the Orion Web Console	275
Manage Orion Polling Engines	275
Use Additional Polling Engines	275
Required Settings	275
View a polling engine status	276
Update polling settings	276
Configure polling interval settings	276
Configure polling statistics intervals	277
Configure the dynamic IP address and hostname resolution	277
Configure Database Settings	278
Configure network settings	280
Configure calculations and threshold settings	281
Calculate node availability	282
Node Status	282
Percent Packet Loss	282
Define baselines for nodes	283
Define a baseline for an individual node	283
Define a baseline for multiple nodes	283
Assign credentials to virtual servers	283

Assign credentials to Hyper-V servers	283
Assign credentials to VMware servers	284
Set general thresholds	284
Set how many retries are necessary before packet loss is reported	284
Set the node warning level	285
Delete polling engines	285
Thresholds	286
Set general thresholds	286
Customize thresholds for single objects	287
General threshold types	287
Baselines and baseline calculations	289
What data is subject to statistical baseline calculation?	289
Use mean and standard deviations as thresholds	289
Customize how the baseline is calculated	290
Set SolarWinds NPM thresholds	290
Define UnDP Warning and Critical thresholds	291
Manage Orion Web Console user accounts	292
Create users	292
Create users based on existing Active Directory or local domain accounts	293
Change account passwords	295
Enable users to authenticate through LDAP	295
Define what users can access and do	296
Set default menu bars and views for users	298
Limit users to specific network areas	299
Restrict user access to network areas by applying limitations	299
Patterns for limitations	300
Create limitations based on custom properties	300
Delete account limitations	300
Configure automatic login	301

Enable Windows Authentication with Active Directory	301
Log in with Windows pass-through security	304
Share views with non-Orion Web Console users	304
Automatically login by passing your credentials through the URL	305
Administrative functions	305
View secure data	305
Handle counter rollovers	305
Configure web proxy settings	306
Orion Web Console and chart settings	307
Web Console settings	307
Auditing settings	308
Chart settings	309
Discovery, Worldwide Map, and Active Alerts settings	309
Active Alerts settings	309
Custom properties	310
Create a custom property	310
Remove a custom property	312
Import custom property values	313
Export custom property data	314
Change custom properties values	314
Edit values for custom properties	314
Filter objects when assigning custom properties	314
Manage the Orion Web Console	316
Customize the Orion Web Console look, views, settings, charts, and maps	316
My Dashboards	316
Customize My Dashboards	317
Specify My Dashboards and Alerts & Activity items for users	317
Add items to My Dashboards	318
Add menu bars	319


Change the Orion Web Console color scheme	320
Change the Orion Web Console logo	320
Use Orion Web Console breadcrumbs	321
Customize breadcrumbs	321
Create, delete, modify, or restrict views	321
Create new views	321
Create views	322
Add resources and columns to views, and define subviews	323
Add resources to the view	323
Add columns	324
Change column width	325
Move resources on views	325
Divide content into subviews	325
Create custom summary views	326
Add external website views	328
Optimize views for TV screens or mobile devices	329
Limit objects on a view	330
Use a view as a template	331
Delete views	331
Specify views for device types	331
Export views to PDF	331
Customize resources in the Orion Web Console	331
Resource configuration examples	332
Display a Network Atlas map in the Orion Web Console	332
Display a list of objects on a network map	332
Display a custom list of available maps	332
Display the Worldwide Map	333
Display events received during a given time period	333
Specify user-defined links	333

Specify Custom HTML	334
Filter nodes	334
Group nodes within a view	335
Add a Service Level Agreement Line to charts (SolarWinds NPM)	335
Filter nodes in resources using SQL queries	336
SQL Query Examples	336
Specify what a Custom Object resource displays	336
Customize charts in the Orion Web Console	337
Drop-down customization options	337
Edit Resource page	337
Custom Chart page	338
Maintain the SolarWinds Orion database	340
Back up and restore the database	340
View database details and data in the Database Manager	340
Add a server to Database Manager	341
View database details	341
View table details	341
Edit database fields	342
Run the database maintenance	343
Best practices and troubleshooting for SolarWinds Orion database	343
Adjust how long you want to keep historical data	343
Design a database maintenance plan	344
Prevent fragmentation problems	344
Troubleshooting	344
Prepare to upgrade or migrate the SolarWinds Orion database	345
Requirements	345
Upgrade your SQL Database	346
Update Orion Platform products to use the new database	346
Create and view reports	348

Predefined reports	348
Create, schedule, export, and import reports in the Orion Web Console	348
Create reports in the Orion Web Console	348
Modify an existing web-based report	348
Create a new web-based report	349
Customize a web-based report layout	352
Add content to a web-based report	353
Add a custom chart or table to a web-based report	353
Add a data series and customize a chart	354
Add a data series and customize a table	355
Build conditions	356
Restrict who can access reports	356
Create or add a report limitation category	357
Restrict user access to the report	357
Generate reports on a schedule	357
Schedule a report to run automatically while creating or editing a report	357
Create and assign report schedules in Report Manager	358
Schedule reports from the Schedule Manager	359
Export reports	360
Export reports as XML	360
Import XML reports	360
Export Excel and PDF reports from the Orion Web Console	360

Prepare a SolarWinds Orion Platform installation

Orion Platform products use a simple wizard to direct the installation process.

 Downgrades of Orion Platform products are not supported. If you are upgrading or installing multiple products, confirm that you are installing them in the order given in the upgrade instructions located in your [SolarWinds Customer Portal](#) or in the Upgrade Guide.


SolarWinds Orion Platform requirements


These minimum requirements are for the Orion Platform. Products that run on the Orion Platform may have different requirements, such as different OS or memory requirements. Consult your product-specific documentation for the exact requirements.



See [SolarWinds Port requirements](#) for a comprehensive list of port requirements for SolarWinds products.

SolarWinds Orion server software requirements

The following table lists minimum software requirements and recommendations for a SolarWinds Orion Platform installation.

- 
- Beginning with Orion Platform 2016.1, you can only install on Windows Server 2008 R2 SP1, 2012, and 2012 R2.
 - SolarWinds does not support installing SolarWinds Orion on domain controllers.
 - SolarWinds neither recommends nor supports the installation of any Orion product on the same server or using the same database server as a Research in Motion (RIM) Blackberry server.

SOFTWARE	REQUIREMENTS	
	Production	Evaluation Only
Operating system	<ul style="list-style-type: none">■ Windows Server 2008 R2 SP1■ Windows Server 2012 and 2012 R2	<ul style="list-style-type: none">■ Windows 7 SP1■ Windows 8 (except for Standard Edition)■ Windows 8.1 (except for Standard Edition)■ Windows 10
	 Installing SolarWinds Orion on Windows Server 2012 R2 Essentials is not supported.	

SOFTWARE	REQUIREMENTS
Operating system languages	<ul style="list-style-type: none"> ■ English (UK or US) ■ German ■ Japanese ■ Simplified Chinese
IP address version	<p>IPv4</p> <p>IPv6 implemented as a dual stack. For more information, see RFC 4213 - Basic Transition Mechanisms for IPv6 Hosts and Routers.</p> <div>  CIDR notation is not supported for IPv6 addresses. </div>
Web server	<p>Microsoft Internet Information Services (IIS), version 7.5 or later, in 32-bit mode</p> <div>  <ul style="list-style-type: none"> ■ DNS specifications require that host names be composed of alphanumeric characters (A–Z, 0–9), the minus sign (–), and periods (.). Underscore characters (_) are not allowed. For more information, see RFC 952 - DOD Internet Host Table Specification. ■ IIS is installed by the SolarWinds installer. You can install this software manually to reduce your installation time or network bandwidth. ■ SolarWinds products are not compatible with IIS version 6.0 installations that use web gardens. </div>
.NET Framework	<p>.NET 4.5</p> <p>Compatible with 4.6.1</p>
Web console browser	<ul style="list-style-type: none"> ■ Microsoft Internet Explorer version 11 or later with Active scripting ■ Microsoft Edge ■ Firefox 44.0 or later (Toolset Integration is not supported on Firefox) ■ Chrome 48.0 or later ■ Safari for iPhone
Other	MSMQ
Services	<p>The following services must be running after installation is complete to collect syslog messages and traps:</p> <ul style="list-style-type: none"> ■ SolarWinds Syslog Service ■ SNMP Trap Service
User privileges	SolarWinds recommends that administrators have local administrator privileges to ensure full functionality of local SolarWinds tools. Accounts limited to the Orion Web Console do not require administrator privileges.

Server port requirements


- 25 (TCP) SMTP port for non-encrypted messages
- 161 (UDP) for statistics collection
- 162 (UDP) for Trap Server listening for incoming messages
- 443 (TCP) default port for https binding and bi-directional ESX/ESXi server polling and for Cisco UCS monitoring
- 465 (TCP) for SSL-enabled email alert actions
- 587 (TCP) for TLS-enabled email alert actions
- 1801 (TCP) for MSMQ WCF binding
- 5671 (TCP) for RabbitMQ messaging
- 17777 (TCP) open for Orion module traffic
- 17778 (HTTPS and TCP) open to access the SolarWinds Information Service API and agent communication
- 17779 (HTTP and HTTPS) for the SolarWinds Toolset Integration
- 17791 (TCP) open for agent communication on any SolarWinds Orion server running Windows Server 2008 R2 SP1


SolarWinds Orion server hardware requirements

The following table lists minimum hardware requirements and recommendations for your SolarWinds Orion server.

Installing multiple SolarWinds Orion Platform products on the same computer may change the requirements.

 Hardware requirements are listed by SolarWinds NPM license level.

HARDWARE	SL100, SL250, SL500	SL2000	SLX
CPU speed	Quad core processor, 2.5 GHz or better	Quad core processor, 2.5 GHz or better	Quad core processor, 3.0 GHz or better
 Do not enable Physical Address Extension (PAE).			

HARDWARE	SL100, SL250, SL500	SL2000	SLX
Hard drive space	2.5 GB minimum	5 GB minimum	20 GB minimum
	 Two 146 GB 15K (RAID 1/Mirrored Settings) hard drives are recommended with a dedicated drive for the server operating system, Orion Platform product installation, and tempdb files.		
	<p>The Orion installer needs 1 GB on the drive where temporary Windows system or user variables are stored.</p> <p>Some common files may need to be installed on the same drive as your server operating system. You may want to move or expand the Windows or SQL temporary directories.</p>		
Memory	4 GB minimum	8 GB minimum	16 GB minimum
	8 GB recommended	16 GB recommended	32 GB recommended

Server sizing recommendations

Listed from the most important to the least important are the primary variables that affect scalability.

Number of monitored elements

An element is defined as a single, identifiable node, interface, or volume. A single polling engine can monitor up to 12,000 elements. Monitoring some node types, such as routers, place more load on the system.

Polling frequency

If you are collecting statistics every five minutes instead of the default nine minutes, the system will have to work harder and system requirements will increase.

Number of simultaneous users

The number of simultaneous users accessing SolarWinds Orion directly impacts system performance. We recommend limiting the number of simultaneous users to between 10 to 20 sessions per web site. You can install additional web sites to handle larger user loads.

Recommendations

When planning a SolarWinds Orion installation, there are four main factors that limit your polling capacity:

- CPU
- Memory
- Number of polling engines
- Polling engine settings

Be aware of these variables, and consider the following SolarWinds recommendations:

Install your SolarWinds Orion product and SolarWinds Orion database on different servers

If you plan to monitor 2,000 elements or more, SolarWinds recommends that you install your product and your database on different servers. Separate servers for the product and the database improve the performance, as the product server does not perform any database processing, and it does not have to share resources with the database server.

Use additional polling engines for 10,000 or more monitored elements


If you plan to monitor 10,000 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 SolarWinds Orion to your network, view the *Scalability Engine Guidelines* for your product in the [SolarWinds Success Center](#), [contact the SolarWinds sales team](#), or visit www.solarwinds.com.


For minimum hardware recommendations, see [SolarWinds Orion server hardware requirements](#).




SolarWinds Orion database server (SQL Server) requirements


Your Orion Platform product and your SolarWinds Orion database should use separate servers.

 Multiple SolarWinds Orion server installations using the same database are not supported.

The following table lists software and hardware requirements for your SolarWinds Orion database server using SolarWinds NPM license levels as a reference.

REQUIREMENTS	SL100, SL250, SL500	SL2000	SLX
SQL Server	<p>SolarWinds supports Express, Standard, or Enterprise versions of the following:</p> <ul style="list-style-type: none">■ SQL Server 2008, 2008 SP1, 2008 SP2, 2008 SP3, or 2008 SP4■ SQL Server 2008 R2, 2008 R2 SP1, 2008 R2 SP2, or 2008 R2 SP3■ SQL Server 2012, 2012 SP1, 2012 SP2, or 2012 SP3 (also with AlwaysOn Availability Groups)■ SQL Server 2014 (also with AlwaysOn Availability Groups) or 2014 SP1■ SQL Server 2016 <div><ul style="list-style-type: none">■ The FullWithSQL installer package automatically installs SQL Server 2014 Express. This is recommended for evaluations.■ Set the recovery model of the database to Simple. SolarWinds does not support other methods.■ SQL Server Compact Edition 3.5 SP2 is only supported for evaluations.</div>		


REQUIREMENTS	SL100, SL250, SL500	SL2000	SLX
	<p> ■ Due to latency effects, SolarWinds does not recommend installing your SQL Server and your Orion server or additional polling engine in different locations across a WAN. For more information, see Install SolarWinds software and SolarWinds database (SQL Server) across a WAN.</p>		
SQL Server collation	<ul style="list-style-type: none"> ■ English with collation setting SQL_Latin1_General_CP1_CI_AS ■ English with collation setting SQL_Latin1_General_CP1_CS_AS ■ German with collation setting German_PhoneBook_CI_AS ■ Japanese with collation setting Japanese_CI_AS ■ Simplified Chinese with collation setting Chinese_PRC_CI_AS <p> We support CI database on an CS SQL Server.</p> <p> We do not support case-sensitive databases.</p>		
CPU speed	Dual quad core processor, 3.0 GHz or better	Dual quad core processor, 3.0 GHz or better	Dual quad core processor, 3.0 GHz or better
Hard drive space	<p>20 GB minimum</p> <p>Mirrored drives for the OS and 6 disk RAID 1+0 for database data files is recommended.</p>	<p>50 GB minimum</p> <p>Mirrored drives for the OS and 6 disk RAID 1+0 for database data files is recommended.</p>	<p>100 GB minimum</p> <p>SolarWinds recommends the following configuration:</p> <ul style="list-style-type: none"> ■ A hardware RAID Controller with a battery backed-up write back cache ■ Disk Subsystem 1 Array 1: 2 x 146 GB 15K disks RAID 1 (mirroring) for the OS ■ Disc Subsystem 2 Array 2: 2 x 146 GB 15K disks RAID 1 (Pagefile + Extra Storage) ■ Disk Subsystem 3 Array 3: with 6x 15k 146 GB or 300 GB disks configured in a RAID 1+0 array to allow for maximum write performance for your SQL MDF and FILEGROUPS.

REQUIREMENTS	SL100, SL250, SL500	SL2000	SLX
			<ul style="list-style-type: none"> ■ Disk Subsystem 4 Array 4: with 4x 15k 146 GB or 300 GB disks configured in a RAID 1+0 array to allow for maximum write performance for your SQL LDF Transaction LOG file
	<p> Due to intense I/O requirements, a RAID 1+0 drive is strongly recommended for the SolarWinds database, data, and log files. RAID 5 is not recommended for the SQL Server hard drive.</p>		
	Per Windows standards, some common files may need to be installed on the same drive as your server operating system.		
Memory	4 GB minimum 8 GB recommended	8 GB minimum 16 GB recommended	16 GB minimum 32 GB recommended
Authentication	Either mixed-mode or SQL authentication		
Other software	<p>If you are managing your SolarWinds Orion database, SolarWinds recommends you install the SQL Server Management Studio component.</p> <p>The Installation Wizard installs the following required x86 components if they are not found on your Orion database server:</p> <ul style="list-style-type: none"> • SQL Server System Common Language Runtime (CLR) Types. Orion products use 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 		

SQL Server configuration best practices

The standard SQL environment for Orion Platform products contains the following components:

- A dedicated SQL Standard or Enterprise Server
- Directly attached (DAS), RAID 10 storage (I/O subsystem)
- LAN attachment between the main Orion server and any additional components

 If there are more databases on a given SQL Server, it is strongly recommended that you use dedicated hard drives for the tempdb database. Use at least one hard drive for data files, and one hard drive for the transaction log. All databases use the same tempdb, therefore the tempdb can be the biggest bottleneck in the I/O subsystem.

Maximizing SQL Server performance

When planning your SQL Server configuration, consider the following information:

- SQL Express is only suitable for small SolarWinds Orion installations without NTA. NetFlow can be a major factor in database sizing, depending on the incoming flow rates.
- WAN connections should never be used between the SQL server and the SolarWinds Orion server. This includes any additional pollers.
- Do not install the SQL Server on the Orion server.
- The performance of the SQL Server is dependent on the performance of the I/O subsystem.
- The more disks there are in a RAID 10 array, the better.
- Many RAID controllers do not handle RAID 01 well.

Hardware settings for SQL Servers

The following section contains the recommended hardware settings for SQL Servers, taking into account different scenarios and the number of logical disks you use.

Recommendations for maximum performance

COMPONENT	RECOMMENDATION
Orion database	<ul style="list-style-type: none">■ A dedicated RAID 1+0 hard drive for data files (.mdf, .ndf).■ A dedicated RAID 1+0 hard drive with fast sequential writing for transaction files (.ldf).
SQL Server temporary directory (tempdb) database	<ul style="list-style-type: none">■ A dedicated RAID 1+0 hard drive for data files (.mdf, .ndf).■ A dedicated RAID 1+0 hard drive with fast sequential writing for transaction files (.ldf).
SQL Server host system (Windows)	<ul style="list-style-type: none">■ A dedicated hard drive of any type.

Recommendations for four HDDs

COMPONENT	RECOMMENDATION
Orion database	<ul style="list-style-type: none">■ A dedicated RAID 1+0 hard drive for data files (.mdf, .ndf).■ A dedicated RAID 1+0 hard drive with fast sequential writing for transaction files (.ldf).
SQL Server temporary directory (tempdb) database	<ul style="list-style-type: none">■ A dedicated hard drive for data files (.mdf, .ndf) and the transaction log (.ldf)
SQL Server host system (Windows)	<ul style="list-style-type: none">■ A dedicated hard drive of any type. This hard drive should be the slowest of the four available disks.

Recommendations for three HDDs

COMPONENT	RECOMMENDATION
Orion database	<ul style="list-style-type: none">■ A dedicated RAID 1+0 hard drive for data files (.mdf, .ndf).■ A dedicated RAID 1+0 hard drive with fast sequential writing for transaction files (.ldf).
SQL Server temporary directory (tempdb) database and SQL Server host system (Windows)	<ul style="list-style-type: none">■ A dedicated hard drive for tempdb data files (.mdf, .ndf), tempdb transaction log (.ldf), and host system.

Recommendations for two HDDs

- Use the disk with the faster sequential writing for the host system and for the transaction log files (.ldf).
- Use the other disk for data files (.mdf, .ldf), for the tempdb data files, and for the tempdb log files.

Recommendations for multi-CPU systems and the optimal settings of the I/O subsystem

On multi-CPU systems, the performance of some operations can be increased by creating more data files on a single hard drive.

 Every logical CPU is considered to be one CPU.


The following example shows the original settings of a system with 16 CPU cores:

- One hard drive for data with the `SolarWindsOrionDatabase.MDF` file in the Primary filegroup.
- One hard drive for the transaction log with the `SolarWindsOrionDatabase.LDF` file.
- One hard drive for the tempdb data with the `tempdb.MDF` file in the Primary filegroup.
- One hard drive for the tempdb transaction log with the `tempdb.LDF` file.

The previous settings can be improved in the following way:

- One hard drive for data, with the following files in the Primary file group:
 - `SolarWindsOrionDatabase01.MDF`
 - `SolarWindsOrionDatabase02.MDF`
 - `SolarWindsOrionDatabase03.MDF`
 - `SolarWindsOrionDatabase04.MDF`
- One hard drive for the transaction log with the `SolarWindsOrionDatabase.LDF` file.

- One hard drive for tempdb data, with the following files in the Primary filegroup:
 - tempdb01.MDF
 - tempdb02.MDF
 - tempdb03.MDF
 - tempdb04.MDF
- One hard drive for the tempdb transaction log with the tempdb.LDF file.

-  ■ Having more files in the filegroup help the SQL Server to distribute the load generated by multiple threads while working with files.
- The recommended ratio between the number of cores and the files in the filegroup is typically 4:1 or 2:1 (for example, 16 cores and four files, or 16 cores and eight files).
- The size and growth setting for all files in a filegroup must be set to identical values in order to distribute the load evenly.
- For the transaction log, it is not effective to create more files, because the SQL Server can only use the first file.
- For the tempdb database, a RAM disk or an SSD disk can be used.
- An SSD disk can be used for data files, but it is not effective for the transaction log where sequential access is most important.

Database file setting recommendations

- Pre-allocate as much disk space as possible to save time.
- Define an absolute auto-growth setting with a reasonable size (500 MB, 1 GB, and so on), instead of an auto-growth percentage.

Memory setting recommendations


- Do not reserve all memory to the SQL Server, because this can lead to a lack of memory for the host operating system.
- Reserve 1 GB of memory to the host operating system if there are no additional services running on the given host system.
- If additional resource-intensive services are running on the host operating system, reserve sufficient memory for the host operating system. SolarWinds does not recommend such configuration.

CPU setting recommendations

- Ensure that power-saving technologies are disabled on the CPU.

Virtual machines and servers requirements

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

 You must maintain your SQL Server database on a separate, physical server.

VM CONFIGURATION	REQUIREMENTS BY NPM LICENSE LEVEL FOR REFERENCE		
	SL100, SL250, or SL500	SL2000	SLX
CPU speed	Quad core processor, 2.5 GHz or better	Quad core processor, 2.5 GHz or better	Quad core processor, 3.0 GHz or better
Allocated hard drive space	2.5 GB minimum	5 GB minimum	20 GB minimum
	💡 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	4 GB minimum	8 GB minimum	16 GB minimum
	8 GB recommended	16 GB recommended	32 GB recommended

Requirements for monitoring Microsoft Hyper-V, VMware ESXi, and ESX Servers

REQUIREMENT	DESCRIPTION
SNMP	SNMP must be enabled on all ESXi and ESX servers. For more information, consult your ESX or ESXi server vendor documentation.
Virtualization software	ESXi and ESX Server version 4.1 or later VMware vSphere version 4.1 or later Microsoft Hyper-V Server versions 2008 R2, 2012, 2012 R2
VMware tools	VMware Tools must be installed on all virtual machines you want to monitor. If your virtual machines are on monitored ESXi and ESX servers, VMware Tools are not a requirement but provide access to additional information, such as IP addresses.

❗ For more information about requirements, see [VIM Minimum Requirements](#) in the SolarWinds Virtual Manager documentation.

The following methods are used by SolarWinds Orion to monitor VMware ESX Servers and their component features.

FEATURES	4	4i	5i	6.0
Datacenter	VMware API			
ESX cluster	VMware API			
Virtual Center	VMware API			
Detection as ESX server	VMware API			
Volumes	SNMP	N/A	SNMP	

FEATURES	4	4i	5i	6.0
Interfaces	SNMP	SNMP (partial)	SNMP	
CPU	VMware API			
Memory	VMware API			
Total CPU (ESX details view)	VMware API			
Total memory (ESX details view)	VMware API			
Network traffic utilization (ESX details view)	VMware API			
Guest VM list (ESX details view)	VMware API			

Security enhancements and exceptions for SolarWinds Orion Platform products

By default, SolarWinds Orion Platform products use the http protocol instead of https. You can increase the security of your data by using SSL or FIPS.

- [Enable secure channels with SSL](#)
- [Enable FIPS](#)

For best performance, SolarWinds also recommends creating an [antivirus directory exclusion](#) for the SolarWinds install folder.

Enable secure channels with SSL

SolarWinds Orion Platform products support the use of Secure Sockets Layer certificates to enable secure communications with the Orion Web Console.

Requirements

- Your server must have the required SSL certificate installed.
- Conduct secure SSL/TLS communications over port 443.




Due to security concerns, SolarWinds recommends that you disable SSL v3.0 and earlier.

1. Add a binding to https port 443 for the SolarWinds NetPerfMon site. For more information, consult the Microsoft online documentation on setting up SSL.
2. [Enable the Orion Web Console for SSL](#).
3. You can also [configure the Orion Web Console to require SSL](#).

Configure the Orion Web Console for SSL

1. Log in to your SolarWinds Orion server using an account with administrative rights.
2. Shut down all SolarWinds services. Start the Orion Service Manager in the SolarWinds Orion > Advanced Features program folder, and click Shutdown Everything.
3. Start the Database Manager from the SolarWinds Orion > Advanced Features program folder.
4. Expand the SQL servers, and navigate to SQL Servers > your SolarWinds Orion database server > SolarWindsOrion > Websites in the left pane.
 - If your SQL Server is not listed in the left pane, click Add Default Server.
 - If your Orion database is not listed in the left pane, add it:
 - a. Click Add SQL Server.
 - b. Using the format `Server/Instance`, select or provide the SQL Server instance you are using as your SolarWinds Orion database.
 - c. Select the login method, providing credentials as required.
 - d. Click Connect to Database Server.
5. Right-click the Websites table, and click Query Table.
6. Replace the default query with the following query, and click Refresh.


```
UPDATE dbo.Websites SET SSLEnabled=1 WHERE WebsiteID=1
```
7. Switch to the Orion Service Manager, and click Start Everything.
8. Change the Orion Web Console port.
 - a. Start the Configuration Wizard in the SolarWinds Orion > Configuration and Auto-Discovery program folder.
 - b. Select Website, and click Next on the Welcome window.
 - c. Enter the SSL port number, and click Next.

 Port 443 is typically reserved for SSL traffic.

- d. Review the configuration summary, and complete the Configuration Wizard.

Configure the Orion Web Console to require SSL

1. In a text editor, open the web console configuration file, `web.config`, on your primary SolarWinds server.

 The default location of `web.config` is `C:\Inetpub\SolarWinds\`.

2. In the `<system.web>` section, add the line:

```
<httpCookies requireSSL="true" />
```
3. Locate the line:

```
<forms loginUrl="~/Orion/Login.aspx" />
```
4. Edit it to `<forms loginUrl="~/Orion/Login.aspx" requireSSL="true" />`.
5. To enable the HTTPOnly flag for added security, locate the `<httpCookies>` tag, and edit it to the following:


```
<httpCookies httpOnlyCookies="true" requireSSL="true" />
```
6. Save and close `web.config`.

Enable FIPS


FIPS (Federal Information Processing Standard) defines security and interoperability standards for computers used by the U.S. federal government.

Monitored nodes and network discoveries must use FIPS-compliant authentication and privacy or encryption methods.

FIPS-COMPLIANT METHODS	
Authentication	SHA1
Privacy or encryption	AES128, AES192, AES256

 SolarWinds recommends that you install all FIPS-compliant SolarWinds software on FIPS-compliant servers and maintain all non-compliant SolarWinds software on non-compliant servers.


1. Configure the Orion Platform product server for FIPS compliance. See the Microsoft Support knowledge base for more information.
2. Start the SolarWinds FIPS 140-2 Manager (`SolarWinds.FipsManager.exe`).

 By default, `SolarWinds.FipsManager.exe` is located in the `Install_Volume:\Program Files (x86)\SolarWinds\Orion` folder.

3. Read the welcome text, and click Next.

The SolarWinds FIPS 140-2 Manager will confirm that the current configuration of your SolarWinds products is FIPS-compliant.

- If an installed Orion Platform product is not FIPS-compliant, click Close, remove any non-compliant Orion Platform products from the FIPS-compliant server, and run the FIPS 140-2 Manager again.
- If FIPS 140-2 is disabled, select Enable FIPS 140-2, and click Next.
- If the FIPS Manager provides a list of objects or saved network discovery definitions that are not FIPS-enabled, complete the following steps.


 To refresh the list of non-compliant objects after editing the credentials, restart the FIPS 140-2 Manager.

- Click the non-compliant monitored node, and edit its Polling Method to be FIPS-compliant.
 - a. Select SNMPv3 as the SNMP Version.
 - b. Select FIPS-compliant Authentication and Privacy/Encryption methods, and provide the passwords.
 - c. Click Submit.
- Click the non-compliant network discovery, and edit SNMP credentials to be FIPS-compliant.
 - a. Confirm that all SNMP credentials are SNMPv3. Delete or edit any credentials that are not FIPS-compliant SNMPv3.
 - b. Confirm that all SNMP credentials use FIPS-compliant Authentication and Privacy/Encryption methods, and provide the passwords.
 - c. Complete the Network Sonar Wizard using the updated credentials.

4. Click Restart now to restart all relevant SolarWinds services.

Antivirus directory exclusions

Ensure that all Orion Platform products have access to all required files by excluding the following directory from antivirus protection.

- 
- Do not exclude executable files.
 - SolarWinds assumes that C:\ is the default install volume.

C:\ProgramData\SolarWinds\

Uninstall SolarWinds NPM

This is a general uninstall procedure, and it may differ slightly from version to version.

SolarWinds recommends to use this procedure when installing daily builds for testing.

1. Click Start > Control Panel > Add or Remove Programs.
2. One-by-one, select the following items, click Remove for each of them, and complete the uninstall wizard:
 - SolarWinds Network Performance Monitor...
 - SolarWinds Job Engine
 - SolarWinds Orion Information Service
3. Start the Registry Editor, and delete SolarWinds-specific folders.
 - a. Click >Start > Run...
 - b. Type `regedit`, and click OK.
 - c. Expand `HKEY_LOCAL_MACHINE > Software`.
 - d. Delete both the SolarWinds and the SolarWinds.net folders.

If you are uninstalling SolarWinds NPM from a 64-bit computer, expand `HKEY_LOCAL_MACHINE > Software > Wow6432Node`, and delete both the SolarWinds and the SolarWinds.net folders.
4. Delete the SolarWinds-specific folders in the following locations:
 - Delete the Program Files folder on your main volume. Typically, the Program Files folder is located at `C:\Program Files\`.
 - Delete the Program Files\Common Files folder on your main volume. Typically, the Common Files folder is located at `C:\Program Files\Common Files\`.
 - Delete the All Users\Application Data\ directory. Typically, this SolarWinds folder is located in `C:\Documents and Settings\All Users\Application Data\`.
 - Delete the SolarWinds website directory. Typically, the SolarWinds website directory is located in `C:\Inetpub\`.
5. Using your SQL Server tools, delete your SolarWinds Orion database and your Orion database user.
 - The SolarWinds Orion database is typically named SolarWindsOrion, and it can be found in the Databases folder of your SQL Server management application.
 - The default SolarWinds Orion database user is SolarWindsNPM. To find the user, expand Security > Logins in your SQL Server management application.

SolarWinds Orion Platform products licensing

Orion Platform products are licensed additively, in terms of monitored nodes.

For example, if you purchase SolarWinds NPM with an SL100 license and SolarWinds SAM with an AL50 license, use the following to calculate how many nodes or components you can monitor:


- The NPM SL100 license monitors up to 100 nodes.
- The SAM AL50 license monitors up to 50 nodes and/or components.

When you purchase both licenses, you can monitor the performance of both interfaces and applications on a total of 150 unique nodes or components because the SAM license adds 50 to the 100 nodes allowed with your NPM license.

For more information, see the administrator guide of your specific Orion Platform product.


Activate your SolarWinds license

When you install your Orion Platform product, you are prompted to provide your licensing information (software license key and customer data), and activate your product.


 To postpone the activation, click Continue Evaluation. You can [activate the license](#) later, with the License Manager.

Activate licenses with Internet access


1. On the Activate Product window, select I Have Internet Access...
2. Find your activation key in the customer portal, and enter it in the Activation Key field.
 - a. Browse to <https://customerportal.solarwinds.com>, and then log in using your Customer ID and password, or your individual user account information.

 If you do not know your SolarWinds Customer ID and password or individual profile details, contact Customer Support and [submit a ticket](#).
 - b. Under the Licensing Management section on the top bar, select License Management.
 - c. Browse to the SolarWinds product, and click the plus sign next to the product to display your activation key.
 - d. Copy your unregistered activation key for the SolarWinds product to the clipboard, and paste it into the Activation Key field in the Activate window.
3. If you are using a proxy server to access the Internet, select I Access the Internet Through a Proxy Server, and enter the proxy address and port number.
4. Click Next.
5. Provide your customer data, and complete the Activation Wizard.

Activate licenses offline

1. On the Activate Product window, select This Server Does Not Have Internet Access, and click Next.
 2. To finalize your registration, click Copy Unique Machine ID.
 3. Paste the data into a new document in a text editor, and save the text document.
 4. Transfer the document to a computer with Internet access. For example, transfer the document to a shared location.
 5. Log in to the SolarWinds customer portal and find your activation key:
 - a. Browse to <https://customerportal.solarwinds.com> from a computer with Internet access, and then log in using your Customer ID and password, or your individual user account information.
-  If you do not know your SolarWinds Customer ID and password or individual profile details, contact Customer Support and [submit a ticket](#).
- b. Click License Management.
 - c. Browse to the SolarWinds product, such as Network Performance Monitor, and click Manually Register License.
 - d. Provide the Unique Machine ID you transferred earlier, and download your license key.
 - e. Transfer the license key to a shared location.
6. Return to the offline computer where you have been running the activation wizard, and browse to the shared License Key File location from the Activate Product window.
7. Click Next to continue, and complete the Activation wizard.

License Manager requirements


ITEM	REQUIREMENT
Install location	SolarWinds License Manager must be installed on the same computer as your installed products. <div> You must install License Manager on a computer with the correct time.</div>
Connectivity	For instant license management, the computer must have internet connectivity. You can also manage licenses using offline activation and deactivation. You must have online access to the SolarWinds Customer Portal from another computer.
.NET Framework	.NET 4.5
Operating system	<ul style="list-style-type: none">■ Windows Server 2008 R2 SP1■ Windows Server 2012■ Windows Server 2012 R2 For evaluation purposes: <ul style="list-style-type: none">■ Windows 7 SP1■ Windows 8 (except for Standard edition)

ITEM	REQUIREMENT
	<ul style="list-style-type: none"> ■ Windows 8.1 (except for Standard edition) ■ Windows 10
Browser	<ul style="list-style-type: none"> ■ Microsoft Internet Explorer 8 or later ■ Microsoft Edge ■ Firefox 44.0 or later ■ Chrome 48.0 or later

Install License Manager

Install License Manager on the computer with SolarWinds products installed. The License Manager can only license products on that computer.

1. Start the SolarWinds License Manager Setup in the SolarWinds program folder.

 If problems with License Manager occur, or if or the computer does not have access to the Internet, download and install the latest version of License Manager from <http://solarwinds.s3.amazonaws.com/solarwinds/Release/LicenseManager/LicenseManager.zip>

2. Click Next to accept the SolarWinds EULA, and click Install.

Activate licenses with the License Manager

With the License Manager, you can manage licenses for multiple SolarWinds products.


1. Start the License Manager in your SolarWinds program folder.

 If the License Manager is not installed on the computer, [install it first](#).

2. Click Activate next to the SolarWinds product, and complete the Activation Wizard.

■ Activate licenses with Internet access

- a. On the Activate Product window, select I Have Internet Access...
- b. Find your activation key in the customer portal, and enter it in the Activation Key field.
 - a. Browse to <https://customerportal.solarwinds.com>, and then log in using your Customer ID and password, or your individual user account information.


 If you do not know your SolarWinds Customer ID and password or individual profile details, contact Customer Support and [submit a ticket](#).

- b. Under the Licensing Management section on the top bar, select License Management.
- c. Browse to the SolarWinds product, and click the plus sign next to the product to display your activation key.
- d. Copy your unregistered activation key for the SolarWinds product to the clipboard, and paste it into the Activation Key field in the Activate window.

- c. If you are using a proxy server to access the Internet, select I Access the Internet Through a Proxy Server, and enter the proxy address and port number.
- d. Click Next.
- e. Provide your customer data, and complete the Activation Wizard.

■ **Activate licenses offline**

- a. On the Activate Product window, select This Server Does Not Have Internet Access, and click Next.
- b. To finalize your registration, click Copy Unique Machine ID.
- c. Paste the data into a new document in a text editor, and save the text document.
- d. Transfer the document to a computer with Internet access. For example, transfer the document to a shared location.
- e. Log in to the SolarWinds customer portal and find your activation key:
 - a. Browse to <https://customerportal.solarwinds.com> from a computer with Internet access, and then log in using your Customer ID and password, or your individual user account information.


 If you do not know your SolarWinds Customer ID and password or individual profile details, contact Customer Support and [submit a ticket](#).

- b. Click License Management.
- c. Browse to the SolarWinds product, such as Network Performance Monitor, and click Manually Register License.
- d. Provide the Unique Machine ID you transferred earlier, and download your license key.
- e. Transfer the license key to a shared location.
- f. Return to the offline computer where you have been running the activation wizard, and browse to the shared License Key File location from the Activate Product window.
- g. Click Next to continue, and complete the Activation wizard.

- 3. Provide your customer data, and complete the Activation Wizard.

Deactivate and reactive licenses

If you decide to move your SolarWinds product to another server, you must deactivate the license on the original computer, and reactivate it on the server with the new installation.

 You can deactivate and reuse the licenses to install product versions that were released during your maintenance period. You cannot deactivate and reuse licenses to install products that were released after your maintenance period expired. To license these products, you must renew your maintenance or re-license your product.

Deactivate, move, and assign licenses online


- 1. Log in to the computer where the licensed SolarWinds product is installed.
- 2. Start the License Manager in the SolarWinds program folder.

3. Select the products you want to deactivate on this computer, and click Deactivate.
You can deactivate more than one product at the same time.
In certain products, you can deactivate licenses by using the internal licensing tool of the product.
4. Complete the deactivation wizard.
5. Log in to the computer on which to install your products, and begin installation.
6. When asked to specify your licenses, provide the information. The license you deactivated earlier is assigned to the new installation.

Deactivate, move, and assign licenses offline

1. Log in to the computer where the licensed SolarWinds product is installed.
2. Start the License Manager in the SolarWinds program folder.
3. Select the products you want to deactivate on this computer, and click Deactivate.
You can deactivate more than one product at the same time. The deactivation file will contain information about each product.
In certain products, you can deactivate licenses by using the internal licensing tool of the product.
4. Complete the deactivation wizard, and save the deactivation file.
5. Log in to the SolarWinds Customer Portal, and navigate to the License Management page.
6. Select your product instance, and click Deactivate License Manually.
7. In the Manage License Deactivation page, locate the deactivation file you created in License Manager, and click Upload.

The deactivated licenses are now available to activate on a new computer.

 The new License Manager tool allows offline deactivation with a created file that can be uploaded to the Customer Portal.

8. Log in to the computer on which to install your products, and begin installation.
9. When asked to specify your licenses, provide the information. The license you deactivated earlier is assigned to the new installation.

Upgrade and synchronize licenses

If you have changed how your product is licensed, such as by increasing the number of objects you can monitor, use the License Manager to apply the change to your products.

1. Start the License Manager from the SolarWinds program group.
2. Click Upgrade in the Action column next to the products for which you want to upgrade the license on this computer.
3. Complete the Activation Wizard.

Synchronize licenses to the Customer Portal

For most Orion Platform products licenses, you can synchronize the data on your Customer Portal with the data in the License Manager.

Synchronizing can include:

- Updating the maintenance end date
- Registering the license again, if it was reset

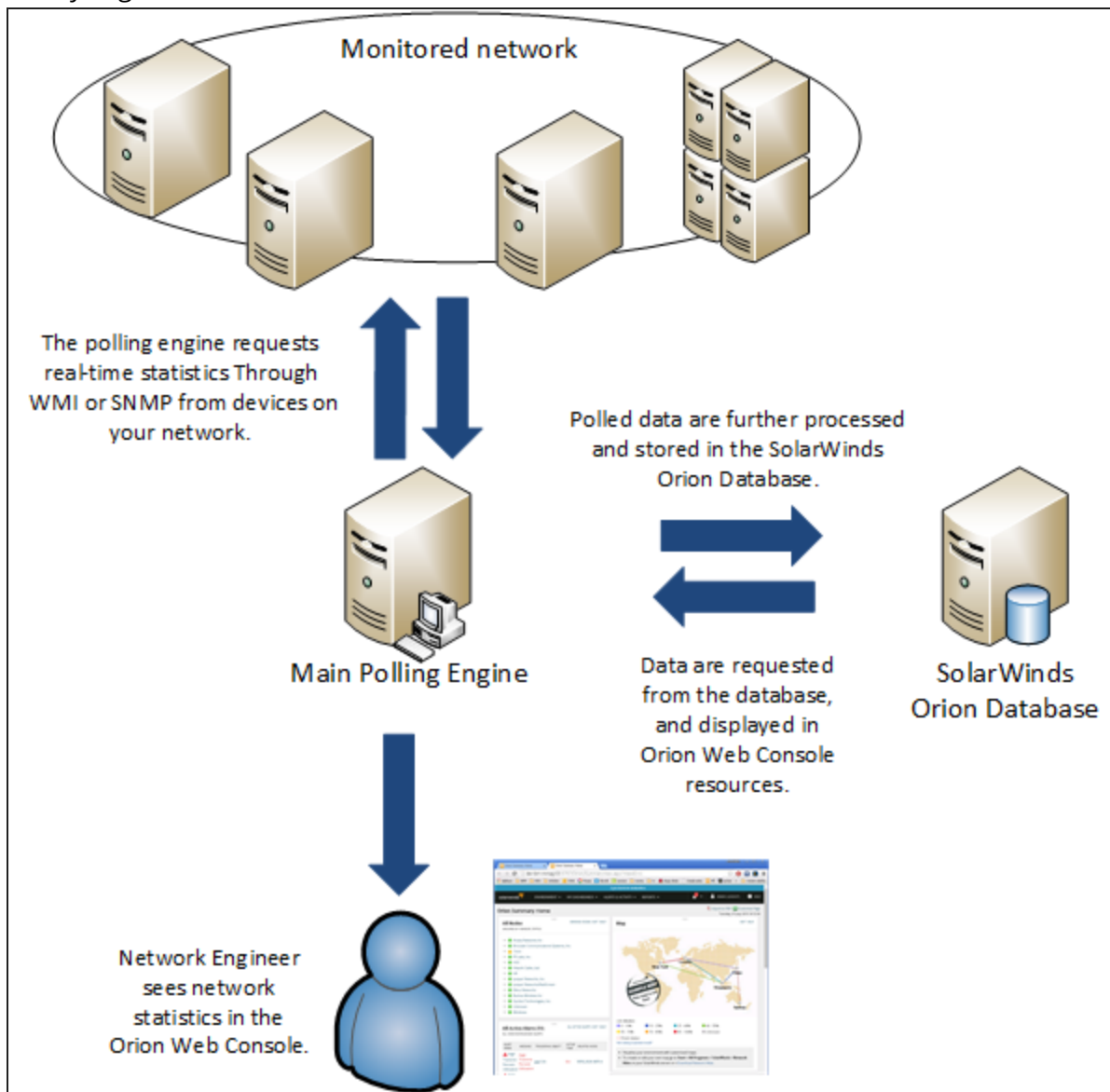
License synchronization takes place automatically once a day. If the automatic synchronization does not occur, or you want to update your licenses immediately, you can synchronize your installed licenses with the SolarWinds Customer Portal:

1. Start the License Manager from the SolarWinds program group.
2. Select the product, and click Synchronize.
3. Click Synchronize again in the Synchronize Licenses window.

The License Manager synchronizes with the Customer Portal and any updates in the Customer Portal are reflected in the License Manager.

How Orion Platform products work

Orion Platform products monitor the health and performance of your network through ICMP, SNMP, WMI, and Syslog communication and data collection.



Discover and add network devices

When you install your Orion Platform product, you must identify the devices you want to monitor, and add them to the SolarWinds Orion database.

- To automatically discover and add a larger number of devices across your enterprise, use the [Network Sonar Discovery](#) and [Network Sonar Results Wizards](#).
- To add individual objects for monitoring, add single nodes using [Node Management](#) in the Orion Web Console.

Discover your network with the Discovery Wizard

Before you begin:

- Enable the networking devices you want to monitor for SNMP.
- Enable Windows devices for WMI.

The first time you discover your network, SolarWinds recommends adding a limited number of edge routers or switches, firewalls and load balancers (if you have them), and critical physical or virtual servers and hosts.

 Add nodes with high latency [one at a time](#).

1. If the Discovery Wizard does not start automatically after configuration, click Settings > Network Discovery.
2. Click Add New Discovery, and then click Start.

3. On the Network panel, if this is your first discovery, add a limited number of IP addresses.

As you scale your implementation, you can use the following scanning options.


Option	Description
IP Ranges	Use this option when you want Orion to scan one or more IP ranges. If you have many IP ranges to scan, consider adding multiple discovery jobs rather than including all ranges in a single job.
Subnets	Use this option to scan every IP address in a subnet. SolarWinds recommends scanning at most a /23 subnet (512 addresses max). Scanning a subnet returns everything that responds to ping, so we recommend only scanning subnets where the majority of devices are objects you want to monitor.
IP Addresses	Use this option for a limited number of IP addresses that do not fall in a range. Since a network discovery job can take a long time to complete, SolarWinds recommends using this option when you are first starting out.
Active Directory	Use this option to scan an Active Directory Domain Controller. Using Active Directory for discovery is particularly useful for adding large subnets because Orion can use the devices specified in Active Directory instead of scanning every IP address.

The screenshot shows the 'Network Sonar Wizard' interface. At the top, there is a navigation bar with tabs: NETWORK, AGENTS, VIRTUALIZATION, SNMP, WINDOWS, MONITORING SETTINGS, and DISCOVERY. The 'NETWORK' tab is selected. Below the navigation bar, the section is titled 'Network Selection'. A subtitle reads: 'How do you want to add devices to Orion monitor? You can use one or more of the options below. Maximum of 512 devices at a time.' There are four main options listed: 'IP RANGES' with a '+ Add Range' button; 'SUBNETS' with a '+ Add' button and a dropdown arrow; 'IP ADDRESSES' with an information icon and a text area labeled 'Write one IP address or hostname per line:' containing the text '10.199.6.1', '10.199.6.3', and '10.199.6.5', with a 'VALIDATE' button below it; and 'ACTIVE DIRECTORY' with an information icon and a '+ Add Active Directory Domain Controller to query...' button.

4. If the Agents panel appears, you enabled the Quality of Experience (QoE) agent during installation. The QoE agent monitors packet-level traffic. If there are any nodes using agents, select the Check all existing nodes check box.

This setting ensures that any agents you deploy, including the one on your Orion server, are up-to-date. If there are no nodes using agents, you can leave this option unchecked.

5. On the Virtualization panel, to discover VMware vCenter or ESX hosts on your network:
 - a. Check Poll for VMware, and click Add vCenter or ESX Credential.
 - b. Select <New credential> and provide required information.

 If you do not add the host credentials, Orion still discovers the virtual machines (VMs) on the host. However, you will not be able to see the relationships mapped between the VMs and hosts.

Add VMware Credential
Enter a local credential for the vCenter or ESX host server.abcd
Choose Credential:
<New credential> ▼
Credential Name:

User Name:

Default ESX user name is "root".
Password:


Confirm Password:


6. On the SNMP panel:
 - a. If all devices on your network require only the default SNMPv1 and SNMPv2 public and private community strings, click Next.
 - b. If any device on your network uses a community string other than public or private, or if you want to use an SNMPv3 credential, click Add Credential and provide the required information.

Add New Credential
SNMP Version:
SNMP v3 ▼
SNMP v3 Credential
Choose Credential:
<New credential> ▼

User Name:

Context:

Authentication Method: None ▼ Password / Key: 

Privacy / Encryption Method: None ▼ Password / Key: 

ADD

CANCEL

7. On the Windows panel, to discover WMI or RPC-enabled Windows devices, click Add New Credential and provide the required information.



SolarWinds recommends that you monitor Windows devices with WMI instead of SNMP.

Network Sonar Wizard

NETWORK > AGENTS > VIRTUALIZATION > SNMP > **WINDOWS**

Windows Credentials

Enter the Windows credentials used on your network. Credentials are used to connect to Windows devices and collect data. WMI is used to collect CPU, memory, and volume data from Windows devices.

+ Add New Credential

Add Windows Credential

Choose Credential:
<New credential>

Credential Name:

8. On the Monitoring Settings panel, SolarWinds recommends manually setting up monitoring the first time you run discovery. This allows you to review the list of discovered objects and select the ones you want to monitor.

When you scale monitoring, you can configure discovery to automatically start monitoring objects it finds.

HOW WOULD YOU LIKE TO SET UP WHAT TO MONITOR?

How would you like to set up what to monitor?

☒ **Manually set up monitoring after devices are discovered** ⓘ
Select this option if you would like to choose what to monitor based on what is found or exclude in monitoring based on what was discovered on the devices, but will not be imported until you go through the Network Sonar Results wizard.

☐ **Automatically monitor based on my monitoring** ⓘ
Select this option if you would like to choose what to monitor upfront. You will have to go through another wizard. Devices will be automatically imported and monitored in the Network Sonar wizard.

9. On the Discovery Settings panel, click Next.
10. Accept the default frequency and run the discovery immediately.


The screenshot shows the 'Network Sonar Wizard' interface with the 'Discovery Scheduling' step selected in the breadcrumb navigation. The main heading is 'Discovery Scheduling' with the instruction 'Configure a schedule for your discovery.' Below this, there is a 'Frequency' dropdown menu set to 'Once'. Under 'Execute immediately:', there are two radio buttons: 'Yes, run this discovery now' (which is selected) and 'No, don't run now'. At the bottom right, there are two buttons: 'BACK' and 'DISCOVER'.

Discovery can take anywhere from a few minutes to a few hours, depending on the number of network elements the system discovers.

The screenshot shows a modal window titled 'DISCOVERING NETWORK...' with a close button. It displays progress for 'Hop 0: Discovering: 10.199.16.135'. There are two progress bars: 'Overall Progress' and 'Current Phase', both showing approximately 25% completion. Below the progress bars, there is a table showing 'Nodes Discovered: 11' and 'Subnets Discovered: 0'. At the bottom right, there are two buttons: 'RUN IN BACKGROUND' and 'CANCEL'.


Add nodes using Active Directory

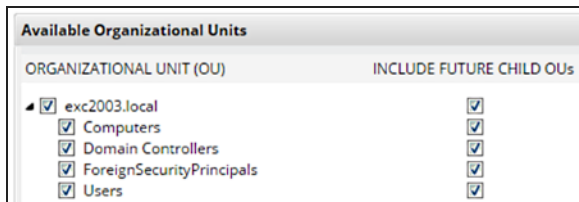
Query your Active Directory Domain Controller to add nodes quickly and efficiently. Your SolarWinds Orion server can use the devices specified in AD instead of scanning every IP address in the subnet.

 Create scheduled discoveries to discover and import any new servers and workstations that have been added to AD automatically.

1. Click Settings > Network Discovery, and click Add New Discovery.
2. On Network Selection, click Add Active Directory Controller to query.
3. On the Add Active Directory DC pop-up, enter your domain controller's IP address/hostname and [credentials](#), and click Next.

4. Select the organizational units (OUs) you want to scan for nodes, and click Finish.

 By default, all OUs are selected, but only servers will be added. Add workstations by clearing the Import servers only check box below the OUs.



On the Network Selection page, you will see the OUs you have added. You can add additional AD controllers, or any other IP addresses that you need before continuing with discovery.



5. [Complete the Network Discovery.](#)

Credentials for Active Directory discovery

When you use Active Directory discovery to add nodes, you must provide the credentials of a Domain Administrator user.

The credentials you provide are added to the discovery wizard as Windows credentials automatically.

If the Active Directory credentials are not same as the Windows credentials for monitoring the node, add credentials for WMI monitoring in the Windows Credentials step.

Automatically add discovered nodes

Automatic monitoring means you do not have to go through the Discovery Import wizard every time you run a discovery. It is useful when you have configured your discovery to find similar nodes or network devices.

1. Click Settings > Network Discovery, and add a discovery, or select an existing one and click Edit.
2. Click through the [Discovery Wizard](#) to the Monitoring Settings page.
3. Choose to include devices that only respond to ICMP (ping). If you decide to exclude devices that only respond to ICMP, your discovery list may be smaller than you expect and you must add those devices manually.

4. On Monitor Settings, select Automatically monitor based on my, and click Define Monitoring Settings.

HOW WOULD YOU LIKE TO SET UP WHAT TO MONITOR?
How would you like to set up what to monitor?




☒ **Manually set up monitoring after devices are discovered** ⓘ
Select this option to choose what to monitor based on what is found during discovery. You must complete another wizard to finish the discovery process. Devices are automatically added to the monitoring list.

☐ **Automatically monitor based on my defined monitoring settings** ⓘ
Select this option to choose what to monitor upfront in Define Monitoring Settings. Monitored devices are selected in a single wizard. Devices are automatically added to the monitoring list after you complete the Network Sonar Wizard.

DEFINE MONITORING SETTINGS...

5. Select the interfaces properties you want to apply to any discovered nodes and click Next. You can also create advanced filters for interfaces under Advanced selection options. This option is available for NPM.

Select the properties of the interfaces you want to monitor:

STATUS	PORT MODE	HARDWARE
<input checked="" type="checkbox"/>  Operationally up	<input checked="" type="checkbox"/> Trunk	<input checked="" type="checkbox"/> Physical
<input type="checkbox"/>  Operationally down	<input checked="" type="checkbox"/> Access	<input checked="" type="checkbox"/> Virtual
<input type="checkbox"/>  Administratively shutdown	<input checked="" type="checkbox"/> Unknown	<input checked="" type="checkbox"/> Unknown

Advanced filtering options

Interface Type contains any keywords



Tips for choosing interfaces

- Only monitor access ports that should always be up. Do NOT monitor desktop access ports because these ports will show an error state when everyone goes home for the day (for example).
- For switches, routers & firewalls, select Up trunk ports and wireless access ports.
- For servers, select Up interfaces.
- Use Advanced Filtering Options for existing interface descriptions to choose your most interesting ports, such as 'uplink', 'WAN', etc.

6. Choose the types of volumes you want to monitor.

Select the types of volumes you want to monitor:

<input type="checkbox"/>	Compact Disk
<input checked="" type="checkbox"/>	Fixed Disk
<input checked="" type="checkbox"/>	Flash Memory
<input type="checkbox"/>	Floppy Disk
<input checked="" type="checkbox"/>	Mount Point
<input checked="" type="checkbox"/>	NetworkDisk
<input checked="" type="checkbox"/>	Other
<input checked="" type="checkbox"/>	RAM
<input checked="" type="checkbox"/>	RAM Disk
<input type="checkbox"/>	Removable Disk
<input checked="" type="checkbox"/>	Unknown
<input checked="" type="checkbox"/>	Virtual Memory



Tips for choosing volumes

- For switches, routers, and firewalls, select Flash memory, and RAM.
- For servers, select RAM, Virtual Memory, Fixed Disk, Mount Points (*nix systems), or Network Disk (Windows).
- We do not recommend monitoring CDs, removable disks, or floppy disks (CDs always show '100% full,' and removable disks disappear and display as unknown).
- Other and Unknown volumes cannot be identified on import, so you may need to take additional actions to identify them.

7. Choose the applications you want to monitor. Only the most commonly monitored applications are available in this screen. You can monitor other applications by using applications templates. This option is available for SAM.

Select the applications you want to monitor:


<input checked="" type="checkbox"/>	Microsoft Exchange Server
<input checked="" type="checkbox"/>	Microsoft IIS
<input checked="" type="checkbox"/>	Microsoft SQL Server
<input type="checkbox"/>	Windows Scheduled Tasks

8. Click Finish.
9. Continue [configuring your discovery](#). When the discovery is run, your monitoring settings will be applied to any discovered devices, and anything that matches will be imported and monitored automatically.

Add discovered devices to SolarWinds NPM

After the Network Sonar Wizard discovers your network, the Network Sonar Results Wizard opens, allowing you to import network elements into SolarWinds NPM. Nodes that are discovered do not count against your license count. Only nodes that you have added to the SolarWinds Orion database count against your license.

When you manually run discovery, by default, the system automatically selects all network elements to be monitored. You must clear the check boxes for elements you do not want monitored.





 If you are discovering your network for the first time, SolarWinds recommends that you monitor a small number of devices.

1. If the Network Sonar Results Wizard does not open automatically, click the Scheduled Discovery Results tab, select nodes you want to monitor, and then click Import Nodes.
2. Ensure the device types you want to monitor are selected, and click Next.


Network Sonar Results Wizard

Device Types to Import

Select the device types to monitor.

<input checked="" type="checkbox"/>	Count		Device Type
<input checked="" type="checkbox"/>	2		Catalyst 37xx Stack
<input checked="" type="checkbox"/>	1		Cisco 2821
<input checked="" type="checkbox"/>	1		net-snmp - Linux
<input checked="" type="checkbox"/>	1		VMware ESX Server


NEXT

 If a device appears as `unknown vendor`, it means that the credentials could not be validated. As a result, the product can only detect if the device is up or down, and cannot collect any other data. To resolve this issue, verify the SNMP configuration on the device. If the credentials still cannot be validated, and you have an active SolarWinds contract, contact [technical support](#).


3. Ensure the interfaces you want monitor are selected, and click Next.

SolarWinds recommends that you do not monitor VoIP interfaces or NULL interfaces.

List of Interfaces					G
<input checked="" type="checkbox"/>	Selected (Available)	Interface Type			
▶ <input checked="" type="checkbox"/>	17 (of 17)	Proprietary Virtual			
▼ <input checked="" type="checkbox"/>	25 (of 25)	Ethernet			
	Interface Name	Node Name	Interface Description	Interface Alias	Port Mode
<input checked="" type="checkbox"/>	● Gi1/0/1	HQDC-3750-CORE.demo.lab	GigabitEthernet1/0/1	WAN Uplink	
<input checked="" type="checkbox"/>	● Gi1/0/2	HQDC-3750-CORE.demo.lab	GigabitEthernet1/0/2	Firewall Uplink	Access
<input checked="" type="checkbox"/>	● Gi1/0/47	HQDC-3750-CORE.demo.lab	GigabitEthernet1/0/47	Uplink to lab-sw-a9-1, Gi0/11, HQ.VM.Mgmt, Users & IPTV for 1st	Trunk

 By default, SolarWinds NPM imports interfaces that are discovered in an Operationally Up state. However, because interfaces may cycle off and on, you can also select Operationally Down or Administratively Shutdown states for import.






4. Ensure the volume types you want to monitor are selected, and click Next.

 SolarWinds recommends that you do not monitor compact disks or removable disks.

Network Sonar Results Wizard






Volume Types to Import

Select the volume types to monitor.




<input checked="" type="checkbox"/>	Count	Volume Type
<input checked="" type="checkbox"/>	11	 RAM
<input checked="" type="checkbox"/>	12	 Virtual Memory
<input checked="" type="checkbox"/>	3	 Other
<input checked="" type="checkbox"/>	19	 Fixed Disk
<input checked="" type="checkbox"/>	4	 RAM Disk

BACKNEXT

5. Review the list of elements to be imported, and click Import.

Network Sonar Results Wizard					
Import Preview - LABORION03					
Select devices, interfaces, and volumes that you wish to ignore or import. All ignored items will be removed from future network discovery, manual or scheduled. If you wish to ignore items, do so before importing.					
<input checked="" type="checkbox"/>	Polling IP Address	Name	Machine Type	Volumes	Polling Method
<input checked="" type="checkbox"/>	 10.196.100.250	HQDC-3750-CORE.demo.lab	Catalyst 37xx Stack		SNMP
<input checked="" type="checkbox"/>	 10.196.200.250	BROF-3750-CORE.demo.lab	Catalyst 37xx Stack		SNMP
<input checked="" type="checkbox"/>	 10.196.202.1	BROF-2821-WAN.demo.lab	Cisco 2821		SNMP
<input checked="" type="checkbox"/>	 10.196.204.11	BOHYV01	Hyper-V Server	RAM, Virtual Memory, Fixed Disk	SNMP
<input checked="" type="checkbox"/>	 10.196.204.12	BOESX01.demo.lab	VMware ESX Server	RAM Disk (4), Fixed Disk	SNMP

6. When the import completes, click Finish.
7. Click the My Dashboards > Summary to begin exploring your network.


Orion Summary Home	
All Nodes	MANAGE NODES EDIT HELP
GROUPED BY VENDOR, STATUS	
▶  Cisco	
▶  F5 Labs, Inc.	
▶  net-snmp	

Add a single node for monitoring



[Check out this video on adding a single node.](#)

As an alternative to using the Network Sonar Discovery wizard, you can add individual nodes for monitoring.

 Adding a single node offers more detail in monitoring and is the recommended approach when you have a node with high latency. Do not include nodes with high latency in a discovery job.

As you add a single node for monitoring, you can:

- Select the statistics and resources to monitor.
- Add Universal Device Pollers.
- Identify how often the node status, monitored statistics, or topology details are updated.
- Add custom properties.
- Edit alert thresholds.

To add a single node for monitoring:

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > Manage Nodes, and then click Add a Node.
3. Specify the node, and click Next.
 - a. Provide the host name or IP address.
 - b. Select the polling method, and provide credentials.

The screenshot shows the 'Polling Method' section of the Orion Web Console. At the top, there is a link 'Help me choose a polling method'. Below it are four radio button options: 'External Node: No Status' (with a description: 'No data is collected for this node. Useful for monitoring a hosted application or other e...'), 'Status Only: ICMP' (with a description: 'Limited data (status, response time, and packet loss) is collected using ICMP (ping). Use...'), 'Most Devices: SNMP and ICMP' (which is selected, with a description: 'Standard polling method for network devices such as switches and routers, as well as L...'), and 'Windows Servers: WMI and ICMP' (with a description: 'Recommended agentless polling method for Windows servers.'). Below the 'Most Devices' option is a grey box containing fields for 'SNMP Version' (set to 'SNMPv2c'), 'SNMP Port' (set to '161'), a checked checkbox for 'Allow 64 bit counters', 'Community String' (set to 'public'), and 'Read/Write Community String' (empty). A 'TEST' button is located below these fields. At the bottom, there are two more radio button options: 'Windows & Linux Servers: Agent' (with a description: 'Optional agent useful for monitoring Windows & Linux hosts in remote or distributed e...').

4. Select the statistics and resources to monitor on the node, and click Next.

The screenshot shows the 'Statistics and Resources' section of the Orion Web Console. It contains a list of items with checkboxes: 'Routing' (checked), 'Routing table' (unchecked), 'IPv6 Routing Table' (unchecked), 'CPU & Memory' (checked), 'Status & Response Time' (checked), 'ICMP (Ping) - Fastest' (selected), 'SNMP' (unchecked), and 'Topology: Layer 3' (checked).

5. If you want to monitor a special metric on the node and have defined the metric using a custom poller, select the poller on the Add Pollers pane, and click Next.

6. Review and adjust the device properties.
 - a. To edit the SNMP settings, change the values, and click Test.
 - b. To edit how often the node status, monitored statistics, or topology details are updated, change the values in the Polling area.

i For critical nodes, you may need to poll status information or collect statistics more frequently than the default polling intervals. Change the polling intervals if polling the nodes takes too long.

- c. Enter values for custom properties for the node.
The Custom Properties area will be empty if you have not defined any custom properties for the monitored nodes. See "Add custom properties to nodes" in the SolarWinds Getting Started Guide - Customize.
- d. To adjust when the status of the node changes to Warning or Critical, edit alerting thresholds for the metric. Select the Override box and set thresholds specific for the node.

7. Click OK, Add Node.

The node will be monitored according to the options you set.

Import nodes from a list of IP addresses

Import devices from a seed file in the Network Sonar Discovery wizard.

i Enter one IP address or host name per line.

See the [Network Performance Monitor Getting Started Guide](#) for more information about network discovery.

1. Open the seed file.
2. Log in to the Orion Web Console, and click Settings > Network Discovery.
3. Click Add New Discovery to create a new discovery, or select a discovery, and click Edit.
4. Click IP Addresses, and copy and paste the IP addresses or host names of the devices from your seed file into the field.
5. Click Validate to confirm that the provided IP addresses and host names are assigned to SNMP-enabled devices.
6. [Complete the discovery](#) and import the devices.

The [Network Sonar Results Wizard](#) opens with the results of your discovery.

Manage 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 listed on this tab.

1. Log in to the Orion Web Console and navigate to Settings > Network Discovery.
2. Click Scheduled Discovery Results.
3. Filter the results the left pane.
4. Update your SolarWinds Orion database to include changed or discovered nodes by selecting all nodes to update or to add, and clicking Import Nodes.
5. Ignore devices in future discoveries by selecting the nodes to [ignore](#), and clicking Add to Ignore List.

Minimize SNMP processing load during discoveries using the Discovery Ignore List

Network discoveries often find devices you do not intend to monitor. Add the devices you do not want to monitor to the Discovery Ignore List to minimize the SNMP load associated with discovering devices not meant for monitoring.

1. Log in to the Orion Web Console, and navigate to Settings > Network Discovery.
2. Click Scheduled Discovery Results.
3. Select devices you want to ignore, and click Add to Ignore List.

 Use items in the Status and Group by lists to help you find devices.

The selected devices will not be discovered by the discovery.

Add ignored devices back to discovery

1. Log in to the Orion Web Console, and navigate to Settings > Network Discovery.
2. Click the Discovery Ignore List, and select the objects you want to monitor.
3. Click Remove from Ignore List.
4. Confirm that you want to stop ignoring selected items by clicking OK.

The devices removed from the list will be included in the discovery again.

Choose the polling method to use

Select a polling method to monitor nodes in the way that best suits your environment.


External Node (No Status)

The node is not polled, and no data is collected from the node. The node is included in your environment and used to monitor an application or another element on the node. This method allows you to build a more complete map of your network environment within your SolarWinds Orion Platform product.

Status Only: ICMP

Limited information is gathered using Internet Control Message Protocol (ICMP) or ping. This polling method is used to monitor status and measure the average response time and packet loss percentage for managed devices.


Use this method when you need limited information or to monitor devices that do not support SNMP or WMI.

 This polling method requires that you enable ICMP on your nodes. Consider adjusting any network intrusion detection systems or your firewalls to allow for the ICMP traffic.

Most Devices: SNMP & ICMP

This method allows you to query the Management Information Base (MIB) and performance indicators that are tied to specific Object Identifiers (OIDs) in addition to polling the device status, average response time, and packet loss percentage. This method is suitable for SNMP-enabled devices such as routers, switches, and computers. You must provide the appropriate SNMP community strings for SNMP v1 or v2c, or SNMP v3 credentials.

Your devices must have ICMP and SNMP enabled to use this polling method. If you want to poll with a specific version of SNMP, you must disable all other versions on the device.


 Consider adjusting any network intrusion detection systems or your firewalls to allow for the ICMP traffic.

Windows Servers: WMI and ICMP

This polling method can only be used for Windows computers. Windows Management Instrumentation (WMI) is a proprietary technology used to poll performance and management information from Windows-based network devices, applications, and components.

When used as an alternative to SNMP, WMI can provide much of the same monitoring and management data currently available with SNMP-based polling with the addition of Windows specific communications and security features.

Your devices must have WMI and ICMP enabled to use this polling method. You can use `WBEMTest.exe`, which is included on every computer that has WMI installed, to test the connectivity between your SolarWinds Orion server and your Windows computer.

 Due to specific characteristics of WMI polling requests, polling a single WMI enabled object uses approximately five times the resources required to poll the same or similar object with SNMP on the same polling frequency. Consider adjusting any network intrusion detection systems or your firewalls to allow for the ICMP traffic.

Windows Servers: Agent

An agent is software that provides a communication channel between the SolarWinds Orion server and a Windows computer. Agents are used to communicate the information that SolarWinds plug-ins collect to the SolarWinds Orion server.


Information collected by plug-ins depend on the type of plug-in installed on the agent. For example, the Quality of Experience plug-in collects packet traffic, while a SAM plug-in collects application data used to monitor the applications. Agents automatically download the plug-ins for all installed products.

This polling method is most useful in the following situations:

- When host and applications are behind firewall NAT or proxies
- Polling node and applications across multiple discrete networks that have overlapping IP address space
- Secure encrypted polling over a single port is required
- Support for low bandwidth, high latency connections
- Polling nodes across domains where no domain trusts have been established
- Full end-to-end encryption between the monitored host and the poller


Manage devices in the Orion Web Console

In the Orion Web Console, you can add and remove devices, quickly view and edit device properties from the Node Management view.


 You need [node management rights](#).

Access the Node Management view in two ways:

- Click Settings > Manage Nodes.
- Click Manage Nodes in the All Nodes resource.

 The All Nodes resource is included on the Orion Summary Home view by default, but you can [include it on any other view](#).


Edit node properties

 Only edit node properties in a single browser tab to prevent database errors and data losses.

 You need [Node Management Rights](#).

Available properties depend on the Orion Platform products you have installed.

1. Click Settings > Manage Nodes.
2. Locate the node for which you want to edit properties.

 To find the node, use the filter and search tools above the nodes list.


3. Select the node, and click Edit Properties.

Edit the node name, web address, and which view opens when you double-click the node

1. To rename the node, type the new name in the Name field.
Changing the node name only affects the way the node is identified on charts and graphs in the Orion Web Console. It does not impact the node as it is referenced on the network.
2. To change the view which displays details about this node, select the View Type from the list.
3. To change the template for the address used in the Node Details resource that allows you to navigate to the node from the resource, scroll down to Web Browse Template, and change the default `http://{HrefIPAddress}`.
4. Click Submit.

Edit polling settings


1. To change the polling IP address, type the new IP address, or click Select IP Address and select the new IP address.

 Changing the IP address affects data collection. Change the IP address only if it changed on your network to continue collecting the statistics without reconfiguring the node.


2. To dynamically assign the IP address of the selected node, select Dynamic IP Address (DHCP or BOOTP), provide the DNS Hostname, and select the IP Address Resolution format.

 If the device is dual-stack, IPv4 resolution will be used by default.

3. [Change the polling method for a node.](#)
4. If you are using SNMP to poll the selected node, you can:
 - a. Edit the SNMP Version and SNMP Port.
 - b. If you have high-speed interfaces, and you are experiencing frequent [counter rollovers](#), confirm that the monitored device supports 64-bit counters, and select Allow 64-bit Counters.

 Some vendor implementations of 64-bit counters produce faulty data. If you notice erratic or incorrect data, clear the box to disable 64-bit counters.

- c. Edit the Community Strings (for SNMPv1 and SNMPv2c) or Credentials, Privacy and Authentication settings (for SNMPv3).

 Changing the community string or SNMP port affects data collection. Do not change the IP address, community string, or SNMP port unless they have changed on your network.

Changing the SNMP port applies to statistics polls, Universal Device Pollers (UnDPs), and SNMP trap collection.

- d. Click Test to test your provided SNMP settings.


5. To change the existing polling intervals, provide new intervals in the Node Status Polling, Collect Statistics and Poll for Topology Data fields.
6. If there are multiple polling engines in your environment and you want to [change the polling engine](#) that polls the node, click Change Polling Engine.
7. Click Submit.

Edit dependencies or custom properties


1. To add, edit, or delete an existing dependency that includes the node, click Manage Dependencies and [adjust the dependencies](#).
2. Provide values for custom properties on the node. If you cannot see the required custom property, click Manage Custom Properties to [create or manage custom properties](#).
3. Click Submit.

Add what additional data you want to poll on the node


1. If the node is a UCS Manager and you want to poll for UCS data, select Poll for UCS, provide the Port on which the UCS manager listens and credentials.

 Click Test to verify that the credentials are valid for the selected UCS Manager.

2. If you have SolarWinds User Device Tracker (UDT) installed and the node has UDT ports attached, you can poll Layer 3 data. Select Poll Layer 3 Data from Device, and enter the Layer 3 Polling Interval.

 Select Disable VRF Context Polling, if required.

3. If SolarWinds SAM is installed, you can monitor Active Directory users that log in to your network. Select Active Directory Domain Controller, and provide the following information.
 - a. Select the credential to be used, or select <New Credential>, and define the credential.

 Administrator credentials are needed only for installing agents.

- b. Click Test to validate.
 - c. Enter the Domain Controller Polling Interval to be used. The default is 30 minutes.
4. To poll for VMware, select Poll for VMware, provide the vCenter or ESX Server credentials, and click Test. See [Monitor virtual infrastructure in the Orion Web Console](#) for more details.
 5. If the node is an F5 device and you want to monitor load balancers, select Poll for i5 Control, and provide the credentials.
 6. Click Submit.

Customize alerting thresholds


Be informed when polled values for a metric on the node reach unwanted values by specifying custom thresholds for the node.

1. Scroll down, select Override Orion General Thresholds for the metric, and [adjust the default values](#).
2. Click Submit.

Suspend collecting data for monitored nodes

Monitored devices are regularly polled for operational status. Collected statistics are displayed in the Orion Web Console.

You can temporarily suspend data collection on individual nodes and resume data collection as necessary.

 If you suspend data collection for a node, it is suspended automatically for all interfaces and volumes on the selected node.

Suspending data collection is helpful when you need to perform maintenance on a node or its components, such as upgrading firmware, installing new software, or updating security. Suspend polling data for the node while the device is down for maintenance to maintain the accuracy of data and prevent unnecessary alert messages.

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > Manage Nodes.
3. Locate the node(s).
4. Select the nodes, and click Unmanage.
5. Provide start and end times and dates for your management suspension, and click OK.
Data for the selected node and monitored resources on the node will be suspended for the specified time period.

Resume data collection for nodes

On Manage Nodes, select the node, and click Remanage.

Information for the selected node, all monitored interfaces and volumes on it will be collected again.

Poll and rediscover devices immediately


Devices are polled for statistics and status regularly, as specified in the [Polling Settings](#). Discoveries run according to their schedule.

Use the Rediscover option to update node data such as machine type, system name, or location. This information does not often change.


You can poll a device or rediscover a node manually at any time.

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > Manage Nodes.
3. Select the node or interface you want to poll or rediscover.
4. To poll the selected node or interface, click More Actions > Poll Now.
5. To rediscover the selected node, click More Actions > Rediscover.


Stop monitoring devices

 Deleting a node also deletes all its applications, interfaces, and volumes. An individual event may be recorded for each deleted network object.

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > Manage Nodes.
3. Select the object, and click Delete.

 To find a monitored application, interface, or volume, expand the parent node, and select the object.


- To find a node, use the filter and search tools above the node list.
- To group found nodes, select a property in the Group By list.

 To delete multiple interfaces on different nodes, use the search tool above the table to find the nodes, and select the interfaces.


4. Click OK to confirm deletion.

Change the polling method for a node

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > Manage Nodes.
3. Select the node for which you want to change the polling method, and click Edit Properties.
4. [Select the Polling Method](#).
5. If you are using SNMP to poll the selected node, select the SNMP version supported on the device, and provide the port and community strings. Click Test to verify that the SNMP settings are correct.

 By default, Orion Platform products use SNMPv2c to poll for performance information. If you want to poll the device using SNMPv1, you must disable SNMPv2c on the device.

For most SNMPv2c devices, the community string `public` gives sufficient access.

 To see the available community strings, click into the Community String field, and press the down arrow key.

To save the community strings as a credential set, provide a Name, and click Save.

6. Click Submit.


Change polling engine node assignments

Reassigning nodes to new polling engines may be required in the following situations:

- Moving or renaming your SolarWinds Orion server
- Deleting an existing polling engine
- Merging two or more SolarWinds Orion server

To change a polling engine node assignment:

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > Manage Nodes.
3. Locate the node to manage using either of the following methods:
 - Use the search tool above the node list to search your SolarWinds Orion database for the device you want to manage.
 - Select a Group by criteria, and expand the group including the node to manage.
4. Select the node for which you want to change the polling engine.
5. Click More Actions, and click Change Polling Engine.

 The current number of Assigned Objects is listed for each available polling engine. This number is updated with each automatic polling engine synchronization. Updates to the Assigned Objects count can only be completed for polling engines that are operationally up.

6. Select the polling engine, and click Change Polling Engine.

Assign Universal Device Pollers (UnDPs) to monitored devices

SolarWinds 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.

If you do not see a poller that meets your monitoring needs, use the Universal Device Poller to create your own poller. See [Monitor custom statistics based on MIBs and OIDs with Universal Device Pollers](#).

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > Manage Nodes.
3. Select the node, interface or volume you want to assign Universal Device Pollers to.
4. Click Assign Pollers in the Node Management toolbar.
5. Expand the poller group, and select pollers to be assigned.
6. Click Submit, and click OK to confirm the assignment.

The selected pollers will now be polled on the node, interface or volume.


View interface status and details about downtime periods

The downtime information might be useful for example for SLA providers who want to prove specific times of interface/port unavailability.

 In some areas, an interface being down does not directly impact Internet or intranet connectivity.

1. Log in to the Orion Web Console.
2. Navigate to the interface or node view, and consult the Interface Downtime resource.

By default, the resource shows the interface status in the last 24 hours, each hour represented as a block in the appropriate color.

 To display downtime for all monitored interfaces on a node, add the Interface Downtime resource on the appropriate node view.

3. To take a more detailed look at a problematic section, position the mouse over the spot on the graph.

Change the time period for checking interface status

By default, the resource displays downtime data for the last 24 hours, one block representing 1 hour. You can display any time frame within the stored history.

1. Go to the Interface Downtime resource, and click Edit.
2. Select Custom in the Downtime Period list, and specify the Beginning and End dates and times.
3. When displaying longer time periods, you might need to change the time frame represented by one block. Select Custom in Display Settings, and provide a time period represented by one block.
4. Click Submit.

Edit the title and subtitle

To edit the resource labels, click Edit, enter labels, and click Submit.

Change how long the interface downtime history is retained

By default, interface status history is stored in the database for 7 days.

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. In the Thresholds & Polling grouping, click Polling Settings.
4. Scroll down to Database Settings, and provide how long you want to keep interface status history in the database in the Downtime History Retention field. Enter a value in days, from 7 to 60 days.

Disable interface downtime monitoring

Monitoring interface downtime can affect the performance of SolarWinds NPM. To decrease the load, disable interface downtime monitoring. For periods where interface downtime was not monitored, the Interface Downtime resource shows gray blocks.

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. In the Thresholds & Polling grouping, click Polling Settings.
4. Clear the Enable Downtime Monitoring box in the Network grouping.
5. Click Submit.

Interface downtime will not be monitored any more. Starting from now, the Downtime Monitoring resource will display the message "Downtime monitoring is disabled. To enable it, go to Polling Settings."

Detect and predict possible duplex mismatches

One of the most common causes of performance issues on 10/100 or 100/1000 Mbit Ethernet links occurs when one port on the link operates at half-duplex while the other port operates at full-duplex.

1. Log into the Orion Web Console.
2. Go to the node details view for the parent node of the interface you want to check for duplex problems.
3. Consult the Possible Duplex Mismatches resource. If there are no errors, the resource is hidden.

The resource lists all duplex interfaces on the node, percentage of transmit and receive errors, the neighboring node and interface. If the neighboring interface or node is not monitored in SolarWinds NPM, the appropriate columns are empty. The last column displays the duplex mode issue - Mismatch, or Unknown.

Duplex Mismatch

To be able to detect duplex mismatches, your nodes need to meet the following requirements:

- The nodes must be monitored by SolarWinds NPM.
- The nodes must be in the up state during the discovery.
- The nodes must support topology and be interconnected.
- Duplex of both devices must be identified as Full or Half.

The resource shows all duplex mismatches, not only 100% duplex mismatches. These are reported on by the Duplex Mismatch alert.

Possible Duplex Mismatch

If at least one of the link interfaces has the duplex mode defined as half or full, the resource helps you identify possible mismatch.

Possible duplex mismatches are visible in the duplex mode column as the Unknown duplex mode. They are identified in the following cases:

- If the switch port reports more than 0.5% receive or transmit errors.
- If the switch port reports CRC errors.
- If the switch port reports Late Collision errors.

How do I resolve mismatches?

To resolve a duplex mismatch, make sure your hardware is working, and unify the duplex mode configuration on neighboring interfaces.

Troubleshooting

The Possible Duplex Mismatches does not display on Node Details view

If the resource does not appear on the node details view, there might be a performance issue due to the amount of interfaces and topology connections. Check the following logs for the occurrence of mismatch information:

```
C:\ProgramData\SolarWinds\Logs\Orion\OrionWeb.log
```

```
C:\ProgramData\SolarWinds\InformationService\v3.0\Orion.InformationService.log
```

The Possible Duplex Mismatches resource does not display percentage of errors

Possible causes:


- No statistical data for these interfaces.
- A performance issue connected with getting statistic information for the resource.

Edit interface properties

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > Manage Nodes.
3. Locate the parent node of the interface you want to manage, and expand the parent node.
4. Select the interface, and click Edit Properties.
5. Make your changes:

Edit the interface name

Adjust the interface name.

-  In interface names, aliases, or descriptions, use only the following recommended characters:
a-z A-Z 0-9 space , . - _ () /
- Do not use \ | : * ? , or angle brackets (< or >). Angle brackets and any strings contained within angle brackets will be removed during polling, as bracketed text may be incorrectly parsed as web markup tags.

To display the interface as unplugged rather than down, select Display Interface as Unplugged.

Designate bandwidth for the interface

Default transmit and receive bandwidths are 1000 Mb/s. If a device does not report its bandwidth, or the interface bandwidth is constrained by other network devices, specify a custom bandwidth that reflects the performance of the interface.

Select Custom Bandwidth, and provide values for Transmit and Receive Bandwidth, in Mb/s.

Change polling interval

Edit how often SolarWinds NPM polls the interface status and performance data.

Interface Status Polling is the interval in seconds between the status checks on the selected interface. By default, interface status is checked every 120 seconds.

Collect Statistics Every is the interval in minutes on which performance statistics for the interface are determined. By default, it is every 9 minutes.

Custom properties and dependencies

Provide values for custom properties for the interface, and edit dependencies. See [Custom properties](#) and [Mirror network object dependencies in the Orion Web Console](#).

Customize alerting thresholds for the interface

You can customize thresholds whose reaching triggers alerts for individual interfaces. You can change alerting thresholds for the following metrics on the appropriate interface:

- Received /Transmit Interface Errors and Discards
- Receive/Transmit Interface Utilization

To customize a threshold, select Override Orion General Thresholds next to the appropriate metric, and provide new values for Warning and Critical Thresholds.

6. Click Submit.

Suspend and resume collecting data for interfaces, or show interface as Unplugged instead of Down


Monitored interfaces are regularly polled for operational status, and collected statistics are displayed in the Orion Web Console

To temporarily suspend collecting data for an interface, unmanage the interface.

If it is not relevant when an interface is down, you can specify that the interface is "unpluggable", and the interface status will not be reflected in the status of the parent node and in alerts.

Suspend collecting data for interfaces

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > Manage Nodes.
3. Locate the parent node of the interface, and expand the parent node.

 To find the node, use the filter and search tools above the nodes list.

4. Select the interfaces, and click Unmanage.
5. Specify the time period in which data collection for the interfaces should be suspended, and click OK.

Resume collecting statistics for interfaces


1. On the Node Management view, select the interfaces, and click Remanage.

Set the interface status as Unpluggable


1. On the Node Management view, select the interface, and click Edit Properties.
2. Select Display Interface as Unplugged Rather Than Down, and click Submit.

Remotely manage monitored interfaces

Using the Node Management utility, you can shut down or enable interfaces, and override configured EnergyWise power settings remotely.


 To remotely manage interfaces, the parent node must have not only Community String, but also Read/Write Community String set correctly. See [Edit polling settings](#).

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > Manage Nodes.
3. Locate the parent node of the interface, and expand the parent node.

 To find the node, use the filter and search tools above the nodes list.

4. Select the interfaces to manage.
5. To shut down the interfaces, click More Actions > Shut Down, and click OK to confirm.
6. To enable the interfaces, click More Actions > Enable.


7. If the selected interface is EnergyWise-enabled, you can override the current power level setting. Click More Actions > Override Power Level, set the power level, and click OK.

 Remote overrides are temporary and will be reset in accordance with your configured EnergyWise policy for the selected interface. See [Temporarily reset the current power level of a monitored EnergyWise interface](#).

Access 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 SolarWinds Orion server are properly registered.

For more information, search the MSDN online help for "Registering an Application to a URI Scheme".

 To use the remote access applications, web browser integration for the user account must be enabled. Navigate to the user account, and ensure [Allow Browser Integration](#) is set to Yes.

Launch remote access applications from any Details view.

Group objects and mirror network dependencies in the Orion Web Console

Groups and dependencies help you organize how data about your network is presented in the Orion Web Console and can improve or simplify alerts.

You can manage Orion objects such as nodes, volumes, applications, interfaces, and even other groups as groups. By using groups, you can logically organize monitored objects, and use the groups as the basis of alerts. For example, you can group nodes from the same location and create alerts and reports about the status of the group.


Dependencies between objects allow you to better represent the status of objects on your network.

Without dependencies, all monitored objects on an unresponsive monitored node report as down. By establishing dependencies, the child objects are displayed as Unreachable instead of down. This prevents false object down alerts.

Group monitored objects

A group is a collection of monitored objects, such as a group of nodes from the same location, or group of all nodes owned by a department.


You can include groups in other groups. For example, you can group all nodes managed by DevOps that are mission critical and then add that group to a more inclusive list of mission critical objects.

 Nesting a group within another does not create a strict parent/child relationship. You can include any group as a member in any number of other groups.

Create groups

Select objects you want the group to contain, or specify group members using a dynamic query based on shared properties. Objects added through dynamic queries are automatically added or removed from the group.

1. Click Settings > All Settings in the menu bar.
2. In the Node & Group Management grouping, click Manage Groups.
3. Click Add New Group.
4. Click Advanced to set the [Status Rollup Mode](#), how often objects refresh in the group, or any custom properties.

 To create custom properties, click Manage Custom Properties in a new tab. See [Custom properties](#).

5. Manually or automatically select objects for this group.
 - Select the check box next to the object to select object manually.
 - Automatically select group members based on shared properties by clicking Add Dynamic Query and creating conditions.

 Click Preview to verify that the dynamic query is selecting the intended objects.


6. Click Create Group.

The new group is listed on the Manage Groups page and can be used in other parts of the product, including alerts and dependencies.


Edit group properties or change the group members

You can edit the properties of an existing group, or add and remove objects. If you remove an object from the group and that object has triggered an alert while it was a member of the group, the alert continues to be active until it's acknowledged.

1. Click Settings > All Settings in the menu bar.
2. In the Node & Group Management grouping, click Manage Groups.
3. Select a group you want to edit, and click Edit Properties.
4. Click Advanced to set the [Status Rollup Mode](#), how often objects refresh in the group, or any [custom properties](#).

 To create custom properties, open Manage Custom Properties in a new tab.

5. To add or remove the group members, click Add & Remove Objects.

 You can also change group members directly on the Manage Groups page.

6. Manually or automatically select objects for this group.
 - Select the check box next to the object to select object manually.
 - Automatically select group members based on shared properties by clicking Add Dynamic Query and creating conditions.

 Click Preview to verify that the dynamic query is selecting the intended objects.

7. Edit an existing query by selecting a dynamic query, and clicking Edit Dynamic Query.
8. To remove an object or query from a group, select the query or object, and click Remove.
9. Click Submit to save the edited objects and queries.
10. Click Submit again to save the group.

Add or remove group members

1. Click Settings > All Settings in the menu bar.
2. In the Node & Group Management grouping, click Manage Groups.
3. Select a group, and click Add & Remove Objects.
4. To add group members, select the objects in Available Objects, and click Add to Group.
5. To remove group members, select the objects in the list of group members, and click Remove.
6. Click Submit to return to the group definition, and click Submit to apply the changes to the group.












Delete groups

1. Click Settings > All Settings in the menu bar.
2. In the Node & Group Management grouping, click Manage Groups.
3. Select a group, and click Delete.





Set the group status based on the status of the group members








The status of a group is determined on the status of the group members.


The Show Best Status selection is useful for displaying groups that are defined as collections of redundant or backup devices.











OBJECT STATES	GROUP STATUS
   (Up, Warning, Down)	 (Up)
  (Up, Down)	 (Up)
   (Warning, Down, Unknown)	 (Warning)

The Show Worst Status selection ensures that the worst status in a group of objects is displayed for the whole group.

OBJECT STATES	GROUP STATUS
   (Up, Warning, Down)	 (Down)

OBJECT STATES	GROUP STATUS
  (Warning, Up)	 (Warning)
   (Warning, Down, Unknown)	 (Down)

The Mixed Status Shows Warning selection 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.


OBJECT STATES	GROUP STATUS
 	 (Critical)
  	 (Critical)
 	 (Mixed Availability)

Mirror network object dependencies in the Orion Web Console

Dependencies are parent-child relationships between network objects that allow you to account for constraints on the network. The constraints can be the result of the design of a specific device, such as interfaces on a switch or router, or the result of the physical architecture of the network itself.

For example, when a parent object, such as a switch, goes down or becomes unresponsive all interfaces on the switch will also be unresponsive, even though they may be working.

To account for this situation, the Unreachable status is used for the interfaces, because their parent node reports as down, and their own status cannot be determined.

 Enable Auto Dependencies in the Polling Settings page to create 1:1 parent-child node dependencies automatically. You can choose to ignore dependencies created this way in the Manage Dependencies view.

Create a dependency between network objects

1. Click Settings > All Settings in the menu bar.
2. In the Node & Group Management grouping, click Manage Dependencies.
3. Click Add New Dependency.

MANAGE DEPENDENCIES

MANAGE IGNORED DEPENDENCIES

GROUP BY:

[No Grouping]

+

ADD NEW DEPENDENCY

EDIT

☐

Dependency Name ▲

4. Select the parent object or group, and click Next.

SHOW ONLY: Nodes

GROUP BY: Vendor

Cisco (7)

F5 Labs, Inc. (9)

net-snmp (2)

Ubiquiti Networks, Inc.

Name ▲

- OKL_OMWT_USER_3750_1.corp.cox.com
- OMA_OW DG_1ST_USER_3850_1.corp.cox.com
- PB20-EL-01-stk
- resp_HWH rainbow walk with all statuses
- SSINUS004SWC001.nasa.group.atlascopco.com
- HQDC-3750-CORE**
- USA001INETSW01.atlascopco.com

To define a dependency so that the reported states of child objects depend on the status of multiple parent objects, [create a group](#) including all parent objects, and select it on this view.

5. Type a Dependency Name, select the child entities, and click Next.

Dependency name: New York IT Department Router

Parent: HQDC-3750-CORE

SHOW ONLY: Groups

GROUP BY: [No Grouping]

Display Name ▲

- Austin
- Branch Office
- New York IT Department**

To define a dependency so that the reported states of multiple child objects depend on the status of one or more parent objects, create a group including all child objects, and select it on this view.

6. Review the settings for the dependency. If there are active alerts on child objects, they are listed on this view.
7. Click Submit.

The dependency appears on the Manage Dependencies page.

You can also display the dependency on custom views in the Orion Web Console.

Edit a dependency between network objects

i Automatic Dependencies cannot be edited.

1. Click Settings > All Settings in the menu bar.
2. Click Manage Dependencies in the Node & Group Management grouping.
3. Select a dependency, and click Edit.

4. Select the parent object or group, and click Next.



To define a dependency so that the reported states of child objects depend on the status of multiple parent objects, [create a group](#) including all parent objects, and select it on this view.

5. Select the child object or group, and click Next.



To define a dependency so that the reported states of multiple child objects depend on the status of one or more parent objects, create a group including all child objects, and select it on this view.

6. Review the settings for the dependency. If there are active alerts on child objects, they are listed on this view. If the parent object is down, the [listed alerts might be suppressed](#).
7. Click Submit.

Changes are saved to the dependency. Active alerts that affect members of the dependency stay active until acknowledged, even if you remove the object from the dependency.

Delete a dependency between network objects



Automatic Dependencies cannot be deleted. You can ignore them in the Manage Dependencies page.

1. Click Settings > All Settings in the menu bar.
2. Click Manage Dependencies in the Node & Group Management grouping.
3. Select the dependency, and click Delete.
4. Click Yes to confirm.

Deleted dependencies are removed from the Manage Dependencies page. The dependencies are not removed from historical logs. Active alerts that rely on the deleted dependency stay active until acknowledged.

View active alerts on child objects when the parent object is down

When a parent object is down and the dependent child objects are Unreachable, alerts based on polled statistics are not triggered, but you can display active alerts on child objects manually.


 Alerts based on default or custom property values are not affected.

If a child object can be polled using a different route, it is polled as usual. Its status does not switch to Unreachable, and alerts are not suppressed.

1. Click Settings > All Settings in the menu bar.
2. Click Manage Dependencies in the Node & Group Management grouping.
3. Select the dependency that includes the child object on which the alerts are active, and click Alerts on Child.

Monitor devices in the Orion Web Console

Like all Orion Platform products, SolarWinds NPM offers immediate insight into the performance of your network.

 Devices you want to monitor must be added to the SolarWinds Orion database. See [Discover and add network devices](#).

View events, alerts, traps, and syslogs in the Orion Web Console Message Center


The Message Center provides a view where you can see all events, alerts, traps, and Syslog messages on your network.

1. Click Alerts & Activity > Message Center.
2. To display messages for specific devices, select device properties in the Filter Devices area.
3. In the Filter Messages area, select the Time period for the messages you want to review, and provide the number of messages you want to show.
4. To show all messages, including messages that have been acknowledged, select Show Acknowledged in the Filter Messages area.
5. To display only certain types of messages, select the messages to be displayed.
6. Click Apply to update the list of displayed messages.

View properties of all monitored nodes and interfaces in the Network Overview

1. Log in to the Orion Web Console, and click My Dashboards > Network > Overview.
2. Select the node property you want to view in the Nodes field, and select the interface property in the Interfaces field.
3. Click Refresh to show the updated overview.

The Network Overview provides a list of monitored nodes and interfaces. The list is sorted alphabetically, and you can select which property you want to see for nodes and interfaces.

 Hover over any icon, IP address, or node name to open a tooltip with the current status information about the node or interface.

Consult the legend below the list for the explanation of used icons.

View the resources and statistics monitored on a node

Resources monitored on a node include interfaces and volumes. The status of objects is signified by an icon. The List Resources view also lists statistics monitored on the node.

1. Click Settings > Manage Nodes.
2. Locate the node to view:
 - Use the search tool above the node list.
 - Select a Group By option, and expand the group including the node to view.
3. Select the node, and click List Resources on the Node Management toolbar.


The interfaces and volumes for this nodes are displayed, showing which are being currently monitored.

View network events in the Web Console

All events that occur to monitored devices on your network are automatically logged and displayed in the Orion Web Console. You can view and remove them as your network management policies require.

Filter the displayed logged events in the Web Console


Network events are logged and shown in the order they occur in the Events view of the Orion Web Console.

 You can choose how long network events are kept in the Events Retention field in [Orion Polling Settings](#) under Database Settings.

1. Click Alerts & Activity > Events in the menu bar.
2. Filter events by object, event type, or time period.
3. In the Show X Events field, provide the maximum number of events to view. Showing a large number of events, such as a 1000, can negatively impact performance.
4. To show events that have already been cleared, select Show Cleared Events.
5. Click Refresh.

Remove events from the Web Console

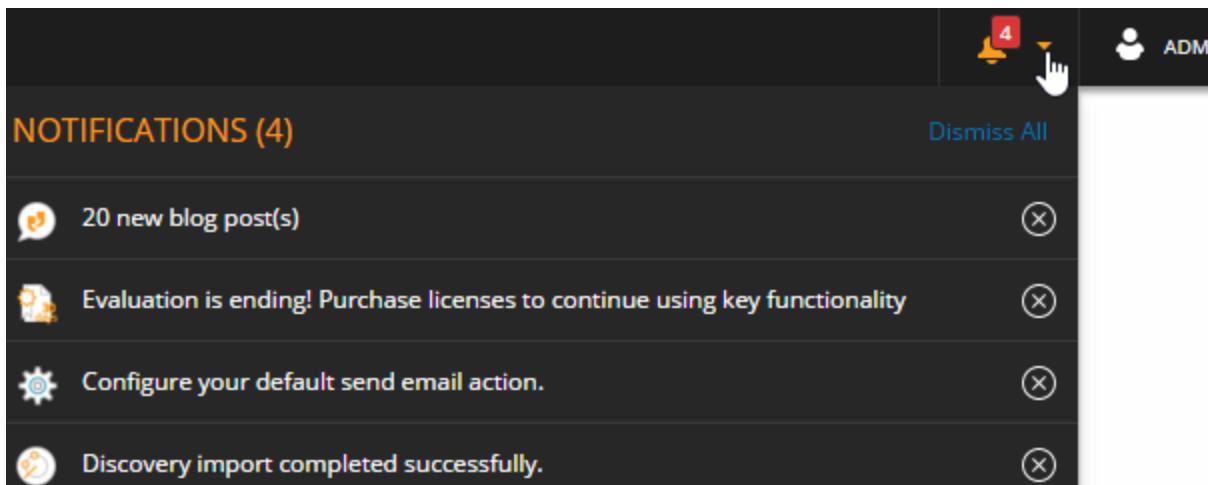
Clearing an event removes the event from the Events view.

 Cleared events are not removed from the event log and can still be used for reporting.

1. Click Alerts & Activity > Events in the menu bar.
2. Select individual events to clear or click Select All.
3. Click Clear Selected Events.

View notifications

Click the bell icon in the top-right corner to display unread notifications.



Notifications include the following messages:













- If you configured the Orion Web Console to check for product updates, an announcement displays when an update, such as any upgrade, service pack, or hotfix becomes available.
- If you 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.
- If you configured a scheduled discovery, results display in the notification bar when the discovery completes.
- If you are monitoring any VMware ESX or ESXi Servers, the notification bar displays the number of ESX nodes found during any discovery, and inform you if any discovered ESX nodes require credentials.
- If you are monitoring Hyper-V nodes, the notification bar informs you when Hyper-V servers were found during a discovery.

Monitor hardware health

Get immediate insight into hardware issues on your network. Monitoring hardware health on Cisco, Dell, F5, HP, and Juniper devices informs you which of these devices are in Up, Warning, Critical, or Unknown states.

1. When adding a device into the SolarWinds Orion database for monitoring, [enable polling hardware health statistics](#).
2. Hardware health statistics are polled through SNMP, from a MIB tree on your devices. For Cisco devices, [make sure that the correct MIB is selected](#).
3. Make sure the [correct sensors are enabled for the nodes](#).

Monitored Hardware Sensors

SENSOR	UP	WARNING	CRITICAL	UNKNOWN
Fan status				
Power Supply status				
Temperature				

Enable hardware health monitoring

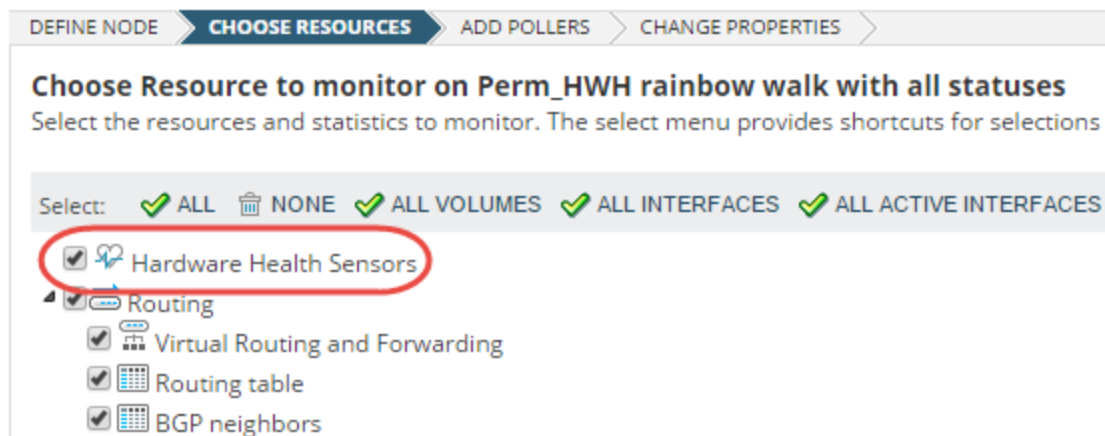
When you add nodes using [Network Sonar Discovery](#), the hardware health sensors are enabled for devices that support hardware health monitoring automatically.

When adding individual nodes with the [Add Node wizard](#), you can enable or disable hardware health monitoring in the wizard.

To verify that hardware health statistics are being collected, list monitored resources for the node and [ensure that hardware health monitoring is enabled](#).

Enable monitoring from the Add Node wizard

When selecting resources for monitoring a node in the Add Node wizard, select the Hardware Health Sensors box to enable hardware health monitoring.



Enable hardware health monitoring on a node

1. Click My Dashboards > Home in the Orion Web Console.
2. In the All Nodes resource, click the node you want to monitor.
3. In the Management resource on the Summary tab of the Node Details view, click List Resources.
4. Make sure the Hardware Health Sensors box is selected, and click Submit.

Hardware health statistics for [enabled hardware sensors](#) are collected for the node.

Enable, disable, or adjust hardware health sensors

To view all currently monitored sensors, click Settings > All Settings, and in the Node & Group Management grouping, select Manage Hardware Sensors. By default, all sensors available in the selected MIB are monitored on devices with enabled hardware health monitoring.

On the Manage Hardware Health Sensors page, you can enable or disable polling on individual sensors, or [change hardware health thresholds](#).

Update hardware health statistics

All changes are applied in the Orion Web Console with the next poll. Look up the current polling interval, and if necessary, poll for the statistics manually.

1. Click Settings > All Settings, and click Polling Settings in the Thresholds & Polling grouping.
2. Scroll down to Hardware Health Polling section, and note the Default Statistics Poll Interval.



- We recommend that you do **NOT** enter a shorter polling interval here because it might affect the polling performance. To immediately update hardware health statistics for a node, see step 3.
- Consider how often you need to update the health statistics and how long you need to keep historical records. To improve the performance, enter a longer polling interval, or shorten the retention periods.

3. Go to the node details view, and click Poll Now in the Management resource.

Hardware health statistics will be immediately updated. This will not affect the performance as if you shortened the polling interval.

Enable hardware sensors

Hardware health information is collected only for nodes where the hardware sensors are enabled.

1. Go to Manage Hardware Sensors view (Settings > All Settings > Node & Group Management > Manage Hardware Sensors).
2. Find the sensor(s) you want to enable. You can either use the Group by pane, or use the Search box.



To find all sensors available on a node, select Node in the Group by list, and then select the node.

3. Select the sensor that you want to enable on the node, and click Enable.

Hardware health information for the selected nodes will be collected now.

Disable hardware sensors

If you do not want to collect specific hardware health information or any hardware health information, disable sensors.

1. Go to Manage Hardware Sensors view (Settings > All Settings > Node & Group Management > Manage Hardware Sensors).
2. Find the sensor(s) you want to enable. You can either use the Group by pane, or use the Search box.



To find all sensors available on a node, select Node in the Group by list, and then select the node.

3. Select the sensor(s) which you want to disable on the node, and click Disable.

Hardware health statistics for the selected sensors on the selected nodes will not be collected now.

Edit hardware health thresholds

Hardware states displayed in the Orion Web Console change based on thresholds set for the sensors. You can either use thresholds available on the device, set a sensor to always appear to be up, or customize thresholds.

When values polled on a node reach the threshold value, an event triggers together with the [alert](#) "Hardware is in warning or critical state."

1. Go to Manage Hardware Sensors view (Settings > All Settings > Node & Group Management > Manage Hardware Sensors).
2. Select the sensor that you want to edit, and click Edit Thresholds.



To find all sensors available on a node, select Node in the Group By list, and select the node.

3. Select how you want to change the selected hardware sensor's status:

Use Orion Defaults

Use thresholds configured on the device. This is the default setting.

Force to Up

If you are not concerned about a sensor, select this option. The sensor will always be displayed as UP, ignoring the real data from the sensor.

Set Custom Thresholds

Use the dynamic query builder to define the status for the selected sensor.

4. Click Submit.

The status of the hardware health sensor will now be governed by the specified threshold.

Change the MIB used for polling hardware health statistics

Hardware sensors information on Cisco devices can be polled using one of the following MIBs.

- CISCO-ENTITY-SENSOR-MIB (default MIB)
- CISCO-ENVMON-MIB

Each MIB contains different OIDs, and information for individual nodes might be included only in one of them. If you see inconsistencies between the actual hardware health and the status shown in the Orion Web Console, change the MIB used for polling hardware health statistics.

Change the MIB tree used for polling hardware health globally


1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.

3. In the Thresholds & Polling grouping, click Polling Settings.
4. Scroll down to the Hardware Health Polling section, and select the MIB in the Preferred Cisco MIB list.
5. Click Submit.

The default MIB used for polling all hardware sensors on all monitored nodes is changed now.

Change the MIB for polling hardware health statistics on a specific node

1. Open the Node Details view, and click Edit Node in the Management resource.
2. Scroll down to the Hardware Health Polling section, and select the MIB.
3. Click Submit.


 Changing MIB for a node overrides the general settings. Once you customize the MIB for polling hardware health sensors, it will not change if you change the general settings.

Change hardware health temperature units

By default, hardware health resources display temperature in degrees Fahrenheit.

1. Log in to the Orion Web Console.
2. Navigate to a node details view.
3. Go to the Current Hardware Health resource, and click Edit.
4. Select the unit for temperature display (Fahrenheit or Celsius).
5. Click Submit.

The selected unit will be applied in all hardware health resources in the Orion Web Console. This setting is user-specific, and it is connected with your user account.

 You can also access the temperature unit setting when [editing a user](#) in the Hardware Health Package Settings.

Monitor virtual infrastructure in the Orion Web Console

SolarWinds Integrated Virtual Infrastructure Monitor (IVIM) is the feature that enables virtual monitoring directly from the Orion Web Console.

It is available as a feature of SolarWinds NPM or SolarWinds SAM, in integration with SolarWinds VMAN, or as a standalone solution.

IVIM monitors the following:

- ESXi and ESX Server version 4.1 or later
- VMware vSphere version 4.1 or later
- Microsoft Hyper-V Server versions 2008 R2, 2012, 2012 R2

Prerequisites to monitoring virtual infrastructure

- SolarWinds NPM or SolarWinds IVIM is installed.
- SNMP on your virtual servers is enabled.
- VMware Tools are installed on all virtual machines you want to monitor.



If your virtual machines are on monitored ESXi and ESX servers, VMware Tools are not a requirement but provide access to additional information, such as IP addresses.

- [ESX credentials](#) on ESX servers are created.
- You [virtual infrastructure is discovered](#).

Create ESX server credentials for SolarWinds Orion products

For polling performance data, you must create credentials on your ESX Servers for the SolarWinds Orion polling engine.

To create the credentials, log in to the ESX server, and create a user. For more information, consult your vendor documentation.



Credentials created for the polling engine must have read-only rights as a minimum.

Add virtual servers for monitoring

Hyper-V nodes, VMware vCenter, ESX servers, and virtual machines which you want to monitor must be added to the SolarWinds Orion database.

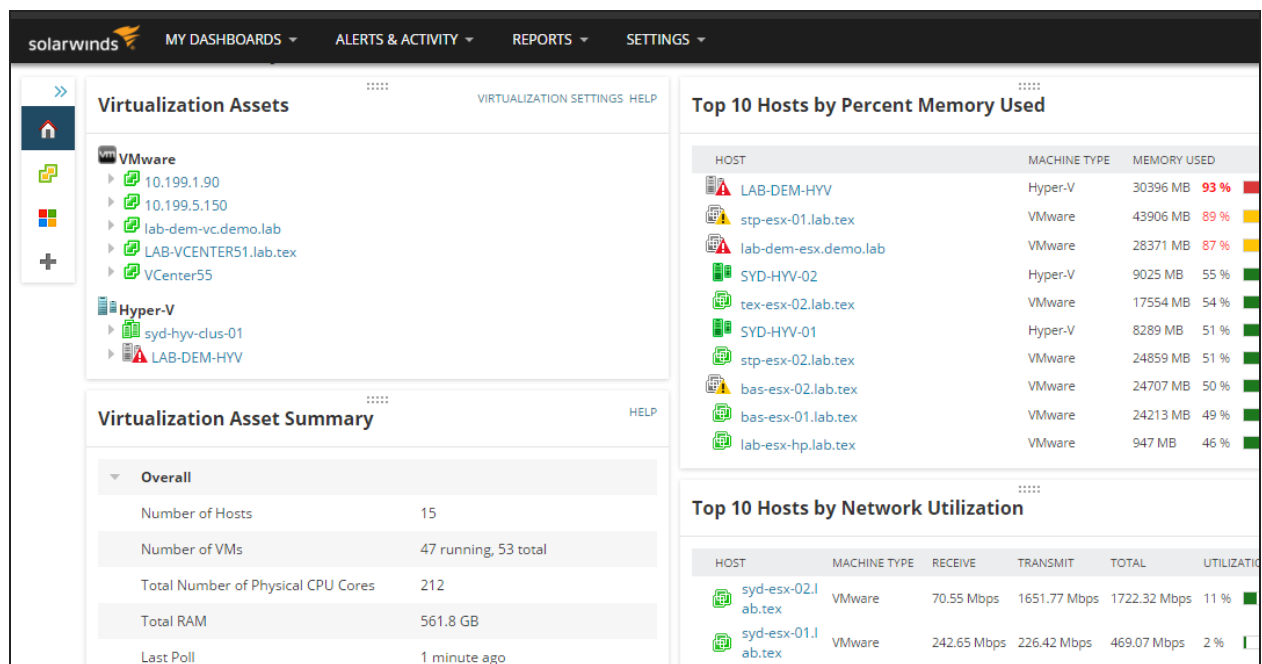
Add the nodes using [Network Sonar Discovery](#).

1. Log in to the Orion Web Console as an administrator.
2. Launch Network Discovery in the Orion Web Console through Settings > Network Discovery > Add New Discovery.
3. On the Virtualization page, select Poll for VMware, and if the vCenter or ESX Credentials are not listed, add them.
4. On the Windows page, add Windows credentials for accessing Hyper-V nodes.
5. Complete the wizard and import the results.

Assess the status of the virtual environment

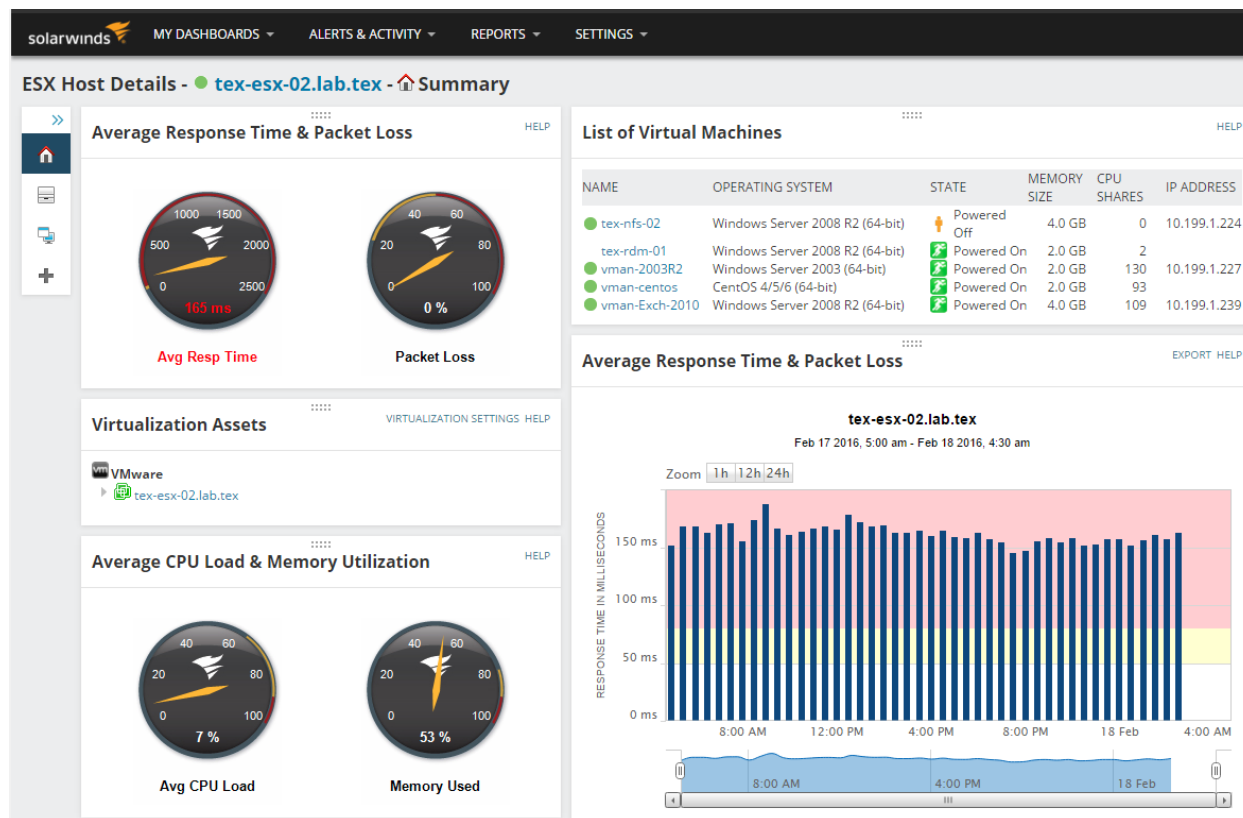
The Virtualization Summary view shows the overall status of your virtualized infrastructure.

1. Log in to the Orion Web Console.
2. Click My Dashboards > Home > Virtualization in the menu bar.



View ESX host details

Click an ESX Host server in the Virtualization Summary page to open the ESX Host Details view.



Assign credentials to virtual servers

If you did not provide the credentials within the Network Sonar Discovery, or when adding the node to the database, assign credentials based on the server vendor.

i VMware ESX or vCenter accounts used as credentials must have read-only permissions as a minimum.

Assign credentials to Hyper-V servers

1. Click Settings > All Settings > Manage Virtual Devices.
2. On the Virtualization Polling Settings page, select Hyper-V.
3. Select a Hyper-V server from the list, and click Edit Properties.
4. Under Polling Method > Windows Servers, choose a credential, or select New Credential, and specify a new credential set.
5. Click Test to verify the credential set, and click Submit.

Assign credentials to VMware servers

1. Click Settings > All Settings > Manage Virtual Devices.
2. On the Virtualization Polling Settings page, select VMware.

3. Select a VMware server from the list, and click Assign ESX Credential.
4. Choose an existing credential, or specify a new credential set.
5. Click Test to verify the credential set, and click Assign Credential to assign it to the VMware server.

Change VMware credentials in the Orion Web Console

If credentials for a VMware account change on the device, update the credentials in the Orion Web Console.


1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. In the Node & Group Management grouping, click Manage Virtual Devices.
4. Click the VMware Credentials Library tab.
5. Select the credential you want to update, and click Edit Credential to make the necessary changes.

Poll ESX hosts controlled by vCenter servers directly

If your VMware ESX hosts are controlled by VMware vCenter servers, Orion Platform products obtain the status of the ESX hosts from the vCenter server.

To poll the ESX servers directly, change the Poll Through setting of the ESX host.

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. In the Product-Specific Settings grouping, click Virtualization Settings > VMware Settings.
4. Select the ESX hosts you want to poll directly.
5. Click Poll Through > Poll ESX server directly.

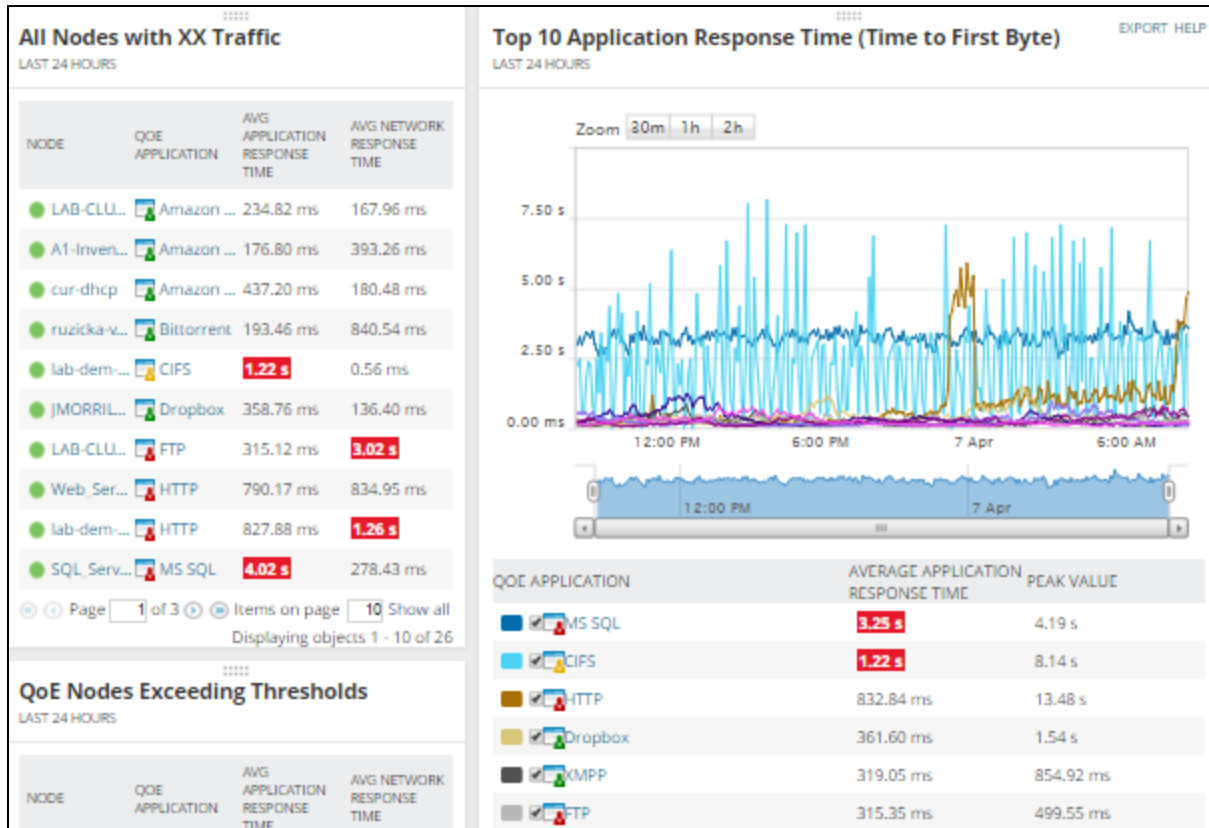
 On the VMWare Settings page, you can also disable and enable polling for ESX hosts and vCenter servers.

Monitor Quality of Experience metrics

On the Quality of Experience (QoE) dashboard you can monitor traffic on your network. QoE uses Packet Analysis Sensors to provide packet-level traffic information about key devices and applications.

With QoE, you can:

- Compare statistics, such as network response time (TCP Handshake) and application response time (Time to First Byte) to determine if a bottleneck is on the application or the network.
- Use data volume trends to pinpoint traffic anomalies and investigate the cause.
- Monitor risky types of traffic, for example, traffic that might bypass firewalls or lead to data leaks.



With the ability to analyze packet traffic, QoE provides real observed network response time (NRT) and application response time (ART). In addition, Packet Analysis Sensors can classify and categorize traffic for over 1000 different applications by associated purpose and risk-level.

Traffic data is captured using Packet Analysis Sensors. These sensors collect packets using either a dedicated Windows SPAN or mirror port monitor or directly on your Windows server. Packet Analysis Sensors capture packets from the local network interface (NIC) and then analyze collected packets to calculate metrics for application performance monitoring. These metrics provide information about application health and allow you to identify possible application performance issues before they are reported by end-users.

For more information about specific implementations of QoE, see [Common Packet Analysis Sensor deployment scenarios](#).


How SolarWinds Packet Analysis Sensors work

SolarWinds provides two types of Packet Analysis Sensors to monitor and analyze your network traffic.

- Packet Analysis Sensors for Networks (network sensor) collect and analyze packet data that flow through a single, monitored switch for up to 50 discrete applications per node.
- Packet Analysis Sensors for Servers (server sensor) collect and analyze packet data of specific applications that flow through a single node.

After a sensor is deployed and configured, it captures packets and analyzes them to calculate performance metrics for the monitored applications. An included communication agent allows the sensor to send back sampled packet data to the SolarWinds Orion server, which includes statistics such as volume, transactions, application response time, and network response time for each application on a node. The packet data are then saved to the SolarWinds Orion database. The information is used to populate your QoE dashboard. You can configure how long you retain the packet data in the [Database Settings](#) section of the Polling Settings screen.

Network Packet Analysis Sensor (NPAS)

 Your network administrator must create a dedicated SPAN, mirror port, or in-line tap monitor on the physical or virtual switch before you can deploy or configure a network sensor.

After you deploy and configure the network sensor to the node monitoring the switch, the sensor captures all packets that flow through the switch and categorize the packets by application.

Packets that correspond to monitored applications are analyzed for QoE metrics, such as response times or traffic volume. Data are then sent to the SolarWinds Orion server using the SolarWinds agent.

Server Packet Analysis Sensor (SPAS)


A SPAS can monitor:

- packet traffic on a single node
- up to 50 applications per node

A SPAS captures packets traveling to and from the node. It identifies packets that are sent to or from the monitored application and analyzes them for QoE metrics, such as response time or traffic volume. Data are then sent to the SolarWinds Orion server using the agent.

Limitations to Packet Analysis Sensors

The number of nodes you can monitor is limited by the data throughput per node, the number of cores, and the amount of RAM available on the monitoring server.


 The system requirements increase for every 100 Mbps of traffic.

SENSOR LIMITATIONS	VALUE
Maximum throughput (NPAS and SPAS)	1 Gbps

SENSOR LIMITATIONS	VALUE
Maximum number of nodes per sensor (NPAS)	50 nodes
Maximum number of node and application pairs (NPAS and SPAS)	50,000 pairs
Maximum number of sensors deployed on your network	1,000 sensors
Maximum number of applications per node or sensor (NPAS and SPAS)	1,000 applications per node


Common Packet Analysis Sensor deployment scenarios

After you install your Orion platform product, [deploy network sensors](#) on a server dedicated to monitoring a network switch or [deploy server sensors](#) directly on physical or virtual servers or workstations.

 If you select QoE during the installation, a sensor is already on your SolarWinds Orion server collecting data about applications that SolarWinds Orion is using.

Based on how you want to aggregate the returned QoE metrics, there are three main deployment scenarios per sensor type.

AGGREGATION LEVEL	SENSOR DEPLOYMENT	CONFIGURATION
I HAVE ACCESS TO MY NETWORK (NPAS)		
Per application	Deploy an NPAS to a port mirror that monitors all traffic to and from the application	Automatic
Per site	Deploy an NPAS to a port mirror that monitors all traffic to and from the site	Add a sampling of endpoints to the NPAS as managed nodes
Per client	Deploy an NPAS to a port mirror that monitors all traffic to and from the site	Add all of the endpoints to the NPAS as managed nodes
I HAVE ACCESS TO MY APPLICATION SERVERS (SPAS)		
Per application	Deploy the SPAS directly on the application server	Automatic
Per site	Deploy the SPAS to select endpoints	Automatic
Per client	Deploy the SPAS to all endpoints	Automatic

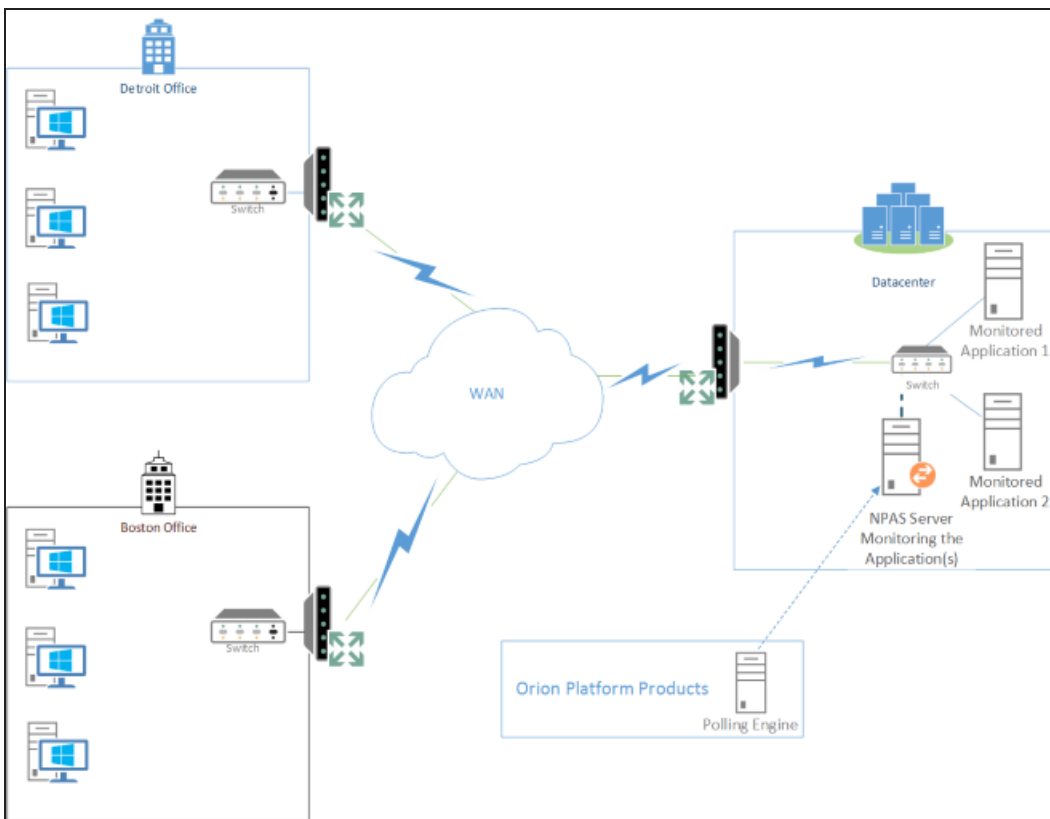
 ■ When deploying both network and server sensors on the same network, ensure that you do not monitor the same node with multiple sensors. This impacts the QoE metrics.

- All monitored nodes must be managed by your Orion Platform product before they can be monitored by sensors.
- Applications and nodes are detected by default if the node is managed by your SolarWinds Orion server. If packet data is not collected, navigate to Settings > All Settings, and click on QoE Settings. Click Manage Global QoE Settings, and activate the auto-detect option. You can also [manually monitor applications](#) and [managed nodes](#) or [ignore](#) them.

Aggregation per application

This deployment scenario provides a broad indication of the overall response time between computers and the monitored application.

Aggregation with access to network (NPAS)

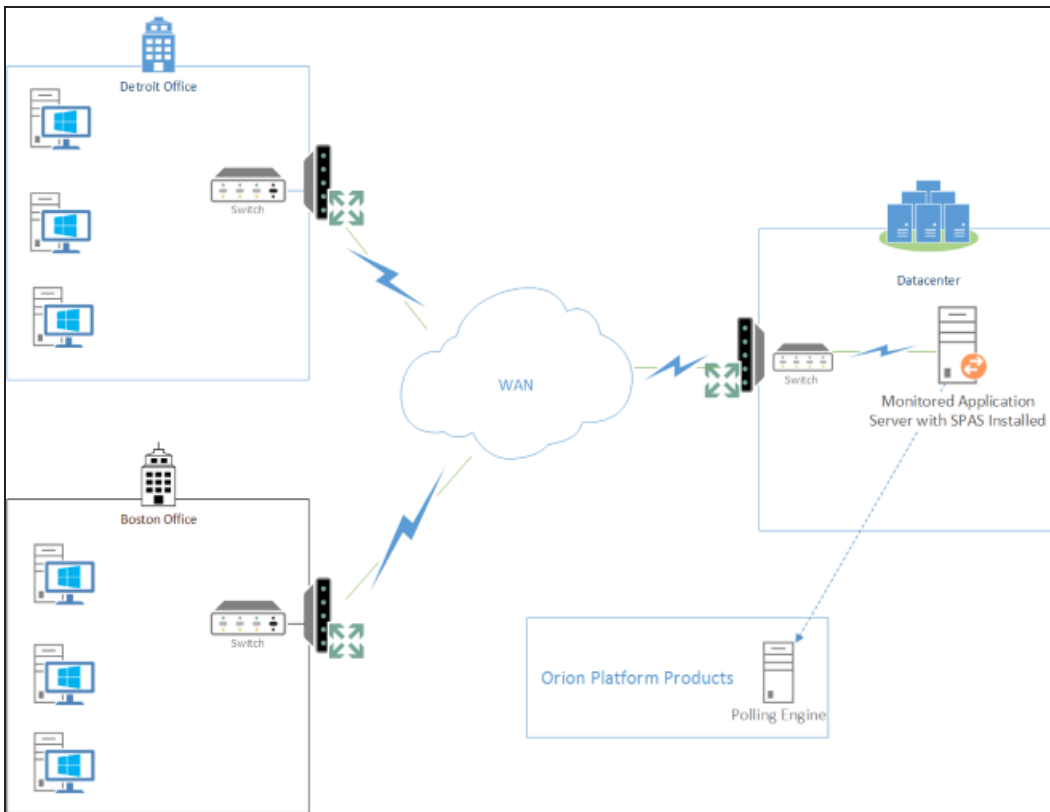


- Create a port mirror, SPAN, or network tap on the switch with all the network traffic to or from the application.
- You can monitor multiple applications using the same NPAS.

1. Click Settings > All Settings in the menu bar.
2. Click QoE Settings > Manage QoE Packet Analysis Sensors > Add Packet Analysis Sensor.
3. Select the Network option, and then click Add Nodes.
4. Choose the node with the port mirror, SPAN, or network tap setup to monitor your network switch.

5. Assign and test the credentials for the selected node.
6. Click Add Nodes and Deploy Agents to deploy the network sensor to the node.

Aggregation with access to application servers (SPAS)



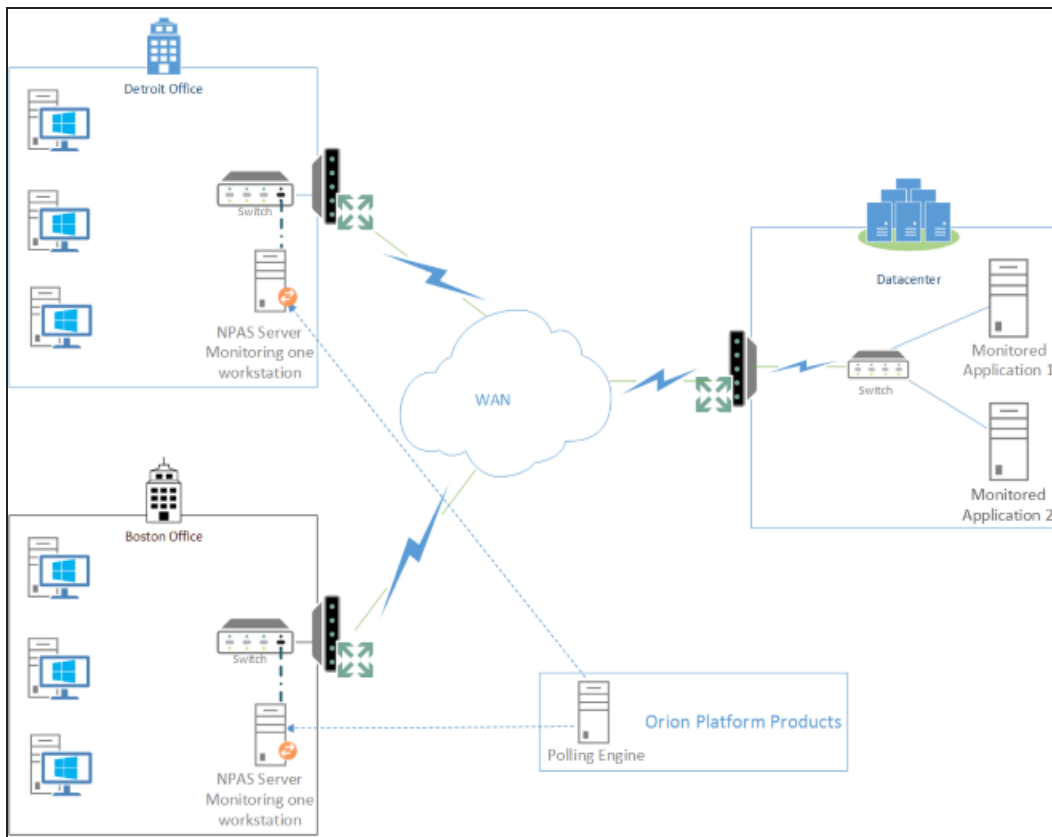
1. Click Settings > All Settings in the menu bar.
2. Click QoE Settings > Manage QoE Packet Analysis Sensors > Add Packet Analysis Sensor.
3. Select the Server option, and then click Add Nodes.
4. Choose the nodes with the application you want to monitor.
5. Assign and test the credentials for each node.
6. Click Add Nodes and Deploy Agents to deploy a sensor on the node.

Aggregation per site

This deployment scenario provides an aggregated response time per monitored site or network to the application. For example, the response time from your Detroit office to your datacenter is one second, but the response time from Boston to your datacenter is seven seconds. If you used the aggregation per application deployment method, the response time for the application is four seconds.

This method requires you to identify users who best represent how the application is used. You then use the users' computers as data points to monitor with Packet Analysis Sensors.

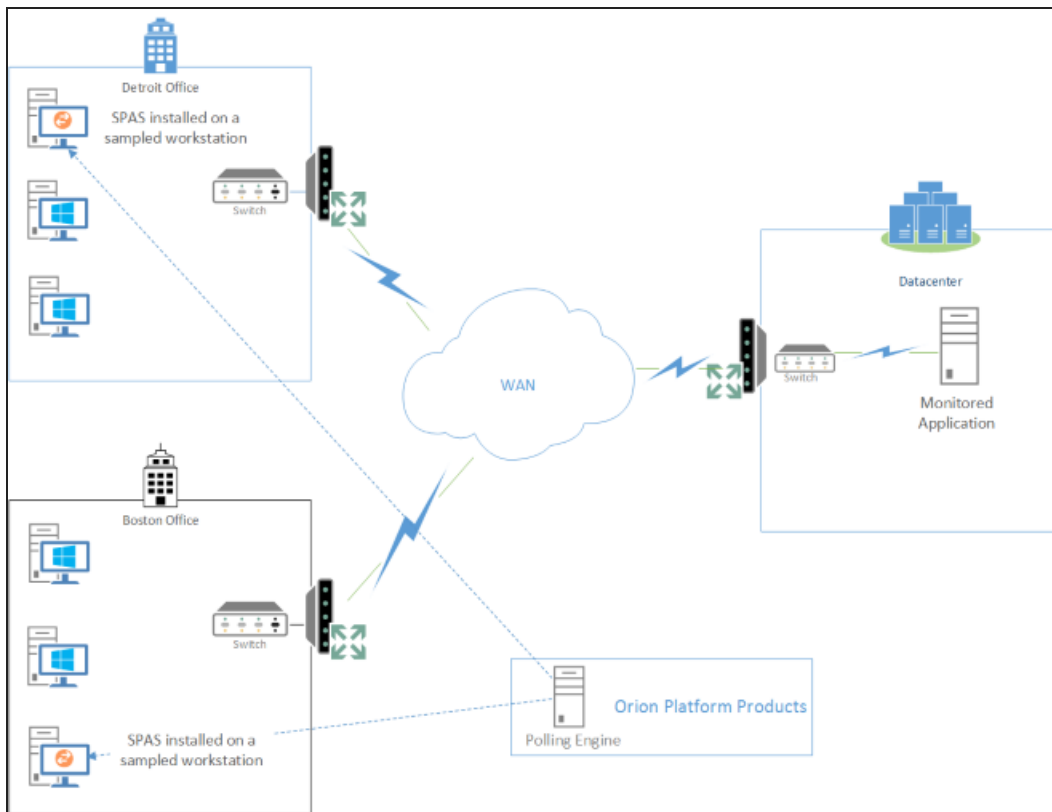
Aggregation per site with access to network (NPAS)



- Create a port mirror, SPAN, or network tap on the switch with all the network traffic to or from the application.
- You can monitor multiple applications using the same NPAS.
- Identify a sample set of users whose computers are monitored by the NPAS.

1. Click Settings > All Settings in the menu bar.
2. Click QoE Settings > Manage QoE Packet Analysis Sensors > Add Packet Analysis Sensor.
3. Select the Network option, and then click Add Nodes.
4. Choose the node with the port mirror, SPAN, or network tap setup to monitor your network switch.
5. Assign and test the credentials for the selected node.
6. Click Add Nodes and Deploy Agents to deploy the network sensor to the node.

Aggregation per site with access to application servers (SPAS)



i Identify a sample set of users whose computers are monitored by the SPAS.

1. Click Settings > All Settings in the menu bar.
2. Click QoE Settings > Manage QoE Packet Analysis Sensors > Add Packet Analysis Sensor.
3. Select the Server option, and then click Add Nodes.
4. Choose the nodes with the application you want to monitor.
5. Assign and test the credentials for each node.
6. Click Add Nodes and Deploy Agents to deploy a sensor on the node.

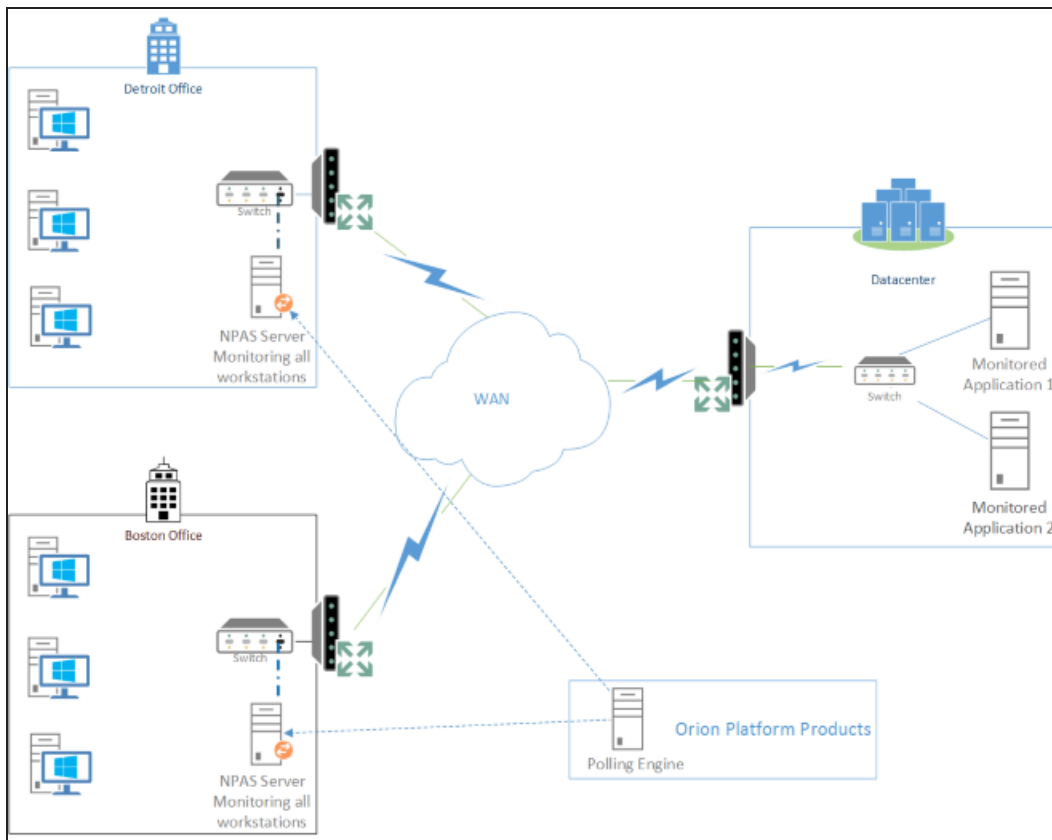
Aggregation per computer

This deployment scenario provides highly granular response times for the application because metrics for each computer are recorded.

One or two workstations can experience long response times, which may not be caught when aggregated per site or per application.

This method requires all workstations to be managed within your Orion Platform product.

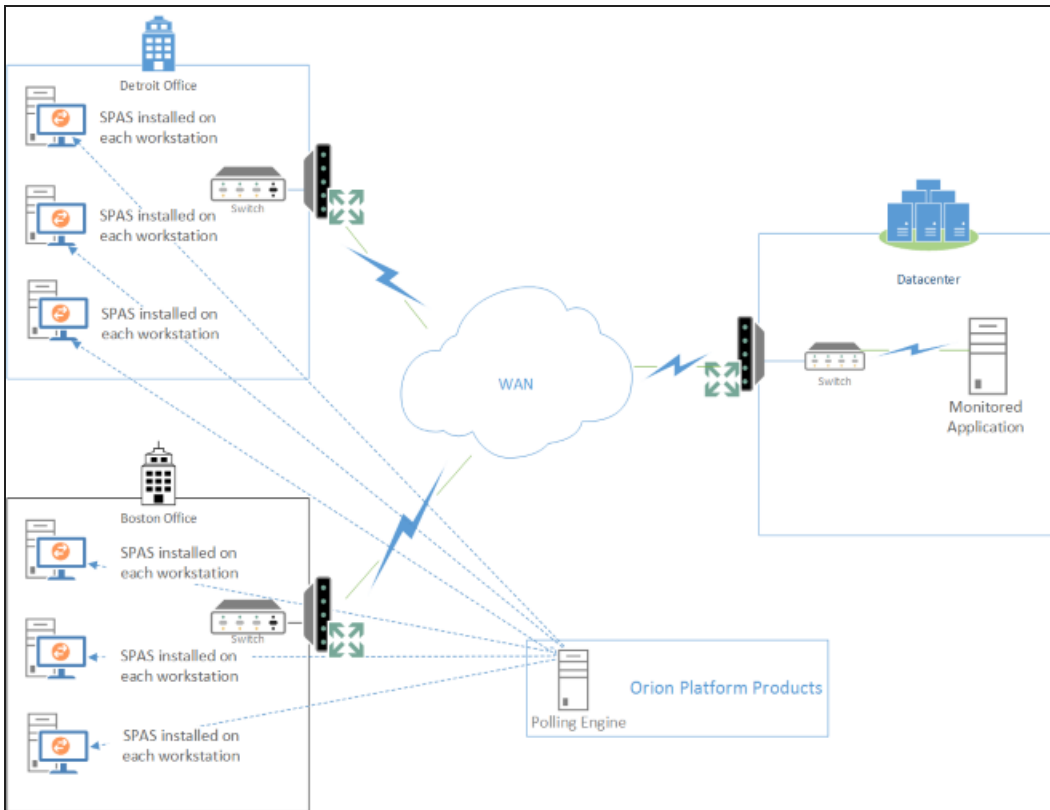
Aggregation per computer with access to network (NPAS)



- Create a port mirror, SPAN, or network tap on the switch with all the network traffic to or from the application.
- You can monitor multiple applications using the same NPAS.

1. Click Settings > All Settings in the menu bar.
2. Click QoE Settings > Manage QoE Packet Analysis Sensors > Add Packet Analysis Sensor.
3. Select the Network option, and then click Add Nodes.
4. Choose the node with the port mirror, SPAN, or network tap setup to monitor your network switch.
5. Assign and test the credentials for the selected node.
6. Click Add Nodes and Deploy Agents to deploy the network sensor to the node.

Aggregation per computer with access to application servers (SPAS)



1. Click Settings > All Settings in the menu bar.
2. Click QoE Settings > Manage QoE Packet Analysis Sensors > Add Packet Analysis Sensor.
3. Select the Server option, and then click Add Nodes.
4. Select the all user computers to monitor.
5. Assign and test the credentials for each node.
6. Click Add Nodes and Deploy Agents to deploy an agent on the node.

Monitor traffic to and from a port mirror, SPAN, or network tap

Network sensors monitor all packets that flow through the switch and categorize the packets by application.

After you deploy a network sensor to the port mirror, SPAN, or network tap, the sensor monitors packets to and from the node, identifies the application or the URL, and analyzes the packets for QoE metrics, such as response time or traffic volume.

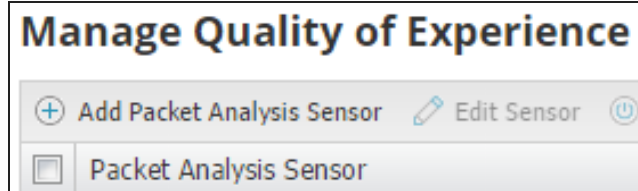
Before you begin

- Data from sensors is directed to the polling engine assigned to the node when the sensor was deployed.
- A high number of applications or nodes can cause performance issues with the sensors.

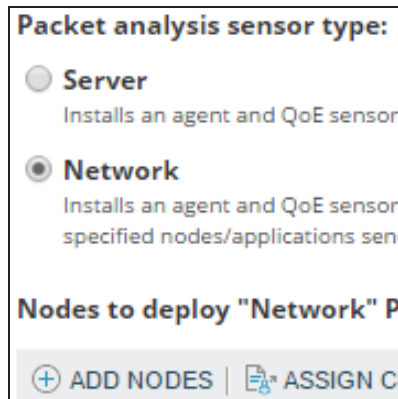
The network sensor must be installed on a Windows computer that is monitoring the switch's SPAN or mirror port.

Install the network sensor


1. Click Settings > All Settings in the menu bar.
2. Click QoE Settings > Manage QoE Packet Analysis Sensors > Add Packet Analysis Sensor.



3. Select Network, and click Add Nodes.




4. Move the node that monitors your switch to the Selected Nodes panel, and click Add Selected Nodes.

 Make sure you select the Windows machine that is monitoring the SPAN or mirror port of the switch.

5. Assign and test the credentials for the node, and click Submit.
6. Click Add Nodes and Deploy Agents.

When the sensors are successfully deployed, a message is displayed in Notifications.

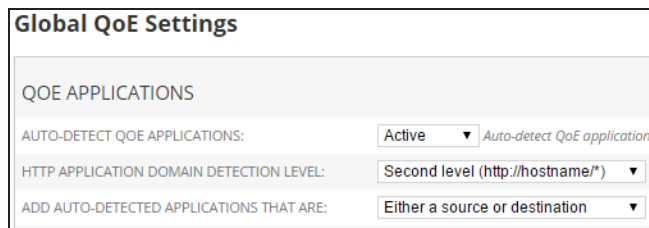
 Deploying the sensor and receiving the first set of data can take several minutes. When the deployment is finished, select the sensor on the Manage Quality of Experience (QoE) Packet Analysis Sensors page, click Edit Sensor, and verify the selected NIC.

Monitor website traffic based on domains

After you deploy a network sensor, you can filter application traffic based on domain names instead of all http traffic.

1. Click Settings > All Settings in the menu bar.
2. Click QoE Settings > Manage Global QoE Settings.

3. Set the HTTP application domain detection level.



Global QoE Settings

QOE APPLICATIONS

AUTO-DETECT QOE APPLICATIONS: **Active** Auto-detect QoE application


HTTP APPLICATION DOMAIN DETECTION LEVEL: **Second level (http://hostname/*)**

ADD AUTO-DETECTED APPLICATIONS THAT ARE: **Either a source or destination**

4. Set the Auto-detect QoE applications option to Active, and click Submit.

 QoE can automatically detect the first 50 applications, or you can add specific applications.

Discovered applications have the "No Risk" Risk Level and the "Both Business and Social" Productivity Rating associated with them. To modify the Risk Level and Productivity Rating, click QoE Settings > Manage (QoE) Applications, and edit the application.

 Use the Global QoE Settings page to disable monitoring or discovery of multiple applications. Select the applications, and click Disable Monitoring or Disable Discovery.

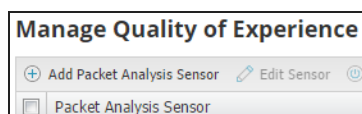
Nodes are automatically detected and added by default. To specify which nodes and applications to monitor manually, see [Monitor QoE applications and nodes](#).

Monitor traffic to and from a specific node




These sensors monitor all the application traffic into and out of the server they are installed on.


After you deploy a server sensor to the application node, the sensor monitors packets to and from the node, identifies the application or the URL, and analyzes the packets for QoE metrics, such as response time or traffic volume.

1. Click Settings > All Settings in the menu bar.
2. Click QoE Settings > Manage QoE Packet Analysis Sensors, and click Add Packet Analysis Sensor.

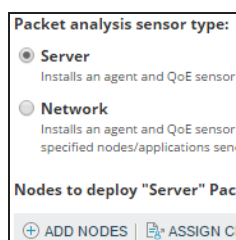


Manage Quality of Experience

 Add Packet Analysis Sensor  Edit Sensor 

 Packet Analysis Sensor

3. Select Server, and click Add Nodes.





Packet analysis sensor type:

☒ **Server**
Installs an agent and QoE sensor

☐ **Network**
Installs an agent and QoE sensor
specified nodes/applications sen

Nodes to deploy "Server" Pac

 ADD NODES  ASSIGN C

4. Move the Windows nodes that will host the server sensors to the Selected Nodes panel, and click Add Selected Node.
5. Assign and test credentials for each node, and click Submit.
6. Click Add Nodes and Deploy Agents. QoE auto-discovers the applications on the servers.

When the sensors are successfully deployed, a message is displayed in Notifications.

- Deployment may take some time and will run as a background process.
- QoE automatically chooses settings, including the interface to capture traffic data and limits to memory and CPU, during deployment. You can change these settings after deployment is complete by selecting the sensor and clicking Edit.
- You can confirm the deployment status on the Manage QoE Packet Analysis Sensors page.

To specify manually which applications to monitor, see [Monitor applications for QoE](#). Applications are automatically detected and added by default.

Remove a sensor

Removing a sensor from a node is a two-step process. First delete the sensor using the Orion Web Console, and then remove the communication agent directly from the node.

1. Delete the sensor using the Orion Web Console:
 - a. Click Settings > All Settings in the menu bar.
 - b. Click QoE Settings > Manage QoE Packet Analysis Sensors.
 - c. Select the node.
 - d. Click Delete Sensor.
 - e. Click Delete when prompted.
2. Remove the agent directly from the node:
 - a. Log in to the computer with administrative credentials.
 - b. Navigate to Control Panel > Programs and Features.
 - c. Select `SolarWinds Agent`.
 - d. Click Uninstall.
 - e. Follow the onscreen prompts to completely uninstall the agent.

The sensor is removed from the list and the communication agent is uninstalled and cannot gather traffic data or send data.

Monitor QoE applications and nodes

By default nodes and applications are automatically monitored by QoE when you deploy a Network or Server Sensor. You can automatically filter which nodes or applications are monitored.

See [Global QoE Settings](#) for more information on changing these settings.

- Server Sensors automatically monitor the top 50 applications on the node they are installed on based on the global settings. You can change which applications are monitored after the sensor is deployed.

Manage global QoE settings


You can control how Packet Analysis Sensors behave by changing the settings on Manage Global QoE Settings page. Settings are distributed to sensors regularly when the agent is updated. You can manually update an agent from the Manage Agents page.

QoE applications

Control how you monitor QoE applications for both Network Packet Analysis Sensors and Server Packet Analysis Sensors.

Auto-detect QoE applications

Use this to detect and monitor traffic associated with all applications that fulfill the auto-detection rules defined on this page. This is active by default. You must select applications manually when this option is disabled.

 If you automatically detect nodes, you should also automatically detect applications to receive all metrics.

HTTP application domain detection level

Choose how QoE breaks up monitored http traffic.

- Top level (http://*) - Monitor all http traffic.
- Second level (http://hostname/*) - Separate and monitor http traffic based on domains.
- Third level (http://hostname/path1/*) - Separate and monitor http traffic based on the domain and first level directory within each domain.

Add auto-detected applications

Refine the monitored applications by choosing to monitor all application traffic sources, traffic destinations, or all application traffic. Packet sources and destinations are based on the source or destination IP address included in the packet.

- Transaction destinations (servers) - Monitor applications that receive traffic based on the destination IP address of the packet.
- Transaction sources (client) - Monitor applications that generate traffic based on the source IP address of the packet.
- Either a source or destination - Monitor all application traffic.

For each node, include top X application that have at least Y% of total QoE traffic.


Filter the number of monitored applications to applications that generate a certain amount of network traffic.

Nodes with QoE traffic

Control how you monitor QoE nodes for Network Packet Analysis Sensor.

Auto-detect QoE nodes

Use this to detect and monitor the first 50 nodes with network traffic. This is active by default. You must select nodes manually when this option is disabled.

 If you automatically detect nodes, you should also automatically detect applications to receive all metrics.


Add auto-detected monitored nodes

Further refine the nodes that are monitored by choosing to monitor all nodes that are traffic sources, traffic destinations, or all nodes that generate or receive network traffic. Packet sources and destinations are based on the source or destination IP address included in the packet.

- Transaction destinations (servers) - Monitor nodes that receive traffic based on the destination IP address of the packet.
- Transaction sources (client) - Monitor nodes that generate traffic based on the source IP address of the packet.
- Either a source or destination - Monitor all traffic.


Monitor applications for QoE

Applications are automatically monitored when traffic is detected by the Packet Analysis Sensor. However, you can manually select specific applications to monitor. QoE installs with the ability to monitor over 1000 pre-defined applications, including FTP, RDP, CIFS, SQL, and Exchange. You can also define your own custom HTTP applications.

- 
- Because of the hardware requirements needed to process large amounts of traffic, SolarWinds recommends that you preferentially monitor business-critical nodes and applications.
 - You should not assign more than 50 applications to a single node due to potential performance issues. However, you can monitor up to 1000 applications.

Monitor QoE applications automatically

While QoE sensors automatically detect and monitor applications by default, the settings may have changed or you may have upgraded from a version of QoE that does not automatically monitor applications.

 Only applications that meet the criteria selected in QoE Applications are monitored automatically.


1. Click Settings > All Settings in the menu bar.
2. Click QoE Settings > Manage Global QoE Settings.
3. Select Active in Auto-detect QoE applications.
4. Change other settings to refine the number of applications you automatically monitor. See [Global QoE Settings](#) for more information on the settings.
5. Click Submit.

It may take some time for the settings to apply.


Monitor applications manually

You may choose to add monitored applications manually to QoE.


1. Click Settings > All Settings in the menu bar.
2. In the Settings grouping, click QoE Settings > Manage QoE Applications.

-  ■ Applications are only listed if there are monitored nodes. You must first add a Network or Server Sensor before you can enable any applications.
- Enabled applications are currently being monitored on at least one node.
- Applications can be disabled, which means that no traffic for the application is currently collected on any node.

3. Click Add New.
4. Select Choose a pre-configured application.

-  Applications that are already enabled do not display in the list.

5. Use the Search or Group By options to find the application you want to monitor, select it, and then click Next.
6. On the Configure Application view, edit the Category, Risk Level, or Productivity Rating as necessary, and then click Next.
7. On the Specify Nodes view, choose the nodes you want to monitor for this type of traffic.

-  Only nodes that have already been specified as nodes to monitor on the Manage QoE Nodes page display in this list.

8. Click Next.
9. Review your choices on the Summary page, and then click Finish.

Your newly enabled application will display on the Manage QoE Applications page in alphabetical order.


Monitor nodes with a network sensor

Nodes are automatically detected and monitored when network traffic originates from or terminates at a node. However, you can manually specify the nodes after the network sensor has been successfully deployed. For information about adding applications, see [Monitor applications for QoE](#).

-  You can monitor up to 50 nodes per network sensor.

Add nodes automatically

While Network Sensors automatically detect and monitor nodes by default, the settings may have changed or you may have upgraded from a version of QoE that does not automatically monitor nodes. QoE automatically monitors the first 50 nodes with traffic.

-  ■ Automatic node discovery may not be 100% accurate due to devices with the same IP addresses in your network.
- Only nodes that meet the criteria selected in Nodes with QoE Traffic are added automatically.

1. Click Settings > All Settings in the menu bar.
2. Click QoE Settings > Manage Global QoE Settings.
3. Select Active in Auto-detect QoE nodes.
4. Change other settings to refine the number of nodes you automatically monitor. See [Global QoE Settings](#) for more information on the settings.
5. Click Submit.

It may take some time for the settings to apply.

Add nodes manually

If a node is already monitored and you want to monitor it with a different sensor, you must delete the node from the original sensor before you can add it to the new network sensor.

1. Navigate to the Manage QoE Packet Analysis Sensors page.
2. Expand the Network sensor that you want to add a node to.

<input checked="" type="checkbox"/> DEV-AUS-MBRU-04	
Node	Applications
10.110.67.159	4Shared, Amazon Web Services, CIFS, FTP, HTTP, MS SQL

3. Click the Add Node to Monitor button.
4. On the Create QoE Node page, choose the managed nodes you want to monitor with this network sensor.
5. On the Select QoE Applications page, choose the applications you want to monitor for these nodes. See [Monitor applications for QoE](#) for more information.
6. Review your selections on the Summary page.
7. Click Finish.


View the nodes and applications selected by expanding the Network Sensor you just configured.

Ignore traffic from applications or nodes

You can ignore traffic generated by applications or from a specific node.

Ignore application traffic

If you decide to no longer monitor an application, disable discovery or monitoring for that application in the Manage QoE Applications page.

 These settings are on a global level. You cannot turn application discovery or monitoring on or off for specific sensors.


1. Click Settings > All Settings in the menu bar.
2. Click QoE Settings > Manage QoE Applications.
3. Toggle Monitoring or Discovery OFF.

Use the following table to determine which combination of settings you want to use.

	MONITORING ON	MONITORING OFF
DISCOVERY ON	Applications are automatically discovered and application traffic is monitored	Applications are automatically discovered, but application traffic is not monitored
DISCOVERY OFF	Applications cannot be automatically discovered, and application traffic is monitored	Applications cannot be automatically discovered, and application traffic is not monitored

Ignore node traffic

You can permanently ignore all traffic from specific nodes that you monitor on a network sensor. This is often used to reassign a node to a different network sensor.

 You cannot add a node back to its original network sensor.

1. Click Settings > All Settings in the menu bar.
2. In the Settings grouping, click QoE Settings > Manage QoE Packet Analysis Sensors.
3. Select a network sensor, and click Edit.
4. Select the node you want to remove, and click Delete.

The node is removed from the sensor and all traffic to and from the node is ignored.

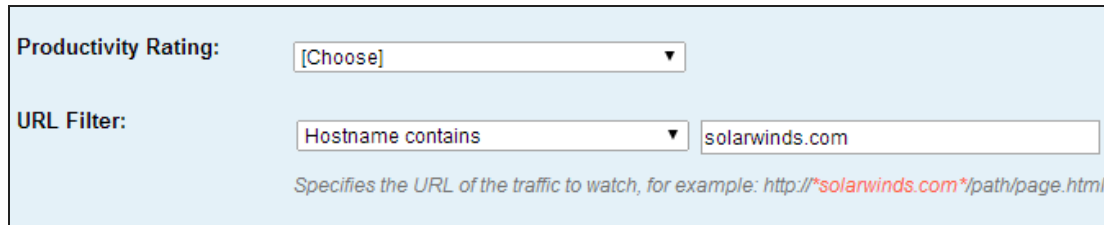
Define custom HTTP applications

In addition to choosing from predefined applications, you can define custom HTTP applications, and add them to nodes you are monitoring.

1. Click Settings > All Settings in the menu bar.
2. Click QoE Settings > Manage QoE Applications.
3. Click Add New.
4. On the Select Application page, select Create a new HTTP application, and click Next.
5. On the Configure Application page, enter the name and description of the application you're creating, and then choose the Category, Risk Level, and Productivity Rating appropriate for the application.

6. Set the URL Filter. This specifies the HTTP application traffic to monitor. When you choose which filter to use in the drop-down, notice that the example changes to indicate how the accompanying text field will be used.

For example, selecting Hostname contains changes the help text to `http://*...*/path/page.html`. Any text you enter will be included in the filter where the "..." is.









7. Enter the hostname or URL for your filter, and then click Next.
8. On the Specify Nodes page, choose the nodes to monitor for this type of traffic. Only nodes that have already been specified as nodes to monitor (on the Manage QoE Nodes page) will display in this list.
9. Click Next. Review your choices on the Summary page, and click Finish.

Your new application will display on the Manage QoE Applications page in alphabetical order.

Advanced sensor configuration

Sensors cannot be edited until they are fully deployed. An entry displays in the notification area when your sensor is deployed, or you can check the Manage QoE Packet Analysis Sensors page. The status of completely deployed and working sensors is Up.

Add Packet Analysis Sensor Edit Sensor Enable Sensor Disable Sensor Delete Sensor							
Packet Analysis Sensor	Enabled	Sensor Type	QoE Nodes	CPU Utilization %	Agent Status	Sensor Status	
    	Yes	Server	1	0.0%	 Connected Manage Agent	Up	

When you click Edit Sensor, you can configure:

- the [monitored interface](#)
- the [allocated CPU cores and memory](#)

Configure which interface to monitor for traffic

When you deploy a sensor, the first available interface is monitored for traffic. Once the sensor is installed, you can go back and change the monitored interface.

1. Click Settings > All Settings in the menu bar.
2. Click QoE Settings > Manage QoE Packet Analysis Sensors.
3. Select the sensor to edit.
4. Click Edit Sensor.
5. Select the desired interface from the Interface to capture QoE data drop-down list.
6. Click Save.


Set the number of CPU cores and the amount of memory QoE can use

When a sensor is deployed, QoE automatically allocates one CPU core and 256 MB of memory to the sensor. After the sensor is installed, you can change the allocated CPU cores and memory.


For sensors, the memory usage scales with the traffic load. The more flows that are going on the line, the more memory you need.

NUMBER OF CPU CORES	GUIDELINES
1	Not Recommended
2	Suitable for 100 Mbps links
3 - 4	Gigabit links with low utilization
5 - 6	Gigabit links with medium utilization
7+	Gigabit links with high utilization

1. Click Settings > All Settings in the menu bar.
2. Click QoE Settings > Manage QoE Packet Analysis Sensors.
3. Select the sensor to edit.
4. Click Edit Sensor.
5. In the Memory field, select the number of GB you want to allocate to the sensor.

 If you allocate less than the recommended amount of memory, you may see reduced performance.

6. In the CPU Cores field, select the number of CPU cores you want to allocate to the sensor.

 If you allocate fewer than the recommended number of CPU cores, you may see reduced performance.

7. Click Save.

Configure QoE thresholds

You can modify the application response time (ART), network response time (NRT), volume, and transaction thresholds that are used to alert you to irregularities in your network.

 We recommend that the sensors collect a few days' worth of data before setting thresholds.

1. Click Settings > All Settings in the menu bar.
2. Click QoE Settings > Manage QoE Applications.
3. Select the application to edit, and click Edit.
4. Click Next, and then click Next again.
5. On the Summary page, click the plus sign by Thresholds.
6. Select Override Orion General Thresholds next to each data type.

7. Change the threshold. You can use specific thresholds or you can use a dynamic threshold based on the baseline established. The default baseline is seven days, which is configurable in the Orion Polling Settings page.
8. Click Finish.

Packet Analysis Sensor agents

The software that provides a communication channel between your SolarWinds server and the monitored object to which you have deployed your Packet Analysis Sensor is called an "agent". Agents are used to send the data that QoE collects back to the SolarWinds Orion server. The agent runs as a service, and it has a small installed footprint (under 100MB installed).


Monitor devices with SolarWinds Orion agents

An agent is software that provides a communication channel between the Orion server and a Windows computer. Agents are used to provide information about key devices and applications that you specify. This can be beneficial in the following situations:

- Polling hosts and applications behind firewall NAT or proxies.
- Polling node and applications across multiple discrete networks that have overlapping IP address space.
- Secure, encrypted polling over a single port.
- Support for low bandwidth, high latency connections.
- Polling nodes across domains where no domain trusts have been established.
- Full ,end-to-end encryption between the monitored host and the main poller.

You can monitor servers hosted by cloud-based services such as Amazon EC2, Rackspace, Microsoft Azure, and other Infrastructure as a Service (IaaS).

After deployment, all communication between the SolarWinds Orion server and the agent occur over a single fixed port. This communication is fully encrypted using 2048-bit TLS encryption. The agent protocol supports NAT traversal and passing through proxy servers that require authentication.

 Java Management Extensions (JMX) polling is not supported using a Windows agent.



Agent requirements

Agent software is free. You remain bound by the limits of the license you own regardless of how information is polled, either through an agent or another polling method.

 ■ Windows agents run as a service.

Before you deploy agents to a target computer, review the following system requirements.

TYPE	REQUIREMENTS
Operating System	The following operating systems are supported for both 32-bit and 64-bit computers:

TYPE	REQUIREMENTS
	<ul style="list-style-type: none"> ■ Windows Server 2008 ■ Windows Server 2008 R2 ■ Windows Server 2008 R2 SP1 ■ Windows Server 2012 ■ Windows Server 2012 R2 ■ Windows 7, Windows 7 SP1 ■ Windows 8, Windows 8.1 ■ Windows 10 <div>  Only Pro, Enterprise, and Ultimate workstation operating systems editions are supported. </div>
Other software	<p>The following software packages are installed by the agent installer if necessary:</p> <ul style="list-style-type: none"> ■ Microsoft Visual C++ 2013 Redistributable Package for 32-bit or 64-bit ■ .NET Framework 4.0 (You must install this manually if you are installing an agent on Windows Server 2008 R2 or earlier or Windows Core) ■ .NET Framework 4.5 (Required for Windows Server 2008 R2 SP1 and later)
Security	<p>The VeriSign Root Certificate Authority (CA) must be current. This is required because the agent software is signed using a VeriSign certificate. To install a certificate, see Certificates and the agent.</p> <p>After the agent is installed, it runs as the Local System account and does not require administrative permissions to function.</p>
Account permissions	<p>If you want to deploy agents from the SolarWinds Orion server, the following requirements must be met:</p> <ul style="list-style-type: none"> ■ The account used for remote deployment must have access to the administrative share on the target computer: \\<hostname_or_ip>\admin\$\temp. ■ User Account Control (UAC) must either be disabled on the target computer, or the built-in Administrator account must be used. <div>  Other remote or mass deployment methods do not have the same requirements. </div>
HDD	Approximately 100 MB of hard drive space on the target computer, for installation only

Agent resource consumption

RESOURCE	CONSUMPTION
CPU	Less than 1% on average under normal operating conditions (0.24% on average)
Memory	10 - 100 MB, depending on the number and types of jobs

RESOURCE	CONSUMPTION
Bandwidth	Roughly 20% (on average) of the bandwidth consumed by the WMI protocol for transmission of the same information For example, Agent: 1.3 kB/s versus WMI at 5.3 kB/s
Storage	100 MB when installed

A single polling engine can support up to 1,000 agents.

Agent port requirements

For agent-initiated communications, port 17778 (inbound) must be open on SolarWinds Orion servers running Windows Server 2012 or port 17791 on SolarWinds Orion server running Windows Server 2008 R2 SP1 and communication through the port must be allowed by the firewall. It is used continuously after the agent is deployed. Communication is initiated outbound from the agent to the Orion server.

For server-initiated communications, port 17790 must be opened (inbound) on the remote computer.

- 135 (DCE/RPC Locator service) Microsoft EPMAP. This port must be open on the client computer (inbound) for remote deployment.
- 445 Microsoft-DS SMB file sharing. This port must be open on the client computer (inbound) for remote deployment.

Agent settings

The Agent Settings page provides access to all of the settings and tools needed to install and manage agents. Additional agent settings can be found in the [Windows Control Panel](#).

Navigate to the Agent Settings page


1. Click Settings > All Settings in the menu bar.
2. Under Product Specific Settings, click Agent Settings.
 - Manage Agents: opens the Manage Agents page from which you can add a new agent, edit, update, or reboot an existing agent.
 - Download Agent Software: opens the Agent Downloads page from which you can mass deploy or manually install an agent.
 - Define Global Agent Settings: opens the Global Agent Settings page from which you can allow automatic agent registration and allow automatic agent updates.

Adjust the Global Agent Settings

1. Click Settings > All Settings in the menu bar.
2. Under Product Specific Settings, click Agent Settings.
3. Click Define Global Agent Settings.

The following options are available on the Global Agent Settings page:

- Allow automatic agent registration: Select this option to automatically register the agent and verify communication with the Orion Server. If this option is disabled, you can register any waiting agents by clicking Settings > All Settings > Manage Agents > Add Agent > Connect to a previously installed agent.
- Automatically create node: Agents are automatically registered as Orion nodes.
- Allow automatic agent updates: Select this option to automatically upgrade the agent software when updates are available. This process pushes a new version of the agent to client computers over the agent communication channel. No extra ports or permissions are needed. After the agent receives the new version, it updates itself. This process typically does not require rebooting.

 If automatic updates are disabled and a new version of the software is installed on the server, outdated agents may not be able to communicate with the server. Ensure all agent versions match the version of the server.

- XX Hours: Control the length of time the agent displays as new in the Manage Agents list.


Quality of Experience requirements

Before you deploy a Packet Analysis Sensor to a device to monitor QoE, review the following minimum system requirements.

You will need administrative privileges for each node or switch.


 Sensors **cannot** be installed on 32-bit computers and do **not** support communication over https.

Network Packet Analysis Sensors (NPAS)

HARDWARE/SOFTWARE	REQUIREMENTS	
OS	Windows 7 or later, 64-bit	
	Windows Server 2008 or later, 64-bit	
	 32-bit operating systems are not supported.	
CPU Cores	2 CPU Cores + 1 CPU Core per 100 Mbps	
Hard drive space	500 MB	
RAM	1 GB + 1 GB per 100 Mbps	
	(2 GB + 1 GB per 100 Mbps recommended)	
Network	1Gbps maximum throughput	
Port monitoring	For a physical monitored switch:	For a virtual monitored switch:
	<ul style="list-style-type: none"> ■ SPAN ■ Mirror port ■ In-line tap 	<ul style="list-style-type: none"> ■ Promiscuous port groups ■ vTap

HARDWARE/SOFTWARE	REQUIREMENTS
	<p>Port monitoring requires at least one extra network interface to collect data from the managed network interface, a server to monitor the copied traffic, and a network cable to connect the mirrored port to the physical server.</p> <p>View your vendor documentation for instructions about how to set up port mirroring. You can create port mirrors for both physical switches and virtual switches.</p>

Server Packet Analysis Sensors (SPAS)

HARDWARE/SOFTWARE	REQUIREMENTS
OS	<p>Windows 7 or later, 64-bit</p> <p>Windows Server 2008 or later, 64-bit</p> <p> 32-bit operating systems are not supported.</p>
CPU Cores	2 CPU Cores + 1 CPU Core per 100 Mbps
Hard drive space	500 MB
RAM	<p>256 MB + 500 MB per 100 Mbps</p> <p>(256 MB recommended + 500 MB per 100 Mbps)</p>
Network	1Gbps maximum throughput

Remote computer port requirements

See [Agent requirements](#).

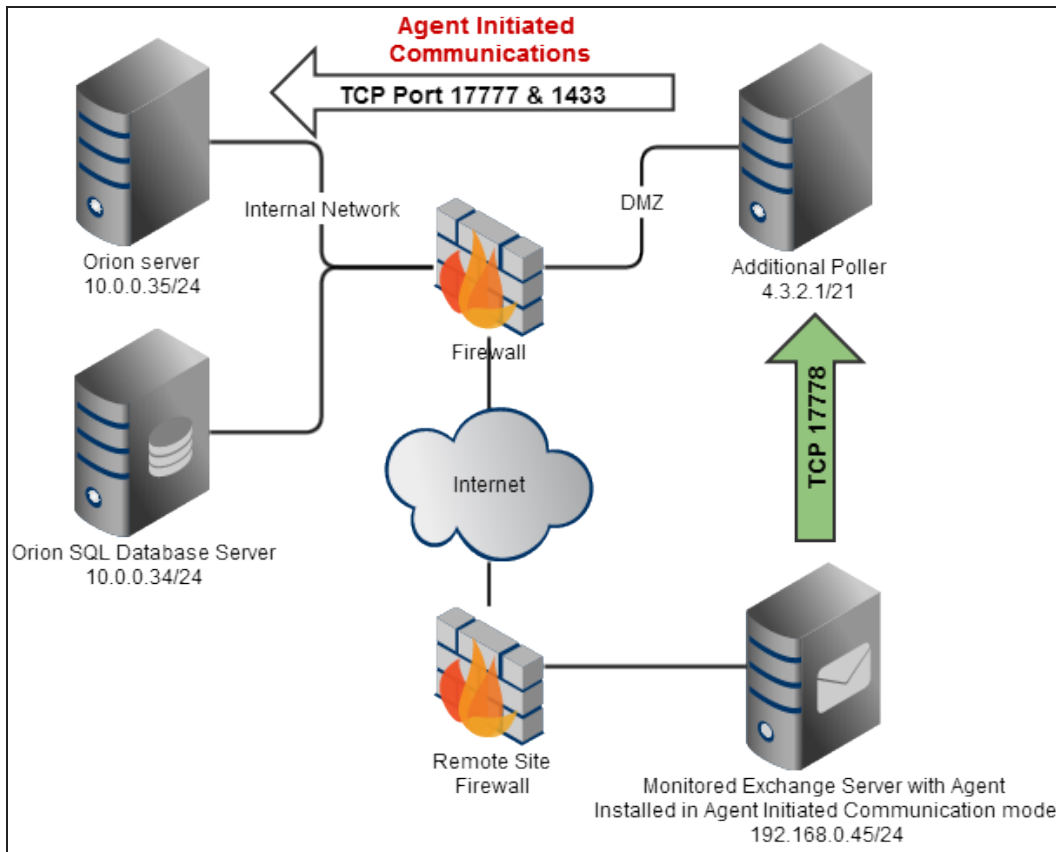
Server-initiated communication

All communication between your Orion server or additional polling engine and the agent is initiated by the Orion server, and the agent does not initiate communication to your Orion server. You must have a direct route from the Orion server or additional poller to the host where the agent is installed. To use this communication method, port 17790 must be open on the firewall of the remote host to retrieve information from the agent.

This communication method is also known as a passive agent.

Agent-initiated communication

All communication between your Orion server or additional poller engine and the agent is initiated by the agent, and your Orion server does not initiate communication with the agent. You do not need to have a direct route from the Orion server or additional poller to the host where the agent is installed. To use this communication method, port 17778 must be open on the Orion server firewall to receive information from the agent.



This communication method is most useful when the agent is installed on a network separated from your Orion server by one or more NAT devices, and you have no easy way to connect the two.

This communication method is also known as an active agent. In active mode, there are no listening ports on the agent.

Windows agent deployment

SolarWinds Orion products supports three methods of deploying an agent to a client computer running Windows.

- Push the agent software from the Orion Server to one or more client computers.
- Mass deploy the agent software to multiple computers using a mass deployment technology, such as Group Policy.
- Manually install the agent on a client computer.

i Agents do not work with AppInsight for SQL when the SQL Server being monitored is in a cluster.

Deploy Windows agent software through a server push


Select this method of deployment to perform a network-wide deployment from the SolarWinds Orion server. This method does not require downloading additional files. In order for this deployment method to succeed, the SolarWinds Orion server must be able to communicate with the client computers.

1. Click Settings > All Settings in the menu bar.
2. Under Node & Group Management, click Manage Agents.
3. Click Add Agent.
4. Select how you would like to add the agent.


Deploy the agent on my network

Select this method to install the agent on multiple client computers.

1. On the Deploy Agent on Network page, enter the IP address or host name of the Windows computer where you want the agent to be installed, or select nodes from the list, and then click Next.

 The IP address field does not accept ranges. Only add computers that are not nodes in the system.

2. On the Agent Settings page:
 - a. Select the computer you selected in the previous step, and click Assign Credentials
 - b. Select a credential from the list, or enter new credentials, and click Submit.

 You can assign credentials to multiple locations or nodes by selecting multiple entries.

3. Click Deploy Agent.


When the connection is successful, the agent displays in the agent list on the Manage Agents page.

Connect to a previously installed agent

Select this method to connect to agents that were configured with server-initiated communication, or if Allow Automatic Agent Registration is not enabled. When you connect to an agent, you first need to select the communication mode that was chosen when the agent was installed. If the communication mode is server-initiated (passive), a shared secret was required during installation. This secret must be entered again here.

1. On the Add Agent page, enter a name for the Agent.
2. Select the agent communication mode.
3. For server-initiated communication:
 - a. Enter the IP address or host name where the agent is located.
 - b. Enter the shared secret.
 - c. Optional: Expand Advanced and adjust the following settings as needed:
 - a. Change the agent port number. This is the port the agent uses for listening.
 - b. Use a proxy. Select a proxy and enter the proxy URL.
 - c. Use proxy authentication, and enter credentials.
4. For Agent-initiated communication, select the agent from the Agent list.

5. Select Allow automatic agent updates to upgrade the agent automatically when upgrading to new versions of Orion Platform modules that support the agent.

 Disabling this option requires you to manually upgrade agents after upgrading your Orion Platform products.

6. Click Submit.

When the connection is successful, the agent displays in the agent list on the Manage Agents page.

Deploy the Windows agent manually

Selecting this method of deployment may be helpful in troubleshooting connectivity issues with another form of agent deployment. This method is also helpful when the Orion server cannot communicate directly with the endpoint where the agent will be installed, such as in the case of Active Agent mode.

1. Click Settings > All Settings in the menu bar.
2. Under Product Specific Settings, click Agent Settings > Download Agent Software.
3. Click Install Manually, and click Next.
4. Click Download MSI.
5. Download and copy the MSI file to the client machine, and execute it.
6. In the Installation wizard, select Agent Initiated Communication or Orion Server Initiated Communication.
7. Enter the SolarWinds Orion server IP address or hostname, and the SolarWinds Orion administrator account credentials.

When installation is successful, the agent displays in the agent list on the Manage Agents page.

Mass deploy a Windows agent

If you are already using a mass-deployment technology, this deployment method is an easy way to get agents on a large number of computers.

Polling engine selection is important. When you download the MST file, the file includes the polling engine IP address and other vital information. When you deploy the agent using the MSI file, along with the MST file on the managed node, the agent will be installed and pointed to the correct polling engine.

What is an MST file?

A Microsoft Transform (MST) file is a collection of specified changes applied to a base Windows Installer package file at the time of deployment. It is an overlay on top of an existing MSI file that defines what specific components or features of an application get installed. The MST file modifies the Microsoft Installer package.

After the software you want to install is packaged in the Windows Installer package format, you can use MST files to customize the software for your organization, such as installing only specific features. The modular design of Windows Installer packages simplifies deployment. When you apply transforms to an MSI file, Windows Installer can dynamically add or modify data in the installation database to customize the installation of the application. Additional information on creating MST files can be found on technet.microsoft.com.

Generate and download the MST file

1. Click Settings > All Settings in the menu bar.
2. Under Product Specific Settings, click Agent Settings > Download Agent Software.
3. Click Mass Deploy to Multiple Machines, and click Next.
4. Select the agent communication mode.
 - For agent-initiated communication, enter the polling engine you want the agent to use. You may need to manually enter the polling engine information if the IP address is different from what the SolarWinds Orion server reports. This happens when the monitored host is behind a NAT or proxy device. In these cases, enter the IP address of the SolarWinds Orion server or the additional polling engine as it is accessible from the host where the agent will be installed.
 - a. To use an existing polling engine, select Use Connection Details from Polling Engine, and then select a polling engine from the list.
 - b. To manually enter the polling engine IP address, select Enter Connection Details Manually, and then enter the host name and IP address. The IP address is required. Use the host name and IP address of the polling engine that you can access from the client.
 - For server-initiated communications, enter your agent communication port number. The default port is 17790.
5. Click Download .MSI, and save the file.
6. Click Download .MST, and save the file.

Add the MST file to a Group Policy

1. Share a folder containing the MST and MSI files with proper permissions.
2. In Active Directory, locate the container where you want to advertise the application, and then access the container properties.

 A container is a site, domain, or organizational unit (OU).

3. Create a Group Policy object.
4. In Advanced Options, add the Software installation policy. Select the network path for the agent MSI and MST files.

The agent is deployed at login and is registered by Orion (if auto-registration is enabled).

Deploy with a Gold Master Image

Use a Gold Master Image when you want to maintain a master image of agent software that is copied when a new server is provisioned. This saves time for virtual machines, physical servers, and cloud instances. Whenever a new server is brought online using this image, the agent will already be installed.

Install an agent offline

1. Click Settings > All Settings in the menu bar.
2. Under Product Specific Settings, click Agent Settings > Download Agent Software.
3. Click Distribute via a Golden Master Image, and click Next.

4. Select the agent communication mode.
 - For agent-initiated communication, enter the polling engine you want the agent to use. You may need to manually enter the polling engine information if the IP address is different from what the SolarWinds Orion server reports. This happens when the monitored host is behind a NAT or proxy device. In these cases, enter the IP address of the SolarWinds Orion server or the additional polling engine as it is accessible from the host where the agent will be installed.
 - a. To use an existing polling engine, select Use Connection Details from Polling Engine, and then select a polling engine from the list.
 - b. To manually enter the polling engine IP address, select Enter Connection Details Manually, and then enter the host name and IP address. The IP address is required. Use the host name and IP address of the polling engine that you can access from the client.
 - For server-initiated communications, enter your agent communication port number. The default port is 17790.
5. Click Download .ZIP, and save the file.
6. Extract the contents of the ZIP file, and double-click `setup.bat`.
7. Follow the instructions in the Installation wizard.

Enable server-initiated communication on deployed agents

If you are deploying a server-initiated agent, take the following steps to enable agent communication with your SolarWinds Orion server.

1. Click Settings > All Settings in the menu bar.
2. Under Node & Group Management, click Manage Agents.
3. Click Add Agent > Connect to a previously installed agent > Next.
4. Enter a name for the agent, and click Server-initiated communication.
5. Enter the IP address of the node where the agent is deployed, and the port number for the agent. The default port is 17790.
6. Click Submit.


Deploy a Windows agent with Patch Manager

You can only perform this deployment method if you have successfully configured Patch Manager to push software in your environment. This method contains four parts you must perform in order: download the installation files, build the package, add deployment rules, and publish the package.

Download the installation files

1. Click Settings > All Settings in the menu bar.
2. Under Product Specific Settings, click Agent Settings > Download Agent Software.
3. Click Mass Deploy to Multiple Machines, and click Next.
4. Select the communication method and enter the required information. For more information, see [Mass deploy a Windows agent](#).

5. Download and save the MSI and MST files to a location on your Patch Manager server.

 Record the Latest Version value under the MSI file download. This is needed when creating a package in Patch Manager.

Optional: Rename the SolarWinds agent files to `SolarWinds Agent <version>` for easier tracking.

Build the package

1. Launch SolarWinds Patch Manager.
2. In the navigation pane, expand Administration and Reporting > Software Publishing, and then click SolarWinds, Inc. Packages.



3. From the SolarWinds, Inc. Packages action pane, click New Package. This launches the Patch Manager Package Wizard.



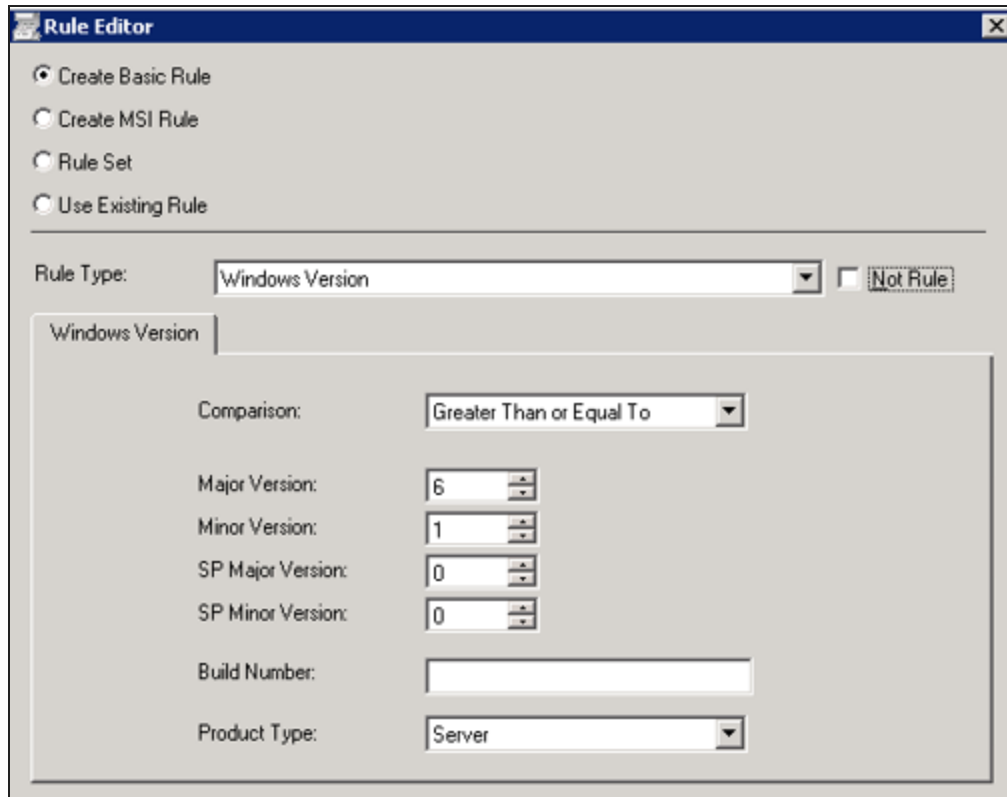
4. In the package information screen, enter the following general information for the package:
 - Package Title: SolarWinds Orion Agent (version number) MSI
 - Description: SolarWinds Orion Agent
 - Classification: Tools
 - Vendor: SolarWinds, Inc.
 - Product: Orion Agent (This must be entered the first time)
 - Severity: None
 - Impact: Normal
 - Reboot Behavior: Can request reboot

 All other fields can be left empty.


5. Click Next.

Add deployment rules

1. On the Prerequisite Rules window, click Add Rule.
2. Select Windows Version as the Rule Type, and enter the following information:



The screenshot shows the 'Rule Editor' dialog box. At the top, there are four radio buttons: 'Create Basic Rule' (selected), 'Create MSI Rule', 'Rule Set', and 'Use Existing Rule'. Below these is a 'Rule Type' dropdown menu set to 'Windows Version' and a 'Not Rule' checkbox. The 'Windows Version' tab is active, showing a 'Comparison' dropdown set to 'Greater Than or Equal To'. Below this are five input fields: 'Major Version' (6), 'Minor Version' (1), 'SP Major Version' (0), 'SP Minor Version' (0), and 'Build Number' (empty). At the bottom is a 'Product Type' dropdown set to 'Server'.

3. Click OK to save this rule, and click Next.
 4. On the Select Package window, select the Package Type as a Microsoft Installer File (.msi), and then select I already have the content for the package locally on my network.
 5. Click the browse icon and locate the MSI file for the SolarWinds Orion agent. The Download URL field will automatically populate.
 6. The GUID product code is extracted from the MSI file and displayed for review. Copy the GUID product code that you will use later.
-  The GUID is detected from the installer. Use the one displayed in your environment.
7. Select Includes additional files with the package, and click the button to the right to open the Package Content Editor.
 8. In the Package Content Editor, click Add Files, and browse to the MST File for the SolarWinds Orion agent.
 9. Click OK to close the Package Content Editor. To confirm that you want to add these files to the cache, click Yes.
 10. Select None for the Binary Language.

11. In the Command Line field, enter: TRANSFORMS= (MST FILE NAME)

Example: TRANSFORMS=SolarWinds_Agent_1.5.0.951.mst

Package

Type: Windows Installer File (.msi)

Details: {E59C88B...}

☐ I do not have the package content (e.g. the MSI, MSP, or EXE locally on my network)

Download URL:

☒ I already have the content for the package locally on my network

Package: C:\Staging\Tools\OrionAgent\SolarWinds_Agent_1.0.0.866.msi

Download URL: file://C:\Staging\Tools\OrionAgent\SolarWinds_Agent_1.0.0.866.msi

☐ Use the Package Boot Helper program when performing installation of the software

☒ Includes additional files with the package

Additional Files: 1 files are included with this package.

Settings

Binary Language: None

Success Return Codes: 0, 1234, 1235, 1236, 1237, 1238, 1239, 1240, 1241, 1242, 1243, 1244, 124
For example: 0, 1, 2, 1029, 3023

Success Pending Reboot Codes: 3010
For example: 1, 3, 128, 3010

Command Line (silent install): TRANSFORMS=SolarWinds_Agent_1.0.0.866.mst
For example: /quiet /norestart NOTE: A MSI or MSP package already has the required arguments for a silent install (/qn) with no reboot (/norestart) and is not required

Advanced

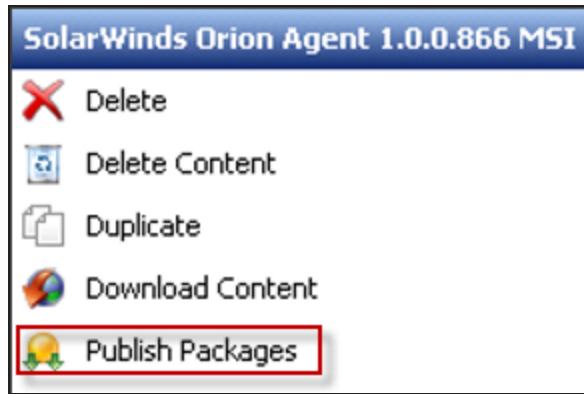
12. Click Next.
13. On the Applicability Rules window, click Add Rule > Create MSI Rule.
14. Select Rule Type: Product Installed, and select Not Rule.
15. Enter the product code without the brackets, and leave all other fields empty.
16. On the Installed Rules window, click OK to save the rule, and then click Next.
17. Click Add Rule > Basic Rule.
18. For the Rule Type, select File Version with Registry Value. Enter the following values:
- Registry Key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SolarWinds\Agent
 - Registry Value: InstallDir
 - Comparison: Equal To.
 - Version: Version number of the agent
19. Click OK to save the rule, and click Next. Review the Summary Page, and enter notes at the bottom.
20. Click Next to save, and click OK.

When the file packaging and uploading completes, a Package Saved dialog displays.

Publish the package

1. In the SolarWinds, Inc. Packages view in Patch Manager, select the SolarWinds Orion Agent package that you created.

2. In the SolarWinds Orion Agent action pane, click Publish Packages.



3. Accept the default selections, or choose a specific Windows Server Update Services (WSUS) server for publication, and then click Next.
4. You are notified when the package publishes.
5. Click Finish to close the Publishing Wizard.


The package for the SolarWinds Orion agent is packaged and published to your WSUS server.

Deploy on Windows Core Servers

If you are installing the agent on a Windows Core Server, you must install the .NET Framework 4.5. Also install the latest Windows service pack and critical updates.

Prerequisites to installing an agent on Windows Core

- Start WoW64.
- Start the .NET 2.0 layer.
- Start the .NET 2.0 layer for WoW64.
- Download and install the .NET framework from www.microsoft.com.

 By default, no web browser is installed with Windows Core. Consider transferring the necessary files with FTP or a flash drive.

After the .NET Framework is installed, you may need to reboot the host server. The agent can then be deployed to the host server and operate normally.

Deploy Windows agents in the cloud

Agents can be deployed in the cloud for use with Amazon Web Services, Microsoft Azure, and other third-party cloud infrastructure services.

Manually deploy a Windows agent on Amazon Web Services

You can manually deploy agents to a virtual machine using Remote Desktop Connection.

Requirements for manual agent deployment

- Agent-initiated communication: The poller must have a public IP address which is visible from the node with the agent installed. Port 17778 must be open on the poller.
- Server-initiated communication: The node with the agent installed must have a public IP address. Port 17790 must be open.

You can manually deploy the agent in one of two ways:

Install through the command prompt

1. Click Settings > All Settings in the menu bar.
2. Under Product Specific Settings, click Agent Settings > Download Agent Software.
3. Click Mass Deploy to Multiple Machines, and click Next.
4. Download the MSI and MST files.
5. Run a command prompt as administrator from the context menu.
6. Enter the following command:

```
msiexec /i "SolarWinds-Agent.msi" TRANSFORMS="SolarWinds-Agent.mst"
```

Deploy the agent manually using the interactive wizard

Follow the instructions in [Deploy the Windows agent manually](#).

Automatically deploy a Windows agent on Amazon Web Services

1. Click Settings > All Settings in the menu bar.
2. Under Product Specific Settings, click Agent Settings > Download Agent Software.
3. Click Mass Deploy to Multiple Machines, and click Next.
4. Download the MSI and MST files.
5. Log in to your Amazon Web Services S3 account.
6. Create a bucket and upload the MSI and MST files.
7. Create a PowerShell script to use on each virtual machine where you want to install the agent. This script will run on each virtual machine when it is launched for the first time, downloading and executing the agent.
8. Log in to your Amazon Web Services account.



You can perform the following steps through the API or AWS command line interface.

9. Create an instance, and paste your PowerShell script under Advanced Details in the User Data text box. Select the As Text option.
10. For instances that are already created, take the following steps:
 - a. Stop the instance where you want to deploy the agent
 - b. Right-click the instance and click Instance Settings > View/Change User Data.
 - c. Paste your PowerShell script in the text box as Plain Text.

Automatically deploy a Windows agent on Microsoft Azure

1. Click Settings > All Settings in the menu bar.
2. Under Product Specific Settings, click Agent Settings > Download Agent Software.
3. Click Mass Deploy to Multiple Machines, and click Next.
4. Download the MSI and MST files.
5. Upload the MSI and MST files to your Azure Blob Storage.
6. Create a PowerShell script to use on each virtual machine where you want to install the agent. This script will run on each virtual machine when it is launched for the first time, downloading and executing the agent.
7. Add your PowerShell script to virtual machines manually on the last step of the Create a Virtual Machine wizard in the Azure management portal.

CREATE A VIRTUAL MACHINE

Virtual machine configuration

VM AGENT

☒ Install the VM Agent

CONFIGURATION EXTENSIONS

☐ Puppet Enterprise Agent
Published by: Puppet Labs | [Learn more](#) | [Legal terms](#)

☐ Chef
Published by: Chef Software, Inc. | [Learn more](#) | [Legal terms](#)

☒ Custom Script
Published by: Microsoft

CUSTOM SCRIPT CONFIGURATION

SCRIPT

InstallAgent.ps1

ARGUMENTS

SECURITY EXTENSIONS

☐ Microsoft Antimalware
Published by: Microsoft | [Learn more](#) | [Legal terms](#)

Windows Server 2012 R2 Datacenter

At the heart of the Microsoft Cloud OS vision, Windows Server 2012 R2 brings Microsoft's experience delivering global-scale cloud services into your infrastructure. It offers enterprise-class performance, flexibility for your applications and excellent economics for your datacenter and hybrid cloud environment. This image includes Windows Server 2012 R2 Update.

OS FAMILY
Windows

PUBLISHER
Microsoft Windows Server Group

NUMBER OF DISKS
1

PRICING INFORMATION
Pricing varies based on the subscription you select to provision your virtual machine.

1 2 3

This step can also be accomplished via the API or AWS command line interface.

Certificates and the agent

The Verisign Root Certificate Authority (CA) must be current. This is required because the agent software is signed using a Verisign certificate. If your certificate is not current, you must download the Root CA certificate and install it to the Local Computer\Trusted Root Certification Authority store on the server hosting the agent.















For more information, search for "Add the Certificates Snap-in to an MMC" at technet.microsoft.com.


Agent management


Check agent connection and deployment status on the Manage Agents page.

1. Click Settings > All Settings in the menu bar.
2. Under Node & Group Management, click Manage Agents.

Manage Agents toolbar options

 ADD AGENT	 EDIT SETTINGS	 DELETE	 CHOOSE RESOURCES	 MANAGE AS NODE	 MORE ACTIONS	Search all agents ... 
Agent/Node		Agent Status	Connection Status	Registered On		
		New  Agent is running	 Connected	5/10/2016, 1:37:38 PM		
	QA-BRN-SAM-03	New  Agent is running	 Connected	5/9/2016, 11:32:16 PM		

BUTTON	DESCRIPTION
Add Agent	Go to the Add Agent page, where you can deploy the agent on a network, or connect to a previously installed agent.
Edit Settings	Go to the Edit Agent Settings page, where you can adjust the agent name and automatic updating.
Delete	Remotely uninstall the agent.
Choose Resources	<p>Displays a list of resources and statistics to monitor. This is only available for agents that are deployed on nodes.</p> <ul style="list-style-type: none">■ For a Single Agent: Go to the List Resources page to choose items on the node you want to monitor.■ For Multiple Agents: From here, Orion discovers available resources on the agents you have selected using Network Sonar Discovery. You can choose items on the nodes to monitor.
Manage as Node	Manage the agent as a new node by navigating to the Add Node page with pre-configured agent details.
More Actions	<ul style="list-style-type: none">■ View installed agent plug-ins: Displays a dialog detailing the node the agent is deployed on, the agent status, connection status, plug-in status, and plug-in version.■ View installed plug-ins report: Generates a report detailing node status, agent DNS name, automatic update enabled, connection status, agent status, agent version, plug-in, plug-in status, and plug-in version.■ Retry agent installation: Attempts to install the agent in the event of a file transfer timeout due to network connectivity issues.■ Reboot Agent Machine: Reboots the server that hosts the selected agent. <div> This button is disabled by default. It is enabled when the installation of an agent requires a system reboot.</div>

BUTTON	DESCRIPTION
	<ul style="list-style-type: none"> ■ Update: Updates the agent software to the latest version available. <div>  This button is disabled by default. It becomes enabled when: <ul style="list-style-type: none"> ■ Automatic updates for the agent is disabled. ■ The selected agent requires an update. </div> <ul style="list-style-type: none"> ■ Reconnect to passive agent: The server tries to re-establish the connection to the passive agent when the connection is lost and automatic reconnection fails. This can also be used for connecting to an agent that was deleted but not uninstalled.

Manage Agents table columns

The table on the Manage Agents page displays information on the status and connection of your agents.

COLUMN HEADER	DESCRIPTION
Agent/Node	Name or IP address of the listed node.
Agent Status	<p>Current status of the listed agent.</p> <p>Agent Status can be as follows:</p> <ul style="list-style-type: none"> ■ Connected/OK: Everything is working. ■ Unknown: The agent is connected but no communication is received. ■ Update Available: The agent version is older than the version on the server and should be updated. ■ Update in Progress: The agent is currently being updated. ■ Reboot Required: The agent needs to be rebooted in order to finish the installation of plug-ins. ■ Reboot in Progress: The agent is currently being rebooted. Once reboot is complete, the agent should finish installation of plugins. ■ Reboot Failed: The agent cannot be rebooted. It may be temporarily offline or there may be some other issue. ■ Plugin Update Pending: A plugin on the agent has an older version than the one that is on the server and should be updated.
Connection Status	<p>Current connection status of the listed agent.</p> <p>Connection status can be as follows:</p> <ul style="list-style-type: none"> ■ Connected/OK: The agent is connected. ■ Unknown: The agent management service is not running. ■ Service not Responding: The agent management service is running, but the agent is not connected. ■ Deployment Pending: An agent deployment is going to start, but has not started.

COLUMN HEADER	DESCRIPTION
	<ul style="list-style-type: none"> ■ Deployment in Progress: The agent is being deployed to the target node. ■ Deployment Failed: Agent deployment failed. ■ Invalid Response: The status displayed if the agent responds in an unexpected manner. ■ Waiting for Connection: The agent was approved, but has yet to connect to the Orion server.
Registered On	Date when the agent was added to the agent management system.
Mode	Agent communication type: <ul style="list-style-type: none"> ■ Agent-initiated: The agent initiates the connection to the agent management system. ■ Server-initiated: The agent listens on its designated port for connections from the Orion server.
Version	Version of the agent software. This is helpful in determining which agents should be updated.

Edit agent settings

Editing the configuration of an agent may be necessary if you experience problems and want to collect diagnostics.

1. Click Settings > All Settings in the menu bar.
2. Under Node & Group Management, click Manage Agents.
3. Select an agent, and click Edit Settings.

Agent settings and troubleshooting options

- Agent Name: change the display name displayed in Orion.
- Communication type: choose whether the agent uses [server-initiated](#) or [agent-initiated](#) communication.
- Allow automatic agent updates: choose whether the Orion server can update the agent software to the latest version available.
- Troubleshooting:
 - Log level: the amount of detail saved to the log.
 - Diagnostics: click Collect new diagnostics, and then Download to save to your local disk. Send the zip file to our support team if requested.

Track your polling method

If nodes are using different polling methods, you may want to keep track of the polling method of each node to troubleshoot issues more easily. There are several methods you can use to identify the polling method of nodes:

STATUS	MEANING
The plug-in is installed	The plug-in is installed, working correctly, and communicating with no problems.
Installation Pending	The plug-in is waiting to be deployed. It may be waiting for the computer it is installed on to reboot, or because some other process on the remote host has interrupted the installation process.
Unknown	The status is unknown due to networking interruptions, communication problems with the agent, or because the plug-in is no longer installed.
Error	The plug-in may have installed incorrectly or failed to load.
In Progress	The plug-in is either being installed or uninstalled.


If you think a plug-in should be available and cannot find it in the list, you may need to check your purchased products or manually update your agent. New plug-ins and updates to existing plug-ins are installed when an agent is updated. It may take a few minutes before the status changes.

Orion deploys and removes plug-ins as needed when you enable and disable features. It is normal for agents to have different plug-ins.

Edit agent settings in the Windows Control Panel

If the agent loses connectivity to the SolarWinds Orion server, or is unable to connect after being manually installed, you can configure its settings in the Windows Control Panel. This enables the agent to reconnect to the SolarWinds Orion server.

1. Open Orion Agent Settings in the Control Panel.
2. Select the Agent Communication Mode.
3. Edit the Connection Settings.

 The Agent Shared Secret is provided for security. When you install the agent, you must set a shared secret. When the SolarWinds Orion server connects to the agent, it verifies the secret to connect.

4. Click OK to save your changes.


Connect to a previously installed agent

You can connect to agents that you installed previously or modify the assigned polling engine of the agent. The steps are different depending on the agent communication mode. You should [confirm the agent communication mode](#) before connecting.

Connect to an agent using agent-initiated communication

1. Click Settings > All Settings in the menu bar.
2. Under Node & Group Management, click Manage Agents.
3. Click Add Agent.
4. Click Connect to a previously installed agent, and click Next.

5. Enter the name of the agent you want to connect to, and select Agent-initiated communication.
6. Select the agent from the Agent list.
7. Expand Advanced to change the proxy.
8. Select Allow automatic agent updates.


 Disabling this option requires you to upgrade agents manually after upgrading your SolarWinds products and modules.

9. Click Submit.

When the connection is successful, the agent displays in the agent list on the Manage Agents page.

Connect to an agent using server-initiated communication

1. Click Settings > All Settings in the menu bar.
2. Under Node & Group Management, click Manage Agents.
3. Click Add Agent.
4. Click Connect to a previously installed agent, and click Next.
5. Enter the name of the agent you want to connect to, and select Server-initiated communication.
6. Enter the IP address or hostname where the agent is installed.
7. Expand Advanced to change the port number, assign the agent to a different poller, or use a proxy to connect to the agent.
8. Select Allow automatic agent updates.

 Disabling this option requires you to upgrade agents manually after upgrading your SolarWinds products and modules.

9. Click Submit.

When the connection is successful, the agent displays in the agent list on the Manage Agents page.

Change the agent communication mode

You can change how the agent communicates with the Orion server. You can select server-initiated or agent-initiated communication.

1. Log in to the host where the agent is installed.
2. Start the Orion Agent Settings application in the Control Panel.
3. Select an agent communication mode.
 - **Agent-initiated communication:** The agent initiates communication with the Orion server on port 17778. This port must be open on the Orion server firewall so the agent can connect. No change to the agent firewall is required.
 - **Server-initiated communication:** The agent waits for requests from the server on a specified port. This port must be open on the firewall of the agent computer so the Orion server can connect. No change to the Orion server firewall is required.
4. Click OK.

Change the agent port

1. On the computer with the deployed agent, edit the following configuration file using a text editor:

```
C:\Program Files (x86)
\SolarWinds\Orion\AgentManagement\SolarWinds.AgentManagement.ServiceCore.dll.config
```
2. Change the port number on the following line:

```
<agentManagementServiceConfiguration messagingPort="17778" />
```
3. Save the file.
4. Restart the SolarWinds Orion Module Engine service.



- If you installed the agent manually, you can change the port number during installation through the wizard in the web console.
- If you deployed the agent from the server, the port number is set automatically.
- If you used the MST file for mass deployment, you must download a new MST file from the server after you change the port number.

Change the port on deployed agents

1. Log in to the computer with the deployed agent.
2. Open Orion Agent Settings in the Control Panel.
3. Enter a new port number, and click OK.

Agent polling method

When the Agent Polling Method is selected, an agent is deployed to the node and installed using the credential you selected. After the agent is installed, it operates under a local account.

Check nodes polling with agents for changes

Agent discovery has an option to keep nodes that use agents updated. Select this option so the Orion server can find new volumes, interfaces, and other objects on nodes that are polled by an agent.

While normal discovery finds new nodes and adds them to the SolarWinds Orion server, this is not true for nodes using the agent. Agent discovery is an extension to the standard discovery process.

A discovery profile may contain:

- Nodes using both the agent and non-agent nodes
- Non-agent nodes
- Agent nodes

Agent performance counters

SolarWinds: Agent Service

NAME	DESCRIPTION
Messages Sent	The number of messages sent to the Agent Management Service.
Messages Received	The number of messages received from the Agent Management Service.
Exchange Received	The number of times the Exchange Receive method was called.
Exchange Sent	The number of times the Exchange Send method was called.


SolarWinds: Agent Management Service

NAME	DESCRIPTION
Messages Sent to Agent Count	The number of messages sent to the agent.
Messages Received From Agent Count	The number of messages received from the agent.
Incoming Timed Out Messages Count	The number of incoming messages that timed out before being processed by the recipient.
Outgoing Timed Out Messages Count	The number of outgoing messages that timed out before they were sent to the target agent.
Incoming Failed Messages Count	The number of incoming messages that failed to process.
Outgoing Failed Messages Count	The number of outgoing messages that failed to process.
Total Agents Fully Connected	The number of total agents fully connected.
Active Agents Fully Connected	The number of active agents fully connected.
Passive Agents Fully Connected	The number of passive agents fully connected.
Passive Agents Disconnected	The number of passive agents disconnected.
Total Agents Connected to Messaging Hub	The number of agents connected to the messaging hub.
Total Agents Connected to Files	The number of agents connected to the files hub.

NAME	DESCRIPTION
Hub	
Messages Processed per Second	The number of messages processed per second.
Incoming Messages Processed per Second	The number of incoming messages processed per second.
Outgoing Messages Processed per Second	The number of outgoing messages processed per second.
Incoming Processing Queue Size	The number of messages waiting in the incoming processing queue.
Outgoing Processing Queue Size	The number of messages waiting in the outgoing processing queue.
Incoming Persistence Queue Size	The number of messages waiting in the incoming persistence queue.
Outgoing Persistence Queue Size	The number of messages waiting in the outgoing persistence queue.
Incoming SignalR Messages	The number of messages received from SignalR.
Outgoing SignalR Messages	The number of messages passed to SignalR to send.
Incoming Exchange Queue Size	The number of messages in the incoming queue with Exchange items.

Monitor Syslog messages

Syslog messages are received by the SolarWinds Syslog Service, which listens for incoming messages on UDP port 514. Received messages are decoded and stored in the SolarWinds Orion database. The SolarWinds Syslog Service can handle large numbers of simultaneously incoming Syslog messages from all your monitored devices.


 A SolarWinds installation can process approximately 1 million Syslog messages per hour, which is about 300 Syslog messages per second. You can process more by increasing your hardware requirements over the minimum requirements.

You can view Syslog messages in the Orion Web Console or in the Syslog Viewer application.

Before you begin


- Confirm that your network devices are configured to send Syslog messages to the SolarWinds Orion server IP address. For proper configuration of network devices, refer to the documentation supplied by the device vendor.

- Ensure `UDP port 514` is open for IPv4 and IPv6.
- The message must be formatted according to the Request for Comments (RFC) requirements.
- If a long message is split into smaller parts, these parts should be formatted to not be skipped.

 SolarWinds recommends setting up Enable RFC Relay in the service to `true` to allow the service to restructure the message by adding the default facility, severity, or date.

Configure the SolarWinds Orion server to use the correct syslog port

By default, SolarWinds Syslog Service listens for syslog messages on port 514 (UDP). If your devices use a different port for sending syslog messages, consider reconfiguring the port on devices, or change the port on which the service listens.

 Running the Configuration Wizard will revert all changes made to the `SyslogService.exe.config` file.

If you run the Configuration Wizard, you must repeat this procedure to restore the port setting.

1. Log in to the Orion Web Console as an administrator.
2. Go to Advanced Configuration settings. Copy `/Admin/AdvancedConfiguration/Global.aspx`, and paste it into your browser address bar, after `/Orion`.

The address in the address bar should look as follows:

`<your product server>/Orion/Admin/AdvancedConfiguration/Global.aspx`

3. On the Global tab, scroll down to `SyslogService.SyslogSettings`, and enter the UDP port number in the `UDPListenPort` entry.
4. Click Save.


Syslog message priorities

At the beginning of each Syslog message, there is a priority value. The priority value is calculated using the following formula:

`Priority = Facility * 8 + 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.

 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

NUMBER	SOURCE	NUMBER	SOURCE
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)
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.


NUMBER	SEVERITY	SUGGESTED ACTIONS
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.

View Syslog messages in the Orion Web Console

The Orion Web Console provides both syslog-specific resources and a syslog view with a table of syslog messages received by your SolarWinds Orion server.

The Syslog view displays a list of all the syslog messages generated by monitored network devices. The messages are listed by time of transmission, with the most recent at the top of the list.

1. Log in to the Orion Web Console, and click Alerts & Activity > Syslogs in the menu bar.
2. To filter syslog messages so that only messages relevant for specific devices are displayed:
 - To view messages for a specific syslog-enabled network object, select it in the Network Object list.

 Only objects that have sent a syslog message to the Orion server will be listed in this field.

- To view messages for a specific device, provide the IP address in the IP Address field.
 - To view messages for a specific device type, select it in the Type of Device list.
 - To view messages for a specific vendor, select the vendor in the Vendors list.
3. To select which syslog messages should be displayed:
 - To view only messages with a severity, select the [severity](#).
 - To view messages for a facility, select the [facility](#).
 - To view messages of a type, type the string into the Message Type field.
 - To view only messages containing a pattern, provide the string in the Message Pattern field.



You can use the following wildcards:

Asterisk (*)

Use * before or after the pattern string if the provided pattern is not the beginning, the end or the full message.

Underscore (_)

Use _ as a placeholder for one character.

- To view syslog messages from a specific period of time, select either a period of time or enter custom Beginning and Ending Date/Times.
 - Type the number of syslog messages you want to view into Number of Displayed Messages.
 - To view cleared and acknowledged syslog messages, select Show Cleared Messages.
4. Click Refresh to update the syslog messages list with your settings.

Syslog messages matching the selected criteria display in a list beneath the search area.


Click Hide or Show in the top-right corner of the view to remove or restore the Syslog messages search criteria area.

Click the Hostname or Message to open the Device Details view for the device.


Define the number of messages displayed, message retention, and the displayed columns in the Syslog Viewer

 You must be able to log in to the computer running your SolarWinds Orion server.


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. Automatically refresh the current messages view by selecting the option, and setting 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.

 This setting significantly affects the database size and performance.

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.

 Clearing Syslog messages is easier if you add the Acknowledged column to your view.

9. To wrap Syslog message text in the Current Messages view, select Word Wrap Long Messages.
10. If you do not expect to use the Syslog Viewer as your primary viewer for Syslog messages, select the Message Parsing tab, and select what should be removed:
 - Remove embedded Date/Time from Syslog Messages
 - Remove Message Type from Syslog Messages
 - Remove Domain Name from DNS Lookups.

 Removing the added data from each record helps you reduce the size of your SolarWinds Orion database.


Clear Syslog messages in the Orion Web Console

1. Log in to the Orion Web Console.
2. Click Alerts & Activity > Syslogs in the menu bar.
3. [Define what you want to see](#) in the Syslog messages table, and click Refresh.
4. Select the messages you want to acknowledge, and click Clear Selected Messages.

The messages are cleared. You can see cleared messages when you select the Show Cleared Messages box.

View and clear Syslog messages in the Syslog Viewer

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. Clear messages you have already read and acted upon.

 You must be able to log in to the computer running your SolarWinds Orion server.


1. Click Start > All Programs > SolarWinds Orion > Syslog and SNMP Traps > Syslog Viewer.
2. Click View > Current Messages.
3. Clear read messages:
 - Right-click any message, and select Acknowledge Selected.
 - Add an Acknowledged column to the Syslog Viewer, and [select the messages that you want to acknowledge](#).

Selected messages are acknowledged now.


Search for Syslog messages in the Syslog Viewer

In the Syslog Viewer, you can search through collected Syslog messages and format search results.

1. Click View > Search Messages.
2. Enter the search criteria.
3. Click Search Database.
4. To group messages for easier navigation, select the type of grouping from the Grouping list.

 You can acknowledge messages both in the search results and in the Current Messages view. See [Define the number of messages displayed, message retention, and the displayed columns in the Syslog Viewer](#).

5. To limit the number of displayed message, enter or select a number in the Maximum Number of Messages to Display field.
6. To view messages that meet your search criteria as they arrive, select a number for the Auto Refresh Every number of seconds field.

 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.

Trigger alerts when receiving specific Syslog messages

 You must be able to log in to the computer running your SolarWinds Orion server.


1. Click Start > All Programs > SolarWinds Orion > Syslog and SNMP Traps > Syslog Viewer.
2. Click File > Settings.
3. Click Alerts/Filter Rules.
4. Click Add New Rule to create a rule, or edit a selected rule.

5. On the General tab, complete the following steps:
 - a. Provide or edit the Rule Name.
 - b. Select Enabled.
 - c. Select the servers from the Apply this Rule To list.
 - d. Enter the IP addresses or subnets to which this rule applies in the Source IP Addresses area.

 Syslog rules may not be applied to nodes in an unmanaged state.

6. To limit the rule only to messages from specific hosts, domains, or host name patterns, click the DNS Hostname tab, and enter a DNS Hostname Pattern.


 The DNS Hostname Pattern rule is case-sensitive.

 To use regular expressions, select Use Regular Expressions in this Rule.


7. To limit the rule only to specific message types or texts within a Syslog message, go to the Message tab, and enter rules for Message Type Pattern and Syslog Message Pattern.
8. To apply specific severity or facility types, go to the Severity / Facility tab, and select the severity and facility types.

By default, all [message severities and facilities](#) are selected.
9. To apply the rule only during a specific period of time, select the Time of Day tab, select Enable Time of Day Checking, enter the time period, and select the days of the week on which to apply the rule.


Messages received outside the specified time frame will not trigger alerts.

 Enabling Time of Day checking creates more overhead for the CPU.

10. 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, and select Define a Trigger Threshold for this Rule.
 - b. Enter option values.

 When Suspend Further Alert Actions For is selected, alert actions are not sent until the specified amount of time has expired. When the time period expires, only new alerts are sent. All alerts suppressed during the time period are discarded.

11. Configure Syslog alert actions on the Alert Actions tab:
 - a. To create an action for the rule, click Add New Action.
 - b. To edit an action for the rule, select the action, and click Edit Selected Action.
 - c. Configure the action.

 Syslog alerts use a unique set of variables.


- d. To delete an action, select the action, and click Delete Action.
 - e. Use the arrow buttons to set the order in which actions are performed.

Actions are processed in the order listed, from top to bottom.
 - f. Click OK to save all changes and return to Syslog Viewer Settings.
12. Use the arrow buttons to arrange the order in which the rules are applied.


Rules are processed in the order they appear, from top to bottom.

Forward syslog messages

The Syslog message forwarding action allows you to forward received syslog messages. Additionally, if you have WinPCap version 3.0 or later installed on your SolarWinds Orion server, you can forward syslog messages as spoofed network packets.

 The following procedure assumes you are editing a Forward the Syslog Message alert action. For more information, see [Trigger alerts when receiving specific Syslog messages](#).

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.

 The default is UDP port 514.

3. Specify what IP address should be used for the source device in the syslog message. By default, the device IP is replaced by the SolarWinds Orion server IP address.
 - a. To designate a specific IP address or hostname as the Syslog source, select Retain the Original Source Address of the Message, select Use a Fixed Source IP Address, and provide the IP address or hostname.
 - b. To keep the original IP address of the syslog source device, select Retain the Original Source Address of the Message, select Spoof Network Packet, and select the Network Adapter.
4. Click OK to complete the configuration.

You have defined the destination, port for sending the syslog message, and the source IP of the device in the syslog message used in the alert action.


Monitor SNMP traps

If you monitor a large number of devices, where each device may have many connected objects of its own, requesting information from each device is impractical. You can set up the SNMP Trap Server, and each managed device can notify it about any issues by sending a trap message.

You can monitor SNMP traps with SolarWinds NPM or SolarWinds SAM.

SNMP traps are received by the SolarWinds Trap Service, which listens for incoming trap messages on UDP port 162, and then decodes, displays, and stores the messages in the SolarWinds Orion database.

The SolarWinds Trap Service can receive and process SNMP traps from any type of monitored network device, and can handle large numbers of simultaneously incoming traps.

 A SolarWinds installation can process approximately 500 traps per second. Higher capacity can only be achieved with significant hardware improvements over minimum SolarWinds requirements.

You can view SNMP traps either in the Orion Web Console or in the Trap Viewer application. The Trap Viewer application allows you to configure trap-specific alerts, to view, filter, and search for traps.

Before you begin


- Configure devices to send SNMP traps to the IP address assigned to the Orion server. For more information about proper configuration, refer to the documentation supplied by the vendor of your devices.
- Make sure the `UDP port 162` is open for IPv4 and IPv6.
- When you use SNMPv3 for polling a device and receiving traps from it, confirm that the same authentication type (auth, noauth, or priv) is configured for both polling and traps.

View SNMP traps in the Orion Web Console

1. Log in the Orion Web Console.
2. Click Alerts & Activity > Traps in the menu bar.
3. To display only traps relevant for a specific device, specify the device:
 - To display only traps for a device, select the device in the Network Object field.
 - To view traps for certain device type, select the device type in the Type of Device field.
4. Define what traps you want to view:
 - To view only traps of a designated type, select the type in the Trap Type field.
 - To view only traps originating from a specific IP address, type the IP Address in the Source IP Address field.
 - To view only traps with a designated community string, select the string in the Community String field.
 - To view only traps from a specific period of time, select the time period from the Time Period menu.
5. Confirm the number of traps displayed in the Number of Displayed Traps field.
6. Click Refresh to update the Traps view with your new settings.

View current traps in the Trap Viewer

The Trap Viewer is an application which allows you to view, [search for traps](#), or [configure filters and alerts](#).


 You must be able to log in to the computer running your SolarWinds Orion server.

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.

The current traps are now displayed according to your settings.

Define how many traps to display, if you want to refresh the traps view, trap retention, and the information displayed in 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 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 to Automatically Refresh the Current Traps View, select the option, and 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 in your trap messages, select Remove Domain Name from DNS Lookups on the Message Parsing tab.

 Selecting this option can slightly reduce the size of your database.

Search for traps in the Trap Viewer

You can search collected trap messages and format the search results list in the Trap Viewer.

1. Click Start > All Programs > SolarWinds Orion > Syslog and SNMP Traps > Trap Viewer.
2. Click View > Search Traps.
3. Enter search criteria, and click Search Database.
4. To group messages for easier navigation, select the type of grouping from the Grouping list.
5. To limit the number of displayed messages, enter or select a number in the Maximum number of messages to display field.
6. To view messages that meet your search criteria as they arrive, select a number for the Auto Refresh Every number seconds field.

 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. 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.

You can now see the traps according to your settings.

Configure Trap Viewer filters and alerts


In the Trap Viewer, you can filter trap messages, and configure actions that trigger when received trap messages match defined rules.


 With the exception of the asterisk (*) and underscore (_) wildcards, SolarWinds recommends against


 using non-alphanumeric characters in filter definitions.


Trap rules are not applied to unmanaged nodes.


1. Click Start > All Programs > SolarWinds Orion > Syslog and SNMP Traps > Trap Viewer.
2. Click File > Settings, and click the Alerts / Filter Rules tab.
3. Click Add Rule or click Edit Rule.
4. Click the General tab, and select Enabled.
5. Select the servers from the Apply This Rule To list.
6. Apply the rule to specific messages.
 - Click DNS Hostname, and enter a DNS Hostname Pattern to apply the rule to messages from specific hosts, domains, or hostname patterns.

 The DNS Hostname Pattern rule is case-sensitive.
 - Click Trap Details, and enter a Trap Details Pattern to apply the rule based on the Trap Details field.
 - Click Community String, and enter the patterns in the Community String Pattern field to apply the rule to specific community strings.
7. Click Conditions to define the what triggers the rule.
 - Select object identifiers and comparison functions from the linked context menus.
 - Click Browse (...) to insert conditions.
8. Click Time of Day > Enable Time of Day Checking to apply the rule during a specific period of time. Messages received outside the specified time frame will not trigger alerts.

 Enabling Time of Day checking creates more overhead for the CPU.
9. Click Trigger Threshold > Define a Trigger Threshold for this Rule to suppress alert actions until a specified number of traps arrive that match the rule.

 When Suspend Further Alert Actions For is selected, alert actions are not sent until the specified amount of time has expired. When the time period expires, only new alerts are sent. All alerts that are suppressed during the time period will never be sent.
10. Click Alert Actions.
 - Associate the rule with a new action by clicking Add New Action, and then selecting an action from the list to configure.
 - Edit an existing action for the rule.
11. Use the arrow buttons to set the order in which actions are performed.

 Actions are processed in the order they appear, from top to bottom.
12. Click OK to save all changes and return to Trap Viewer Settings.
13. Use the arrow buttons to arrange the order in which the rules are applied.

 Rules are processed in the order they appear, from top to bottom.

Trap messages are now filtered by the rules and alert actions are triggered when the rule conditions are met.

What is a Trap Template?

Trap templates are used to format your trap messages. You can use SolarWinds macros or variables in the OID Value and ValueName attributes or call values from your MIB.

The templates are placed in the following locations:

- /SolarWinds/Common/Orion-Detailed-Alert.trap
- /SolarWinds/Common/Orion-Generic-Alert.trap
- /SolarWinds/Orion/ForwardSyslog.trap

The following table describes the OIDs section of the Orion Generic Alert trap template. This is the section you modify to display the information you want in your trap messages.

TEMPLATE OID LINE	INFORMATION RETURNED
OID OID="1.3.6.1.2.1.1.3.0" MIB="RFC1213-MIB" Name="sysUpTime.0" Value="0" DataType="67" ValueName="0" HexValue=""	This line displays how long the device has been up.
OID OID="1.3.6.1.6.3.1.1.4.3.0" MIB="SNMPv2-MIB" Name="snmpTrapEnterprise.0" Value="1.3.6.1.4.1.11307" DataType="6" ValueName="enterprises.11307" HexValue=""	This line displays the enterprise associated with the trap.
OID OID="1.3.6.1.4.1.11307.10.1" MIB="SNMPv2-SMI" Name="enterprises.11307.10.1" Value="\${AlertMessage}" DataType="4" ValueName="\${AlertMessage}" HexValue=""	When the template is used in an alert, this line displays the alert message associated with the triggered alert.


Add more information by adding another OID element and incrementing the OID.

Monitor capacity usage trends on the network and forecast capacity issues

Capacity forecasting is available for the following metrics of nodes, interfaces, and volumes monitored by SolarWinds NPM:

- CPU utilization on nodes
- Memory usage on nodes
- Space usage on volumes
- Receive (in) utilization on interfaces
- Transmit (out) utilization on interfaces

Capacity usage trends are calculated based on historical data. By default, the longest time period taken into account for calculating the capacity forecast is 180 days.

 The more historical data up to 180 days are available, the more precise is the calculated forecast.

Forecast calculation methods

- **Peak calculation** forecasts trends using daily maximum values. This method is suitable for important devices and connections where it is important to completely avoid reaching a certain usage level (threshold).
- **Average calculation** forecasts trends using daily average values. This method is suitable for non-critical network devices or connections where short periods exceeding the threshold level are acceptable.



By default, the forecast calculation method is set globally for all monitored objects. You can also customize the method for individual objects (nodes, interfaces, or volumes).

Requirements

Capacity forecasting is available for nodes, interfaces, and volumes that meet the following requirements:

- The nodes, interfaces, and volumes must be managed in SolarWinds NPM.
- You need to have enough historical data in the database. By default, 7 days of data are required.

Forecast capacity for nodes, interfaces, or volumes

Consult graphs or tables to see usage trends of devices on your network, and find out when the capacity of the devices will be fully used.

Locate pending capacity problems

Consult the Top XX Capacity Problems resource to see a list of objects whose usage trend is rising.

If the resource is not in a view, [add it](#).

View capacity usage trends and forecast in graphs

To see a graphical display of capacity usage trends, go to the details view for the node, volume, or interface, and consult the forecast chart:

- CPU Capacity Forecast Chart
- Memory Capacity Forecast Chart
- Storage Capacity Forecast Chart
- Interface Utilization Receive Forecast Chart
- Interface Utilization Transmit Forecast Chart

View capacity usage trends and forecast in tables

For a brief overview of usage trends for a node, volume, or interface, go to the details view for the object, and consult the resource:

- Node Capacity provides an overview of both CPU load and percent memory usage in the past 6 months, a forecast when the warning and critical thresholds will be exceeded, and when the resource will be fully used.

- Volume Capacity provides an overview of volumes capacity usage in the past 6 months, a forecast when the warning and critical thresholds will be exceeded, and when the volume capacity will be fully used.

Forecasts in this resource are calculated using the default method (peak or average) specified for the resource.

Add capacity forecasting resources

Capacity forecasting resources display only on views for which they are relevant. For example, interface utilization resources can only be added on interface detail views.

1. Log in to the Orion Web Console and go to the view where you want to add the resource.
2. Click Customize Page in the top right corner.
3. Click the + icon on the Customize page, and type "forecast" or "capacity" into the Search field.
4. Select the resource, and click Add Selected Resources.
5. Click Done to add the resource on the view.
6. Click Submit. The resources will now appear on the view.


Change capacity forecasting settings globally

Capacity forecasting settings include the forecast calculation method and thresholds for the metrics. By default, the settings are set globally.

See [Customize capacity forecasting settings for single nodes, interfaces, or volumes](#).

Change calculation method and thresholds for nodes or volumes

1. Click Settings > All Settings, and select Orion Thresholds in the Thresholds & Polling section.

 If you are in a capacity forecasting resource, click Edit, and click Orion General Thresholds.

2. Specify values for Critical Level and Warning for the metrics:
 - AVG CPU Load for CPU usage on nodes
 - Disk Usage for volume capacity usage
 - Percent Memory Used for memory usage on nodes
3. For each metric, select the calculation method.
 - Calculate exhaustion using average daily values
 - Calculate exhaustion using peak daily values
4. Click Submit.

You have changed the method and thresholds for calculating capacity forecast for monitored nodes and volumes.

Change calculation method and thresholds for interfaces

1. Click Settings > All Settings, and select NPM Thresholds in the Thresholds & Polling section.
2. Go to the Interface Percent Utilization section, define the Critical and Warning threshold values for the metric.

3. Select the calculation method:
 - Calculate exhaustion using average daily values
 - Calculate exhaustion using peak daily values


4. Click Submit.

You have changed the method and thresholds for calculating capacity forecast for monitored interfaces.

Customize capacity forecasting settings for single nodes, interfaces, or volumes

You can set different forecast calculation methods and thresholds for individual nodes and volumes.


For interfaces, the calculation method is set globally, and you can customize only the thresholds.

 Set warning and critical thresholds for critical nodes, interfaces, or volumes to lower percentages, so that you have enough time to take measures before capacity issues occur.


Customize capacity forecasting thresholds and calculation methods for nodes:

1. Log in to the Orion Web Console as an administrator.
2. Open the Edit Properties page for the node.

Go to Settings > Manage Nodes, select the node, and click Edit Properties.

 If you are in a capacity forecasting resource, click Edit, and click the link to the node's Edit Properties page.

3. On the Edit Properties page, scroll down to Alerting Thresholds.
4. Select Override Orion General Thresholds for CPU Load or Memory Usage, and define the Warning and Critical threshold levels.
5. Select the method for calculating trends:
 - Calculate exhaustion using average daily values
 - Calculate exhaustion using peak daily values

 If you want to use baseline thresholds, click Use Dynamic Baseline Thresholds. See [Baselines and baseline calculations](#).


6. Click Submit.

You have changed the method and thresholds for calculating capacity forecast for the node.

Customize capacity forecasting settings for interfaces:


1. Log in to the Orion Web Console as an administrator.
2. Open the Edit Properties page for the interface.

Go to Settings > Manage Nodes. Expand the parent node, select the interface, and click Edit Properties.

 If you are in an interface capacity forecasting resource, click Edit, and click the link to the interface's Edit Properties page.

3. On the Edit Properties page, scroll down to Alerting Thresholds.

4. Select Override Orion General Thresholds for Receive Interface Utilization or Transmit Interface Utilization, and customize the Warning and Critical threshold levels.


 If you want to use baseline thresholds, click Use Dynamic Baseline Thresholds. See [Baselines and baseline calculations](#).

5. Click Submit.

You have changed the thresholds for calculating capacity forecast for the interface.

Customize capacity forecasting settings for volumes:

1. Log in to the Orion Web Console as an administrator.
2. Go to Settings > Manage Nodes.
3. Select the volume, and click Edit Properties.

 To find the volume, locate the node, and click the + sign to display interfaces and volumes on the node.

4. Select Override Orion Capacity Thresholds for Percent Disk Usage.
5. Customize the Warning and Critical threshold levels.
6. Select the appropriate method for calculating trends:
 - Use Average values
 - Use Peak values
7. Click Submit.

You have changed the method and thresholds for calculating capacity forecast for the volume.

Monitor fibre channel devices and virtual storage area networks (VSANs)

VSANs and fibre channel devices on the network are automatically recognized when they are added to the SolarWinds Orion database for monitoring.

To see an overview of monitored VSANs in the Orion Web Console, click My Dashboards > Network > VSANs in the menu bar.

Click a VSAN to go to the VSAN details view.

Use the Fibre Channel Units and Ports report and the VSAN-specific resources on the views.

Monitor custom statistics based on MIBs and OIDs with Universal Device Pollers


SolarWinds Universal Device Poller (UnDP) is a customization feature of SolarWinds NPM. With UnDP, you can create custom monitors for almost any statistic provided by SNMP based on its Management Information Base (MIB) and object identifier (OID).

With Universal Device Poller, you can monitor:

- Interface traffic
- CPU temperature
- Addressing errors
- UPS battery status
- Current connections to a website

Before you start configuring UnDPs

- Consult your vendor documentation, and find out which OID you want to monitor.
- Create a list of nodes that you want to poll the custom statistic on.

 UnDPs do not collect data from Orion Failover Engine or Hot Standby Engines. If a SolarWinds NPM server fails, data collection for any Universal Device Pollers stops on the server.

UnDPs are tied to the polling engine on which they are hosted. If you move a monitored node from one polling engine to another, you must also move the UnDP poller.

Define a custom statistic to monitor

Statistics monitored on your devices are specified by pollers. Pollers hold information about a monitored property, how to get the current value for the property, and where and how to display the retrieved data.

Defining a custom statistic for monitoring means creating a UnDP poller.


1. Click SolarWinds Orion > Network Performance Monitor and start the Universal Device Poller.
2. If prompted, [download and install the MIB database](#).
3. Click New Universal Device Poller.
4. Specify the OID:
 - a. Click Browse MIB Tree, and click Search MIBs in the upper-right corner.
 - b. Select a Search By option, enter a string, and click Search.
 - c. Select the OID, and click Select.




- If you know the OID, fill it in.
- If you know approximately where in the MIB tree you can find the OID, click Browse MIB Tree, navigate in the MIB tree to the OID, and click Select.

5. Test the selected OID against a device. Select a node, and click Test. See [Troubleshooting failed tests](#) if the test fails.
6. On the Define Your UnDP screen, edit the suggested Name and Description. The name is required and cannot contain spaces.

7. To customize the value type, SNMP Get type, polling type or interval, click Advanced Options, and change the defaults:
 - a. Select the expected format of values in MIB Value Type.
 - For Rate or Counter, provide a Unit and Time Frame.
 - For Raw Value, select a display Format for the polled raw values .
 - For Raw Value > Enumerated, click Map Values to provide strings corresponding to the values returned by the poller.
 - b. Select SNMP Get Type, and decide whether the poller should poll nodes or interfaces.
 - c. Specify the Polling Interval in minutes. Use values between 1 and 600.


 If you want to use the poller in a transformation, make sure that all pollers in the transformation have the same Polling Interval.

8. Keep default settings for Status (Enabled) and Keep Historical Data (Yes). With these options enabled, you can see the trend of polled values in Orion Web Console views.
9. Specify the Group to which you want to add the poller, and click Next.

 To create a new group, type a name for the group into the Group box.

10. Select devices to poll the statistic, click Test, and then click Next.
11. If the selected OID is a table, specify the labels.
12. Select the Orion Web Console views that can display the poller as a chart, gauge, or table, and click Finish.

The new poller is added to All Defined Pollers and will be polled on the selected nodes or interfaces. You can now see the polled values in the selected Orion Web Console resources.

- 
- To view the poller status on maps, create a network map, add the poller into the map, and add the map on a view. See [View UnDP status on maps](#).
 - To check that your UnDP pollers are properly configured, start Orion Diagnostics in your SolarWinds Orion > Documentation and Support program folder, right-click a UnDP, and select Run Tests.

Troubleshooting failed tests

If the test fails on a node or interface, make sure that the following settings are correct:

- Verify that the test node is being polled using the correct community string. See [Edit node properties](#).
- Does the device support the polled MIB or OID? See the vendor documentation to confirm the MIBs supported by your device.
- Can your SolarWinds NPM server access the device? Make sure that the device is responding to both ICMP and SNMP requests.

Select nodes or interfaces to poll a custom statistic

When you have defined the custom statistic to monitor and created a UnDP poller, specify the devices (nodes or interfaces) to monitor the statistic.

Before you begin, make sure the UnDP poller is created and enabled. See [Define a custom statistic to monitor](#).

1. Click SolarWinds Orion > Network Performance Monitor and start the Universal Device Poller.
2. Click Assign Pollers.
3. Navigate the poller tree, select the pollers you want to assign, and click Next.

By default, there are two poller groups:

- Example - all predefined out-of-the box UnDP pollers.
- Default Group - all user-defined UnDPs if they are not assigned to any other group.



Selecting a poller group selects all pollers in the group. If you do not want to assign all pollers, clear the pollers that you do not want to assign.

4. Expand the node tree down to the interface level, and select the elements to apply the pollers.



- Interfaces are not displayed unless you are assigning an interface poller.
- Selecting a node automatically assigns a selected interface poller to all interfaces on the node. Clear boxes for interfaces that should not be assigned to the poller.

5. Click Test to see current results of the selected pollers on the selected nodes or interfaces. If the test fails, see [Troubleshooting failed tests](#).
6. After you have completed your poller assignments, click Finish.

Transform poller results

Values polled by a custom poller are often better understood after a calculation transforms the value to a different format.

For example, if a poller returns temperature values in Celsius, you might want to see the values in Fahrenheit.

Pollers that you use in a transformation must be assigned to the nodes to poll for values that will be transformed.

1. Click SolarWinds Orion > Network Performance Monitor and start the Universal Device Poller.
2. Click Transform Results, and click Next to acknowledge examples of transformations.


3. Enter a name and a description for the transformation, and click Next. Names must be unique.

Names are required. Any spaces in the name are removed.


Descriptions are optional but might be helpful in identifying the type of information generated by the transformation.

You can also change other default settings:

- a. Select Yes in the Keep Historical Data section. You will be able to view the transformed poller data in charts and gauges in the Orion Web Console.
- b. Select Enabled as the Status if you want your transformation to begin calculating results immediately.

 If you select Disabled, the transformation will not transform polled data.

- c. In the Group field, select a group where you want to add the transformation. To add a group, provide the new group name.
- d. Optional: provide a polling interval.

 Make sure all pollers in the transformation use the same polling interval.

4. Provide the formula for calculating the transformation.

- a. Click Add Function, and select a function.
- b. Click within the bracket, click Add Poller, and select the poller you want to transform.
 - Separate pollers with commas. The following example averages the results of three pollers:
`avg({poller1},{poller2},{poller3})`
 - Use standard mathematical operations:
`{poller1}+{poller2}`
 - Use the mathematical constants e and π , as `E()` and `PI()`, respectively.
 - Nest formulas. The following example returns the average of two poller comparisons:
`avg(min({poller1},{poller2}),max({poller3},{poller4}))`


5. Test the transformation on a device, and click Next.

Troubleshooting failed transformation tests


If the test fails, verify the following items:

- Is your formula correct? Ensure that all braces 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 [Edit node properties](#).
- Does the device support the polled MIB or OID? See the documentation supplied by the device vendor to confirm supported MIBs for your device.
- Can you access the device from the SolarWinds Network Performance Monitor server? Confirm that the device is responding to both ICMP and SNMP requests.


6. Select nodes for the transformation, and click Test.

-  ■ Available groups are listed in the Group By field. Select a group to limit the node tree.
- Interfaces are not displayed unless your poller transformation operates on an interface poller.
- When assigning an interface poller transformation, selecting a node assigns that transformation to all interfaces on the node.
If you do not want to apply the poller transformation to an interface, expand the parent node, and clear interfaces to which the transformation should not be assigned.

7. If the transformation output is a table, select labels for the rows in the table, and click Next.
8. Select Orion Web Console views where you want to include the transformed values as a chart or table, and click Finish.

-  Click Preview to see how your poller resource will display in the selected Orion Web Console view.


The new transformation is added to All Defined Pollers and applied on the selected nodes or interfaces. You can now see the transformed values in the selected Orion Web Console resources on views for nodes or interfaces.

-  If the transformation combines data from other pollers, make sure that it is assigned to the same node or interface as the pollers used for the transformation and that it has the same polling interval.

Create pollers by duplicating and adjusting pollers

When creating similar pollers, consider copying a poller and modifying it.


1. Click SolarWinds Orion > Network Performance Monitor and start the Universal Device Poller.
2. In the All Defined Pollers pane, locate the poller that you want to duplicate.

-  To confirm that you have selected the appropriate poller, view the poller properties in the main Universal Device Poller window.

3. Right-click the poller, and select Duplicate Poller.
4. Change the Name of the poller.
5. Adjust the poller settings. See [Define a custom statistic to monitor](#).


Import UnDP pollers

You can import custom UnDP pollers exported from UnDPs installed with earlier SolarWinds NPM versions.


-  You cannot import device-specific MIBs into the SolarWinds MIB Database, but you can import UnDP pollers based on OIDs from device-specific MIBs. Import a poller and assign it to nodes or interfaces in your environment.

1. Click SolarWinds Orion > Network Performance Monitor and start the 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 locate the poller.
 - b. Select the poller, and click Open.
4. Select the pollers to import from the list on the left, and click Import. Selected pollers will move to the pane on the right.

-  ■ To select multiple pollers, hold down SHIFT or CTRL, and click the pollers you want.
- To remove a poller from the Selected Pollers list, select the poller and click Remove.
- To collapse all folders and see just the group names, hold down SHIFT, and then click – next to any of the group names.

5. Click OK.
6. To begin polling, enable the poller.
 - a. Select the imported poller in the All Defined Pollers pane of the Universal Device Poller window.
 - b. Click Edit Properties.
 - c. Confirm that the poller Status is Enabled, and click Finish.

 If Disabled, the poller will not collect data until you enable it.


7. Specify nodes or interfaces to be polled by the imported poller. See [Select nodes or interfaces to poll a custom statistic](#).

When the imported poller is enabled and assigned to the devices, the poller begins collecting statistics. To view the statistics, log in to the Orion Web Console, go to a view for the node or interface to which the poller is assigned, and consult the poller resource. See [View Universal Device Poller statistics in the Orion Web Console](#).

Export UnDP pollers

If you want to use your custom UnDPs in later SolarWinds NPM versions or on different polling engines, you need to export them first.

1. Click SolarWinds Orion > Network Performance Monitor and start the Universal Device Poller.
2. Click File > Export Universal Device Pollers.
3. In the Pollers pane on the left, navigate to the pollers that you want to export.

-  ■ To select all pollers in a group, select the group.
- To select multiple pollers, hold down SHIFT or CTRL and click the pollers to export.

4. Select the pollers, and click Export. Pollers will move to the Selected Pollers pane.

 To remove a poller from the list of pollers for export, select the poller and click Remove.

5. Click Save.
6. Navigate to the location where you want to export the selected pollers, provide a File name, and click Save.

Selected pollers will now be stored as a .UnDP file in the specified location. You can use the .UnDP file to import the pollers on another polling engine.

Temporarily suspend collecting statistics for pollers

When you assign a poller to nodes or interfaces, it starts collecting statistics on the selected elements. If you want to suspend data collection for a poller without deleting it, disable the poller.

1. Click SolarWinds Orion > Network Performance Monitor and start the Universal Device Poller.
2. In the All Defined Pollers pane, navigate to the poller you want to disable.



To confirm that you have selected the appropriate poller, view the poller properties in the main Orion Universal Device Poller window.

3. Select the poller, and click Edit Properties.
4. Set Status to Disabled, and click Finish.

The poller will now still be available in the Universal Device Poller application, but will not collect any statistics.

Define UnDP Warning and Critical thresholds

If values polled by UnDPs on a device reach a certain level (critical or warning threshold), the UnDP on the device is highlighted in the Orion Web Console.



To get notified about exceeding a threshold in an email, configure an alert. See [Alerting on printer toner running low based on a custom UnDP poller](#) for an example of using custom pollers in alerting.

To see pollers with exceeded thresholds in a map, see [View UnDP status on maps](#).

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. In the Thresholds & Polling grouping, click Custom Poller Thresholds.
4. Select a poller.
5. Select whether the expected polled value is a Text or a Number.



The Poller Value Type determines how the polled value will be interpreted. It also influences the set of possible comparison functions.

- For the Number type, available values include `is greater than` or `less than`.
- For the Text type, available values include `for example contains`.

6. Build conditions to define both Warning and Critical Thresholds:
 - a. Select whether All Child Conditions Must Be Satisfied (AND) or if only At Least One Child Condition Must Be Satisfied (OR).
 - b. Select a comparison relation, and provide a threshold value on which the comparison is based.

CISCOENVMONTEMPERATURESTATUSVALUE
Poller Value Type: ☐ Text ☒ Number

Warning Threshold

Where: All child conditions must be satisfied (AND)

Value: is greater than 70

Critical Threshold

Where: All child conditions must be satisfied (AND)

Value: is greater than 80

- c. Click + to add additional conditions, as required, to define the poller threshold.

7. After configuring all thresholds, click Submit.

If a value reported by the device belongs to the range defined by the Warning Threshold, pollers in maps will be yellow.

If a value reported by the device belongs to the range defined by the Critical Threshold, pollers in maps will be red.

View Universal Device Poller statistics in the Orion Web Console

If you want to see a poller results in the Orion Web Console, you need to define which resources should be displayed on which views.

Prerequisites


The poller must be enabled, and assigned to the devices.



Set the poller to collect historical statistics. Without historical data, Orion Web Console resources will only display the last polled value, and you cannot add charts with the poller results to the Orion Web Console.

Define resources with UnDP results for Orion Web Console views

1. Click SolarWinds Orion > Network Performance Monitor and start the Universal Device Poller.
2. In the All Defined Pollers pane, select the poller whose results you want to add as a Orion Web Console resource.
3. Right-click the poller, and click Web Display.
4. Confirm that Yes is selected, and select the types of poller resources that you want to display on individual Orion Web Console views.

 Click Preview to see what the poller resource will look like in the Orion Web Console view.

5. Make sure Do Not Show This Poller If It Is Not Assigned is selected. It ensures that the custom poller resource appears only on views for nodes or interfaces that have the custom poller assigned to them and enabled.
6. Click Finish.

When you log in to the Orion Web Console, the selected resources with poller data will appear on selected views for nodes or interfaces that have the poller assigned to them and enabled.

See also [View UnDP status on maps](#).

View UnDP status on maps

In the Orion Web Console network maps, you can see when a Universal Device Poller on a device returns values that exceed the warning and critical thresholds.

1. [Create a Universal Device Poller](#) in the UnDP application.
2. Assign the poller to nodes.
3. [Define warning or critical thresholds](#) specifying when you want the pollers to be highlighted.
4. Create a network map in the Network Atlas, drag the UnDPs into it, and save the map.



To add a UnDP on a map, start the Network Atlas, navigate to a node on which the UnDP is enabled (Vendor > Node Name > Custom Node Poller), and drag the poller into the map.

5. Log into the Orion Web Console, go to the map view.
6. Locate the Map resource (or add it if not available), click Edit and select your map.

You can now see UnDPs for your nodes in the Orion Web Console map. When the polled UnDP values exceed the warning threshold, the UnDP icon turns yellow on the map. After reaching the critical threshold, the icon turns red.

Cannot find OIDs? Update 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. The MIB database is updated regularly.

When you are creating a UnDP poller and cannot find an OID in the MIB tree, update the MIB database.

1. Log in to the Customer Portal (<https://customerportal.solarwinds.com/>) using your SolarWinds Customer ID and Password.
2. On the left under Helpful Links, click Orion MIB Database.
3. If you are using Internet Explorer and it prompts you to add the SolarWinds downloads site <http://solarwinds.s3.amazonaws.com>, add the site to your trusted sites.
4. Specify a location where the file will download.
5. After the download completes, extract `MIBs.zip` to a temporary location.

6. Open the folder with the extracted MIBs .zip, and copy MIBs .cfg to the SolarWinds folder on your default install volume.

The default location depends on the operating system:

- Windows Server 2003 and XP:
C:\Documents and Settings\All Users\Application Data\Solarwinds
- Windows Server 2008 and Vista:
C:\ProgramData\Solarwinds

 You may need to restart the Universal Device Poller after installing the MIB database.

Manage pollers using Device Studio

With the Device Studio, you can create custom pollers in the Orion Web Console.

Custom pollers allow you to monitor specific technologies or unique devices that are not automatically detected for monitoring in your SolarWinds environment.

What is a poller?

Statistics monitored on your devices are specified by pollers. Pollers hold information about a monitored property, how to get the current value for the property, and where and how to display the retrieved data.


What do you need custom pollers for?

- To monitor a specific metric which is not monitored out-of-the box.
- To monitor special equipment.
- To monitor objects although the number of monitored objects exceeds a poller's capacity limitation.

Manage unique devices on the network

If you have devices on your network that SolarWinds does not recognize for polling, you can either edit an existing poller to suit your device needs, or create a poller specifically tailored to your device.

SolarWinds Orion polls values based on OIDs from the SolarWinds MIB database. There can be OIDs you might want to poll, which are not polled by SolarWinds Orion by default. If these OIDs are in the SolarWinds MIB database, you can create either an UnDP, or use Device Studio to poll for that value, and add support for vendors and technologies that are not natively supported by SolarWinds Orion.

 Orion Platform products poll devices based on OIDs according to the device vendor's MIB. These OIDs must be included in the SolarWinds MIB database. When you create custom pollers, you select OIDs from the SolarWinds MIB database.


To poll an OID which is not in the SolarWinds MIB database, define it manually. See [Define object identifiers \(OIDs\) that do not exist in the SolarWinds MIB database](#).


With Device Studio pollers you can:

- Poll devices that do not support any of the OIDs polled for by SolarWinds pollers.
- Poll devices that return incorrect data when polled by SolarWinds pollers.
- Override polled values to display custom static values.

Device Studio technologies

Device Studio supports a number of technologies. Each technology has a defined set of properties that you can monitor on your devices. The technology you select defines how the polled data are processed, stored, and presented.

TECHNOLOGY	USAGE
CPU & Memory	<p>CPU & Memory is used for collecting data about the CPU and memory load of single processor systems.</p> <p>It provides data to resources related to CPU and memory, such as Average CPU Load & Memory Utilization, Min/Max/Average of Average CPU Load, or Top CPUs by Percent Load.</p> <p>To use this technology, specify a single OID that reports a value from 0 to 100.</p> <p>For example, if a natively polled OID returns incorrect CPU load values, search for an OID that returns a possible value. In the case of CPU load, the load can vary between 0% and 100%, so you must look for an OID that returns a value between 0 and 100.</p> <div>  To determine the OID, consult your device vendor, or carry out a search for an OID that reports the correct value for your device. </div>
Multi CPU & Memory	<p>Multi CPU & Memory provides data to the same resources for multiprocessor systems as the CPU & Memory technology provides for single processor systems.</p> <p>For example, if a natively polled OID returns incorrect CPU load values, search for an OID that returns possible values. In the case of CPU load, the load can vary between 0% and 100% on each CPU core, so you must look for an OID that returns a table of values between 0 and 100, where each row corresponds to a CPU core.</p>
Node Details	<p>Node Details provides data for the Node Details resource, and can be used for devices that are not supported out of the box.</p> <p>To use this technology, specify custom OIDs to poll for Vendor, Machine Type, Software Version, and other data. You can also define custom text to be used instead of the polled value.</p>

 Pollers using other polling technologies, such as VLAN and VRF, are also displayed in the Manage Pollers view. However, it is not possible to create pollers using these technologies in Device Studio.

Data sources used in Device Studio

By creating Device Studio pollers, you can define custom polling definitions in a way that allows you to view the defined set of pollers and the data polled by them as fully integrated entities in the Orion Web Console, including charts, alerts, and reports.


You can define a set of polled data, and then associate these data points with monitored nodes.

The data source you use for polling devices can be:

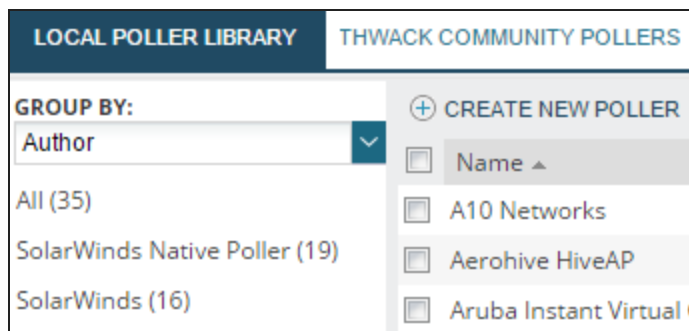
- A polled value or values reported by a device on an OID.
- A calculated value that results from the transformation of polled values.
- A fixed value in the form of a constant number or text. This value is not polled. For example, you can specify the software version of your device as 15.

Create pollers in Device Studio


To poll unique devices or technologies not supported by default, create a custom poller.

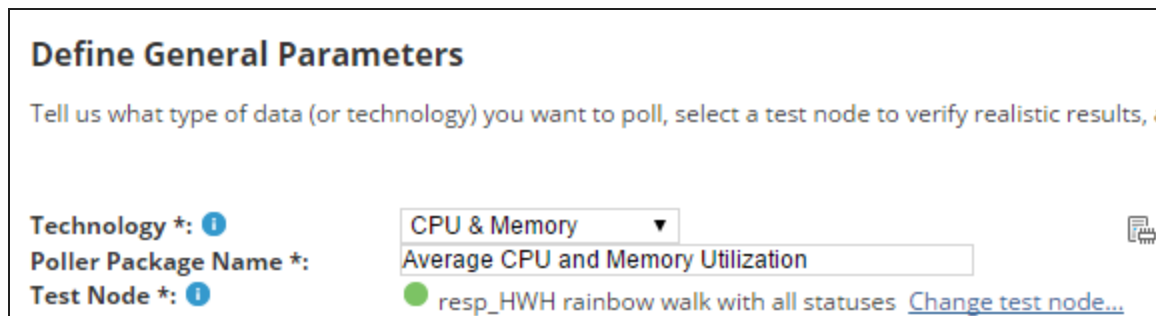
 Reduce the number of Unknown nodes by creating a custom poller.

1. Click Settings > All Settings, and in the Node & Group management grouping, click Manage Pollers.
2. Click Create New Poller.

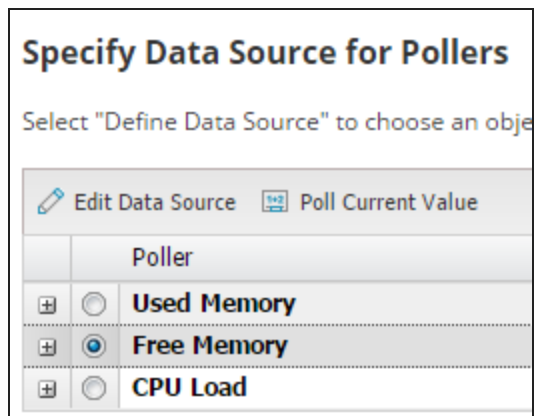


3. Select a polling technology, type the Poller Package Name, select a test node, and click Next.

 When you are creating the poller, the test node is polled to provide a preview of the results returned by the poller.








4. On the Specify Data Source tab, select a metric you want to define, and click Define Data Source.



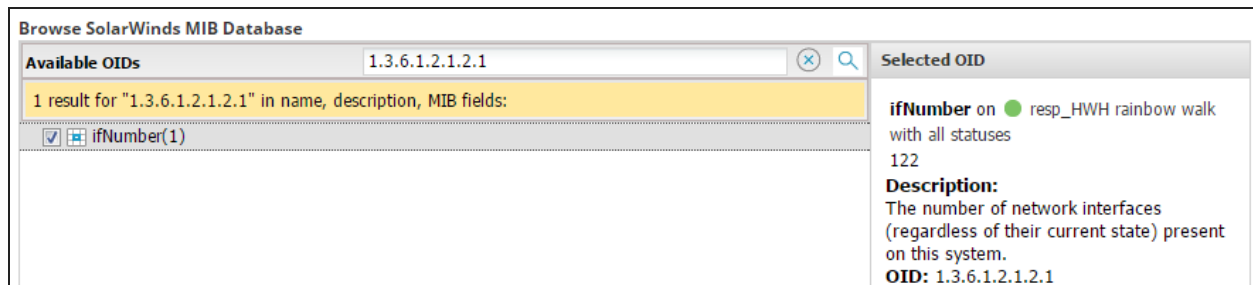
Specify Data Source for Pollers

Select "Define Data Source" to choose an object



 Edit Data Source  Poll Current Value

Poller	
	<input type="radio"/> Used Memory
	<input checked="" type="radio"/> Free Memory
	<input type="radio"/> CPU Load



5. On the Pick Object Identifier screen, type the OID, or search the MIB database. For information about manually defining OIDs, see [Define object identifiers \(OIDs\) that do not exist in the SolarWinds MIB database](#).



Browse SolarWinds MIB Database

Available OIDs:  

1 result for "1.3.6.1.2.1.2.1" in name, description, MIB fields:

Available OIDs	Selected OID
<input checked="" type="checkbox"/>  ifNumber(1)	ifNumber on  resp_HWH rainbow walk with all statuses 122 Description: The number of network interfaces (regardless of their current state) present on this system. OID: 1.3.6.1.2.1.2.1

6. If necessary, click Add Calculated Value to transform the multiple returned values into a single value, or select a different OID.



Transforming multiple values to a single value is useful if, for example, the device returns CPU usage as a table of four values (with one value for each CPU core), but you want to use a single value for CPU usage. In this case, you can use the Average function to convert the table of values into a single value.

For more information, see [What is a formula?](#)

7. In the Create a Calculated Value screen, select a function, select an input from the lists, and click Test. You can also define a constant value, for example, if you are creating a CPU and memory poller, and the device you want to poll only supports CPU values.



Continuing with the previous example, to create an average value out of the four reported values, select the Average function and specify the input values.

Select function... Select input...

Select function...

KiloToByte - multiplies input by 1024

MegaToByte - multiplies input by 1024*1024

GigaToByte - multiplies input by 1024*1024*1024

Average - input column to output average of values in all rows

Sum - input column to output sum of values in all rows

Count - input column to output total number of rows

Condition - create an if/then statement

For more information, see [Formulas used for transforming Device Studio poller results](#).

8. After testing whether the value is as expected, click Yes, the Data Source Is Reasonable.
9. To automatically test the poller on newly added nodes, select Automatically poll nodes during network discovery, and click Next. The test determines whether the Device Studio poller can be assigned to the newly added node.

Network Discovery Settings

☒ **Automatically poll nodes during network discovery, add node,**
This poller will be enabled on nodes where OIDs are polled successfully

10. On the Summary tab, review the poller package settings, and click Submit.

Review Your Poller Package Settings

Technology: CPU & Memory

Poller Package Name: Average CPU and Memory Utilization

Description:

Tags:

Author:


The poller is now available in the list of pollers, and you can assign it to nodes.

Define object identifiers (OIDs) that do not exist in the SolarWinds MIB database

1. On the Pick Object Identifier screen, select the check box under Manually Define Object Identifier (OID).
2. Type the name and OID.
3. Select the SNMP get type. See [What is the SNMP Get Type?](#) for more information.
4. Click Poll Current Value From Test Node.

What is the SNMP Get Type?

The SNMP Get type defines the type of query you have to run to retrieve the appropriate information. You can retrieve scalar values by using either GET or GET NEXT, and you can retrieve values from a particular column in a table value by using GET TABLE.

 For table records, only the first five values are returned.

What is a formula?

Values polled by a custom poller are often better understood after a calculation transforms the value to a different format. For example, if a poller returns values in MB, you might want to work with the values presented in GB. The calculations and transformations that are used to manipulate poller results are called formulas.

Two types of values or data sources are available:

- Scalar: one value
- Tabular: column of values

When a new data source is created, the name is generated automatically according to the syntax:

<Property name>Formula<Number>

For example: UsedMemoryFormula1

Formulas used for transforming Device Studio poller results

FORMULA	DESCRIPTION
KiloToByte	Multiplies input by 1024
MegaToByte	Multiplies input by 1024 x 1024
GigaToByte	Multiplies input by 1024 x 1024 x 1024
Average	Returns the average of values from the input columns
Sum	Returns the sum of values from the input columns
Count	Returns the total number of input columns
Condition	Creates an if/then statement
Truncate	Rounds the input decimal number up or down to an integer
Length	Returns the number of characters in the input string
Replace	Replaces the content in the string
IndexOf	Returns the position in the string
SubString	Defines the section of the string of interest

The formulas are divided into three main groups.

TYPE OF FORMULA	DESCRIPTION
Transformations	Transform data between different units. For example, transform megabytes to bytes.
Aggregations	Transform the values from the input table columns to scalar values. For example, transform the values from the input columns into the average of values.
Conditions	Transform values according to a logical formula according to the following syntax: if(logical formula), (action to perform if formula is true), (action to perform if formula is false)

Example syntax

SubString

The SubString(,,) calculation takes the following syntax:

```
SubString ([formula],index start,length)
```

For example, if your input is "test", the output will be "es" if you use the following calculation:

```
SubString ([UsedMemoryFormula],1,2)
```

As another example, if your input is "test", the output will be "st" if you use the following calculation:

```
SubString ([UsedMemoryFormula],2,2)
```

Replace

The Replace(,,) calculation takes the following syntax:

```
Replace([formula],search string,replacement string)
```

For example, if your input is "test", the output will be "resr" if you use the following calculation:

```
Replace([UsedMemoryFormula], "t", "r")
```

Use Regex formulas for transforming poller results

When you define a Regex formula, use the following syntax:

```
Regex([variable], "regular expression")
```

Examples of correct formulas include:

- `Regex([description], "^[a-zA-Z]*[^\,]*")`
- `Regex([description], "(V.[^\,]*)")`
- `Regex([description], "(T.*)")`
- `Regex([description], "(C.[^\,]+)")`

Limitations of Regex formulas

When you define a Regex formula, the input string from the test device is interpreted up until the nearest `\r` (new line) character.

The following methods of defining Regex formulas are not supported:

- A backslash sequence for special characters such as the following: (,) , { , } , .
- Grouping regular functions such as the following: \w, \W, \s, \S.
- Defining multiple conditions in square brackets such as the following: [^ , -].

Test Device Studio pollers

A Device Studio poller may not always be seamlessly supported by the device it is tested on. For example, errors occur if the OID the Device Studio poller polls for is not supported by the device, or if the returned value is not of the expected data type defined by the Device Studio poller.

To get the Device Studio poller working in your environment, try the following:

- Test the Device Studio poller on a different node.
- If the device you use for testing is not fully compatible with the Device Studio poller, upgrading the firmware of your test device might help.
- Modify the Device Studio poller to suit the devices you have. For example, you can modify the OID that is used to poll the device.



- Modifying Device Studio pollers this way requires familiarity with the MIB database structure.
- Some of the pollers provided by SolarWinds cannot be modified with Device Studio. You can only modify the poller definition of these pollers in a text editor.

Monitor devices using thwack community pollers

Apart from creating your own Device Studio pollers, you can also import pollers provided by contributors of the [thwack community](#).

The thwack community pollers are available in the Orion Web Console under Manage Pollers > thwack Community Pollers. The list is updated automatically every 30 minutes, and it contains the device pollers that have been made available on thwack, under Network Performance Monitor > NPM Content Exchange > Device Pollers > Documents.

You can group the available pollers according to tags, author, or technology. Click the name of a device poller to view the description of the poller.

To verify whether a poller suits your specific device, test the poller before importing it.


Test thwack Device pollers

1. Select the thwack community poller from the list, and click Test Device Poller.
2. Type your thwack credentials, and click Submit.
3. Select an SNMP node for testing, and click Test Poller.

After the test is finished, you can directly assign the device poller to the test node.

Import Device pollers from thwack

1. Select the thwack community poller from the list, and click Import Device Poller.
2. Type your thwack user credentials, and click Submit.
3. After the import is finished, the poller will be available in the Local Poller Library, and you can assign it to a device. For more information, see [Assign Device Studio pollers to monitored devices](#).


 If the poller was already imported earlier, you can either overwrite the existing poller, or create a new one.

Import thwack community pollers to an environment without Internet connection


The thwack community pollers are only updated automatically if you have a working Internet connection. To import thwack community pollers to an environment that does not have an Internet connection, download the pollers from a computer which can access the Internet, save them to a portable drive or a USB drive, and import them manually.

Export Device Studio pollers to the thwack community

1. On the Manage Pollers screen, click the Local Poller Library tab, and select a poller.

 You can export Device Studio pollers that you created, but you cannot export pollers that are provided by SolarWinds.

2. Click Export, and select Export to Thwack.
3. Type your thwack user credentials, and click Submit.

 If you already logged in to thwack from the Orion Web Console during the same session, you do not have to enter your credentials again, and the Device Studio poller will be exported immediately.

The Device Studio poller will be available on thwack, in the Network Performance Monitor > NPM Content Exchange > Device Pollers > Documents section.

Why can't I connect to thwack?

Your SolarWinds Orion server must be able to open internet connections to connect to thwack. If the connection is blocked by a firewall or a proxy the list of shared pollers cannot be retrieved from thwack, and any operation that relies on communication with thwack, such as the upload or download of a poller will fail.

Check your firewall and proxy settings to make sure that your SolarWinds Orion server can connect to the internet.

Assign Device Studio pollers to monitored devices

Specify devices on which you want to poll the statistics defined by the poller.

1. On the Manage Pollers page, select a poller, and click Assign.
2. Select the node you want to assign the poller to.

3. If the node has not been scanned yet, click Scan Now.
4. If the scan result is a match or a multiple match, select the node, and click Enable Poller.

 You can only scan SNMP nodes whose status is Up.

Scan monitored objects to verify if the OIDs match

When a monitored node is scanned, the OIDs of the monitored node and the OIDs specified in the poller are compared to see if they match.

These scenarios are possible:


- If the OIDs do not match, the scan returns a result indicating the mismatch, and the poller cannot be assigned to the monitored node.
- If the OIDs match, and there is no other poller supporting the specific technology, then the poller is automatically enabled on the node.
- If the OIDs match, but there is already another poller for the technology, the new poller is not enabled. You can enable the poller manually. See [Assign Device Studio pollers to monitored devices](#).

Monitor F5 BIG-IP devices

The performance statistics you can monitor on F5 BIG-IP devices include device status and availability, CPU and memory performance statistics, and interface performance details.

 F5 node, interface and status reporting is supported for F5 firmware versions 11.2 and later.

F5 interfaces statistics are available in existing interface resources. Other statistics are shown in specific F5 resources.

 To add an F5 resource, click Customize Page on the view, click the + icon, and type F5 into the Search field. Select the F5 resources you want to see on the view, and add them.

Network Insight for F5[®] BIG-IP[®] load balancers

Network Insight provides comprehensive monitoring for the F5 BIG-IP family of load balancers, giving you the insight you need to keep your most important services running smoothly. Use Network Insight to:

- Monitor the health and performance of all components of application delivery including WideIPs, virtual servers, pool members, and more.
- Identify the components that are contributing to slowness, service outages, or any service that could be affected by an infrastructure problem.
- Visualize your entire application delivery environment and get an instant status of a service or device. Click on any status indicator to see additional details about that component or to show relationships.

- Graphically display relationships and component status. Easily view the relationships from the service through the traffic managers, virtual servers, pools, and pool members along with a detailed status of each component.

Set up Network Insight for F5® BIG-IP® load balancers


To monitor the servers and connections in your load balancing environment, make sure your F5 devices meet the following requirements, add the F5 devices for monitoring, and enable F5 iControl.

Requirements

REQUIREMENT	DETAILS
supported modules	F5 Local Traffic Managers (LTMs) BIG-IP DNS (formerly called Global Traffic Managers or GTMs)
SNMP	used to poll everything except for health monitors TMOS version 11.2 and later (including 12.0)
iControl by F5	used to poll health monitors and to enable and disable the rotation of pool members . TMOS version 11.6 and later

Add F5 devices and enable iControl

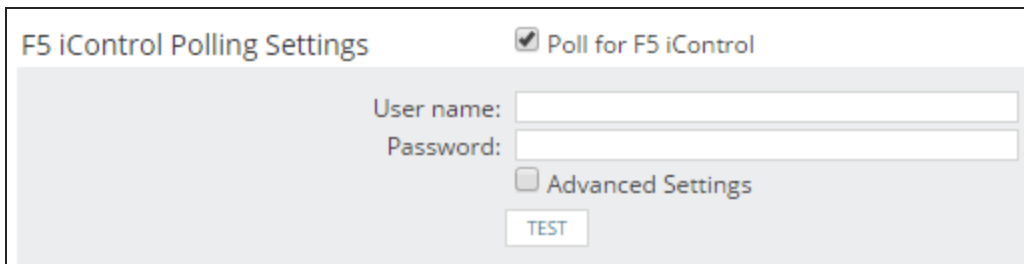
[Add F5 devices](#) hosting global traffic managers (GTM) and local traffic managers (LTMs) for monitoring.

 You need Node Management Rights. See [Define what users can access and do](#).

1. Click Settings > All Settings, and click Add Node in the Getting Started grouping.
2. Enter the IP address for the device.
3. Select Most Devices: SNMP and ICMP as the polling method.

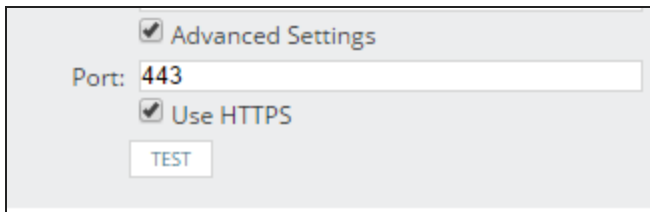
4. Enable F5 iControl:

- a. Scroll down to Additional Monitoring Options, select Poll for F5 iControl, provide the credentials for accessing the iControl API on the F5, and click Test.



The screenshot shows a dialog box titled "F5 iControl Polling Settings". It has a checkbox labeled "Poll for F5 iControl" which is checked. Below this are two input fields: "User name:" and "Password:". There is also an unchecked checkbox labeled "Advanced Settings" and a "TEST" button at the bottom right.

- b. If iControl does not run on the default port 443, select Advanced Settings, and provide the port.



The screenshot shows a dialog box titled "Advanced Settings". It has a checked checkbox labeled "Advanced Settings". Below this is a "Port:" label followed by an input field containing the number "443". There is also a checked checkbox labeled "Use HTTPS" and a "TEST" button at the bottom.

5. Complete the Add Node wizard.

Both status information and health statistics will be collected on the F5 device, and you can now monitor your load balancing environment:

- [Monitor services delivered by F5® BIG-IP® load balancers](#)
- [Take an F5 pool member out of rotation](#)

 See [Discover your network with the Discovery Wizard](#) to add more F5 devices at the same time.

Enable iControl on F5 load balancers

When your F5 devices are already monitored in SolarWinds NPM, make sure iControl is enabled. F5 iControl API is used for collecting health monitor statistics from load balancers, and for enabling and disabling the rotation of pool members.

1. Click Settings > Manage Nodes.
2. Select the node, and click Edit Properties.
3. [Enable F5 iControl](#).
4. Click Submit.

You will now be able to enable and disable the rotation of pool members and see the health monitors polled on the node.

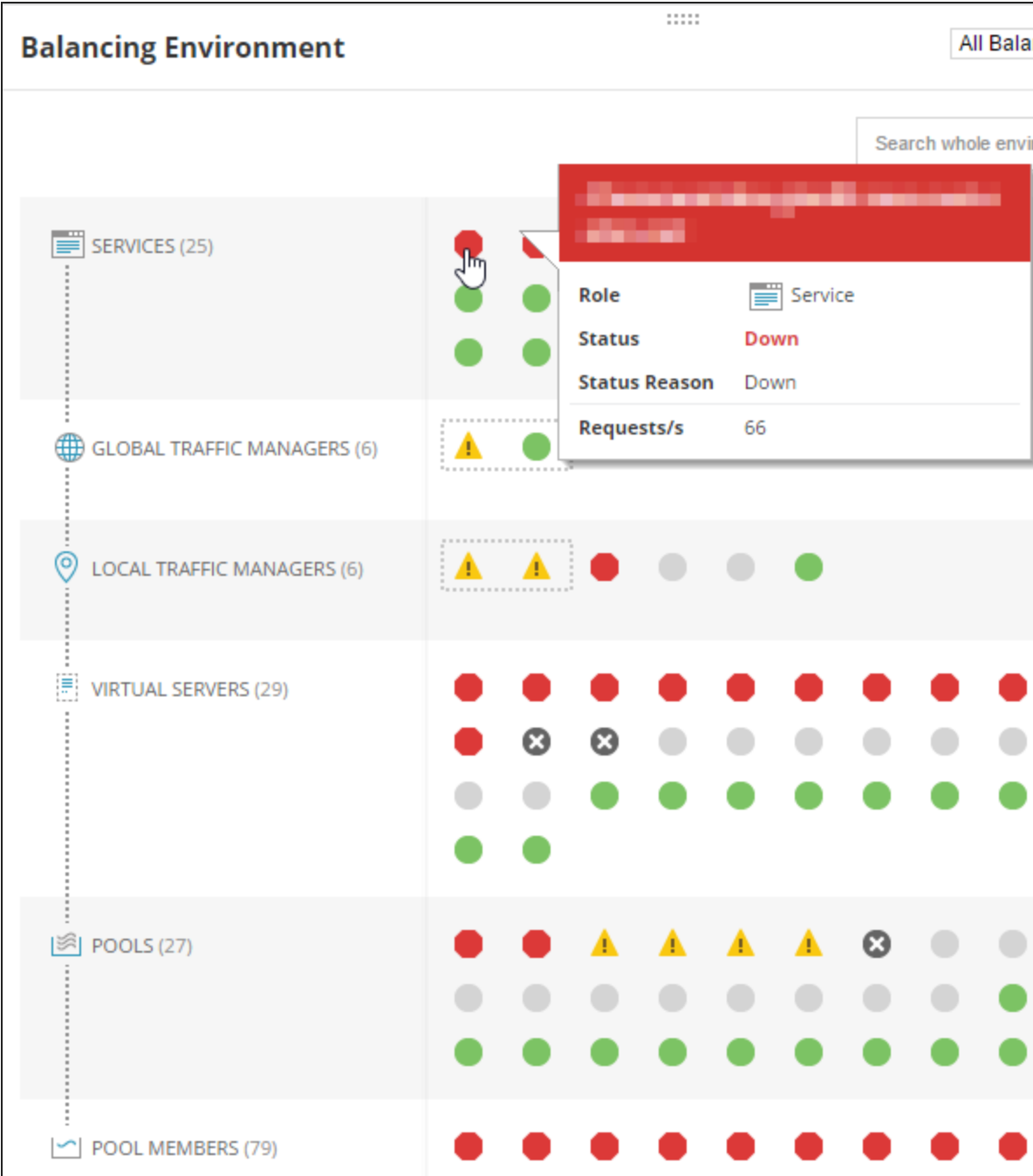
Monitor services delivered by F5® BIG-IP® load balancers


A load-balanced service is comprised of many components that work together. The Balancing Environment resource allows you to browse all of these components and their relationships and status.

- 1. Go to My Dashboards > Network > Load Balancing.

The page shows an overview of your load balancing environment.

At the top, you can see your load balanced services. Below Services, there are Global Traffic Managers (GTMs) that host the services. The GTMs send users to your Local Traffic Managers (LTM). Your LTMs present virtual servers which are made up of pools, and individual pool members hosting the content.




 Dotted rectangles highlight high availability (H/A) clusters.

2. Point to a service to review the tooltip.
3. To see more detailed information about the component, such as the number of concurrent connections and the load balancing algorithm, click the service and select Display Details Page.


F5 SERVICE DETAILS:


Service Details


STATUS  Down


STATUS REASON Down


Balancing Environment


for 


Search 


SERVICES (1) 

GLOBAL TRAFFIC MANAGERS (2) 

LOCAL TRAFFIC MANAGERS (2) 

VIRTUAL SERVERS (2) 

POOLS (2) 

POOL MEMBERS (5) 

Concurrent Connections

TOP 5 VIRTUAL SERVERS BY NUMBER

Apr 29 2016, 5:16 pm

Zoom 1h 12h

CONNECTIONS

50.0 k

40.0 k

30.0 k

20.0 k

10.0 k

30 Apr

18 Apr

Virtual Server


Role

Status **Down**

Status Reason Down

Port


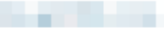
IP Address


Assigned pool 

Connections 176

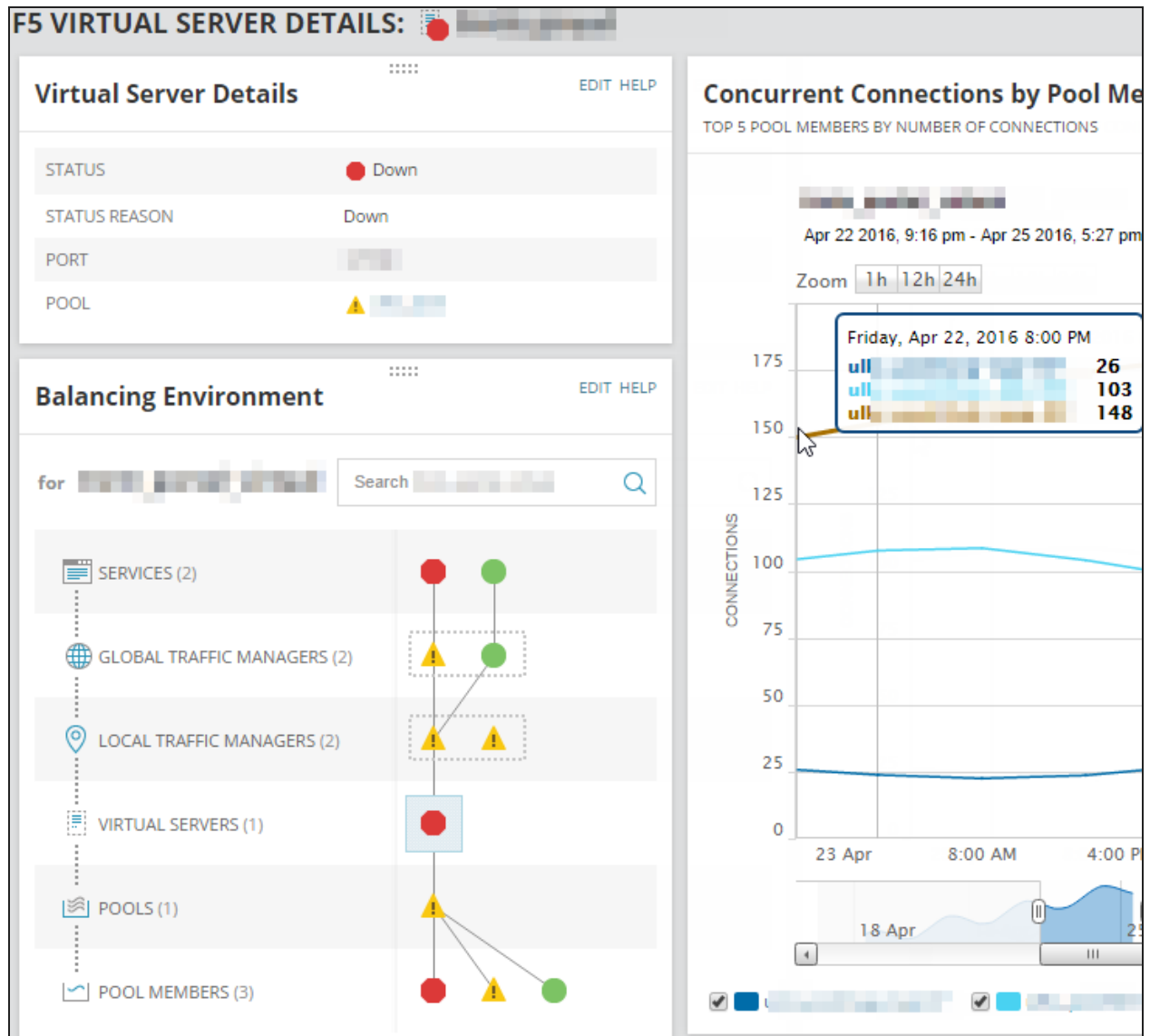
F5 Events

LAST 12 MONTHS

ACTIVITY	TIME
 Status of F5 GTM service  changed to Down.	4/25/2016 2:41:44 PM

 The light blue square in the Balancing Environment resource indicates your current position.

- The relational view of the load balancing environment sticks with us on the details page so we can continue to explore around. Select a virtual server, and click Display Details Page. This shows us the number of active connections for each pool member. We can see the load balancing algorithm and how evenly it is distributing load.




- Navigate through the load balancing environment to view the health of individual components.
- Drill in to the components with issues, review the data provided by SolarWinds NPM, such as the status of load balancing components and the reason why they are not up. Use the data to troubleshoot the issues.

Status of F5 devices













F5 status is information polled directly on the F5 device through SNMP. SolarWinds NPM also polls the status reason from the F5 device and displays the reason in the element's tooltip and on the details pages.

The status for GTM and LTM modules is calculated. LTM status is calculated based on virtual server, GTM status is calculated on the WideIP (service).

 F5 status is not the same as the node status. Both node statistics and F5 statistics are polled through SNMP, but from separate parts of the MIB tree. That's why a node can be up (Orion statistics), but the corresponding load balancing component is down (F5 statistics).



F5 device status mapping to Orion status





We mapped the status icons used for F5 devices to Orion Platform icons. For explanation of F5 statuses, see [F5 support help online](#).

F5 STATUS	ORION STATUS
 Available	 Up
 Unavailable	 Warning
 Down	 Down
Disabled  (error)  (unlicensed)	Unmanaged  (disabled on F5)  (unreachable)
 Unknown	 Unknown

F5 status in Orion

The table explains what the Orion statuses mean for individual components in the load balancing hierarchy. Status is usually polled on devices, but for some components, such as GTMs and LTMs, it is calculated based on polled values for their child objects.

STATUS	LOAD BALANCING COMPONENT						
	SERVICE	GTM	LTM	VIRTUAL SERVER (VS)	POOL	MEMBER	F5 SERVER
	Reported on the device	All services assigned to the GTM are up	All virtual servers are up	F5 device reports the VS as up	F5 device reports the pool as up	F5 device reports the pool as up	F5 device reports the server as up
	Reported on the device	At least one service is not up	At least one virtual server is not up	Unavailable based on connection limit	No members are currently available	Unavailable based on the connection limit	Unavailable based on the connection limit

STATUS	LOAD BALANCING COMPONENT						
	SERVICE	GTM	LTM	VIRTUAL SERVER (VS)	POOL	MEMBER	F5 SERVER
	Reported on the device	All services are not up	All virtual servers are not up	Associated objects marked the VS as unavailable. User action necessary	All members are unavailable	The parent F5 server is down or the monitor on the member marked it as down	Down based on monitor
	-	-	-	Unmanaged: Disabled on the F5	-	Unmanaged: Disabled on the F5	Unmanaged: Disabled on the F5
	-	-	-	Unreachable: Parent LTM is down	Unreachable: Parent LTM is down	Unreachable: Parent LTM is down	-
	Reported on the device	GTM is added but not polled yet	LTM is recognized by GTM, but not managed in Orion	Unknown	Unknown	No monitors assigned	No monitors assigned

F5 high availability

High availability (H/A) is configured on the device level. It does not matter whether you have a GTM or LTM installed on the device, the module is covered by H/A. Devices are connected in traffic groups. If one device fails, another device in the group handles its requests. Devices in a traffic group synchronize the configuration. The configuration is reflected by the synchronization status.

In SolarWinds NPM, we poll the failover and synchronization status.

Devices in one traffic group are connected by dotted rectangles on the Balancing Environment resources. Display the tooltip to see details about the H/A failover and synchronization status.

Balancing Environment

Search whole environment

SERVICES (25)

GLOBAL TRAFFIC MANAGERS (6)

LOCAL TRAFFIC MANAGERS (6)

VIRTUAL SERVERS (29)

Warning
One or more Services are not Up.

Role	Global Traffic Manager
Status	Warning
Status Reason	One or more Services are not Up.
IP Address	[Redacted]
Hosting Node	[Green Dot]
H/A Status	Standby and In Sync
Requests/s	518

You can see the H/A statuses in tooltips, and on the LTM or GTM detail views. The GTM or LTM details resource shows the H/A status and synchronization status. In the High Availability resource, you can check the details about other members of the traffic group.

Global Traffic Manager Details

EDIT HELP

STATUS

Warning

STATUS REASON

One or more Services are not Up.

POLLING IP ADDRESS

HOSTING ORION NODE

H/A STATUS

Standby

H/A SYNC STATUS

In Sync

High Availability

EDIT HELP

NAME

POLLING IP

H/A STATUS

SYNC STATUS

Active

In Sync

F5 health monitors

To monitor the health of your load balancing environment, SolarWinds NPM polls health monitors on your F5 servers (nodes), and on F5 pool members. Health monitors run periodic tests for network service availability, such as ICMP, HTTP, IMAP, or MSSQL.

To get the health statistics, [F5 iControl API must be enabled](#).

F5 health monitors are not related to hardware health. The status of an element is based on health monitors polled by F5 iControl API.

Go to a pool member or an F5 server details page to review the health monitors resource.

Pool Member Health Monitors

EDIT HELP

MONITOR NAME

TYPE

PORT

STATUS REASON

icmp

ICMP

0


-

sw_web_http

HTTP





80

Unable to connect. No successful responses received before deadline.

 Health monitors require at least one pool member to be up. If no pool members are up, the LTM, the virtual server, and the pool will all be marked as down. Drill down into the pool member to see why it is down.

Events, alerts, and reports for Network Insight for F5® BIG-IP® load balancers

Each F5 details page includes the F5 Events resource that displays events relevant for the object. Click an event to go to the details page for the object with issues and review the situation.

F5 Events		EDIT HELP
LAST 12 MONTHS		
ACTIVITY	TIME	
 Pool [redacted] on F5 device [redacted] is Down.	4/21/2016 4:02:53 PM	
 F5 server [redacted] is Unknown.	4/21/2016 3:58:33 PM	
 F5 server [redacted] is Unknown.	4/21/2016 3:58:24 PM	
 F5 pool [redacted] has 0% of active servers. The alert triggers when less than 30% servers are active.	4/21/2016 1:50:44 PM	

Load balancing events include:

- A component status changes to down
The components include virtual IP, Pool, Server, Wide IP, GTM, or servers.
- Health probe status changes up and down
- H/A peer status or synchronization change
- Server is taken out and placed in rotation
- Concurrent connections per pool member exceed a threshold

Out-of-the-box alerts for F5 load balancers

Out-of-the-box alerts cover the most critical issues in your F5 load balancing environment. For example, alerts warn you if the status of your F5 service changes or if a server goes down.

Out-of-the-box reports

SolarWinds NPM includes several out-of-the-box reports for F5 that you can use to view trends, establish baselines, or identify potential issues, such as:


- Average LTM Connections over the last 30 days
- Average service availability over the last 30 days
- Average service resolutions per second over the last 30 days

Take an F5 pool member out of rotation

When you need to perform maintenance on one of the pool members providing a service, take the server out of rotation so that you can perform maintenance without impacting end users.

Taking server out of rotation means you put the pool member in maintenance mode.

F5 devices support Disabled and Forced Offline modes. SolarWinds NPM uses the Disabled maintenance mode.


 Taking a pool member out of rotation requires that you have [enabled F5 iControl on the device](#).

Why shouldn't I start maintenance immediately after I take a pool member out of rotation?

When you put a pool in maintenance mode, there are still users connected to the server. Disabling the server only disables brand new connections.

The maintenance mode only changes how the LTM handles incoming requests.

- New users are not sent to the server while the servers is in maintenance mode.
- In the Disabled mode, new connections with existing sessions are not affected. Users who open a new TCP session but were previously using the server, will continue to be sent to this server.
- Existing connections are not affected. Users with an open TCP session with the server will continue to use it.

 SolarWinds recommends that you wait until the existing connections end or time out not to impact the connected users.

Take a pool member out of rotation

1. Click My Dashboards > Network > Load Balancing, and locate the parent pool of the pool member.
2. Click the parent pool, and click Display Details Page.
3. On the Pool Details view, find the Pool Members resource, and click Change Rotation Presence.

4. Click the green check mark icon next to the pool member to remove it from rotation, and click Submit.

Change Rotation Presence

Remove or add pool members from / into rotation.

MEMBER

QA-BRN-PSTI-03

QA-BRN-PSTI-05


QA-BRN-PSTI-02

QA-BRN-PSTI-04

Scheduled maintenance

Displaying members 1-4 of 4

Note:

 Add a reason for taking the pool member out of rotation in the Note field. An info icon will appear next to the pool member, and your note will be displayed as a tooltip when you hover over the info icon.

The pool is removed from rotation now. To prevent user impact, watch the connection count for the pool member. It should decline over time as existing users finish their sessions and no new users are added. After the connection count has become low, you can begin maintenance.

Monitor wireless networks

SolarWinds Network Performance Monitor can monitor any 802.11 IEEE-compliant autonomous access point (AP) or wireless controller, and provide details about access points (AP), wireless clients, wireless controllers, thin APs, and rogue APs.

SolarWinds NPM automatically recognizes your wireless APs and controllers as wireless devices when they are added to the SolarWinds Orion database. See [Discover and add network devices](#).

The wireless interfaces are not found during discovery process. When a wireless device is added and an inventory search is performed, each wireless interface found is added to the database and polling begins.


Migrate data from the Wireless Networks Module

If you have already used an earlier version of the Wireless Network module to poll your wireless devices, historical data will automatically be migrated to the new format.

- The wireless migration is performed in batches during scheduled database maintenance.
- The migration will notify users when a node is migrated and when all nodes have been migrated in the event log.
- You will not see historical data immediately because this process is throttled.


View wireless data in the Orion Web Console

The Wireless Summary view displays a list of all wireless access points (APs) and clients connected to each AP.

 You can display the coverage of your wireless access points or the location of connected clients in a map. See [Create wireless heat maps](#) and [View the location of clients connected to access points in maps](#).

Access point details include the AP name, 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 IPv6 statistics are currently not monitored:

- Connections between wireless users and access points
- Connections between thin access points and controllers


To view wireless access points and clients:

1. Log into the Orion Web Console.
2. Navigate to Wireless Summary View through My Dashboards > Wireless in the Network menu.
3. In the Show list, select what you want to see (Access Points or Clients).
4. To find an access point or client, type a search string into the Search field, and click Search. If there are too many items, select a Group By method to filter the result.
5. To see clients currently connected to an access point, locate the access point, and expand the access point name.
6. To display the details view for an access point, click the access point. The node details view is specific for the selected device. See [Specify views for device types](#).

Monitor EnergyWise devices


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 enabling the energy-saving features of EnergyWise-capable devices, 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.

In the Orion Web Console, you can consult the EnergyWise Summary view and related resources to help you monitor the energy expended on your network and the energy savings provided by EnergyWise-enabled devices.

-  ■ Fully upgrade the IOS of all EnergyWise-enabled devices on your network. For more information, consult your device documentation or www.cisco.com.
- If the EnergyWise Summary view does not display in the Orion Web Console menu bar, see [Add the EnergyWise Summary View to the Orion Web Console menu bar](#).

Add the EnergyWise Summary View to the Orion Web Console menu bar

1. Log in to the Orion Web Console as an administrator.
2. Click My Dashboards > Configure.
3. Click Edit beneath the menu bar to which you want to add the EnergyWise Summary view.
4. Drag the EnergyWise button from the Available items list on the left to the correct location in the Selected items list on the right.

 Selected items display from left to right in the selected menu bar as they are listed from top to bottom.


5. Click Submit.

Temporarily reset the current power level of a monitored EnergyWise interface

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.


To remotely reset the current power level of an interface, the parent node must have not only Community String, but also Read/Write Community String set correctly. See [Edit polling settings](#).

Policies are configured either manually on the monitored device itself or with a configuration management utility, such as SolarWinds NCM. See www.solarwinds.com.

-  Some Cisco IOS versions report EnergyWise levels as values 1–11 instead of 0–10. In SolarWinds NPM 10.1.2 and later versions, the levels are automatically corrected. IOS's on some devices are not affected by this issue.

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > Manage Nodes.


3. Locate the device to edit:
 - Use the search tool above the node list to search your database for the parent node of the EnergyWise interface entity you want to reset.
 - Select a Group By option, and click the group including the parent node of the EnergyWise interface entity you want to reset.
4. Expand the parent node, and select the interface entity.
5. Click More Actions > Override Power Level.
6. Select a power level, and click OK.

 To reset the current power level, you can also go to the Interface Details view, and click Set Power Level in the EnergyWise Interface Details resource.

Set up and monitor Cisco Unified Computing Systems (UCS)

To gain an overview of all information provided by UCS, add the UCS master device, and the primary fiber interconnect devices into the SolarWinds Orion database for monitoring.

1. Confirm that LDAP authentication is not enabled on your UCS device. See the device documentation for details.
2. Verify in the UCS console that the fiber connects have external IP addresses.
If the external gateway, external IP address, or external mask are set to 0.0.0.0, edit them with values valid for external devices.
3. Add the UCS Master node to the database.

 If the node shows up in the All Nodes list in italics or with 'n/a' as the state, click on it, and click Yes to add the device.

- a. Click Manage Nodes in the All Nodes resource if the node is not in the list.
 - b. Click Add Node. Provide the IP Address, or provide the host name and select Dynamic IP Address.
 - c. Select External Node or Status Only: ICMP as the polling method.
 - d. Select UCS Manager Credentials, and provide the credentials.
 - Polling Engine
 - UCS Port
 - UCS User Name
 - UCS Password
 - e. Click Test under the UCS fields, and click Next.
 - f. Select the resources to monitor on the node.
 - g. Add relevant pollers.
 - h. Review your information, and click OK, Add Node.
4. Add each UCS fabric interconnect switch and blade device. Repeat step 3 for each device.
 5. Double-click on the UCS Master node in All Node, and find the UCS Overview resource.

 To select the proper view we use the existing View By Device Type feature.


To ensure that Standard Poller does not overwrite MachineType and other fields, we use EntityType to identify UCS node in the Standard Poller (and so force Standard Poller not to overwrite our required fields). This same mechanism is also used for the ESX VMWare API.

6. If any UCS device shown in the UCS Overview is not currently managed, double-click the device, and add the node.

Monitor Cisco[®] SwitchStack[®]

With SolarWinds NPM, you can view the health of individual Cisco SwitchStack members, monitor power and data connections between the members, and quickly locate a switch with issues.

Out-of-the-box events and alerts notify you when a member, or a connection between members goes down.

 [Add the Cisco SwitchStack for monitoring](#) as a node. The IP address is always assigned to the master switch (highlighted with a crown icon).

View stack members and rings

When you receive an alert about a SwitchStack problem, go to the SwitchStack node details page, and click the SwitchStack subview.

The subview provides member-specific monitoring with topology maps showing how the data ports and power ports are connected, and information to pinpoint switches with issues.

You can quickly see which switch is having issues, locate it by serial number in the stack, and replace it or resolve the issue.

>>

Home

Dashboard

Network

Switch Stack

+

Node Details - [redacted] - Switch Stack

Switch Stack Members

EDIT HELP

SWITCH	PRIORITY SW	HW	MODEL	SERIAL NUMBER	MAC ADDRESS	RAM	CPU
Switch #1	15	0	WS-C3850-48P	[redacted]	[redacted]	38.76%	2%
Switch #2	10	0	WS-C3850-48P	[redacted]	[redacted]	38.33%	1%

Stack Power Ring

EDIT HELP

RING NAME

Powerstack-1

REDUNDANCY RUNNING

Power sharing

```
graph LR; S1[Switch #1] --- P1((#)); S1 --- P2((#)); S2[Switch #2] --- P1; S2 --- P2;
```

View the health of stack members








When you are monitoring hardware health on a Cisco SwitchStack node, you can see the health of individual switches in the stack. The health indicators inform you when the values on a switch are near the safe limits, or when they reach the critical stage.


1. Log in to the Orion Web Console, and go to the SwitchStack node details page, and click the Network subview.
2. Consult the Current Hardware Health resource.

3. Expand a switch in the stack to display hardware health monitors.

Current Hardware Health

MANAGE SENSORS EDIT HELP

DEVICE NAME	STATUS	VALUE
▼  Switch 1	 3	
▶  Fan		
▶  Power Supply		
▶  Temperature		
▶  Switch 2	 3	

 The item in the Status column describes the number of sensors monitored on the switch, grouped by the status of the sensor.

You can now troubleshoot the SwitchStack member that is experiencing issues.

See also [Monitor hardware health](#).

Cisco SwitchStack events

Events for Cisco SwitchStack include messages about the following issues and changes:

- Stack ring redundancy loss
- Stack ring failure
- Members being added or removed
- Member number changes
- Master switch changes
- Power redundancy loss
- Power capacity change

Out-of-the-box alerts for SwitchStack


Out-of-the-box SwitchStack alerts inform you about the following items and more:

- SwitchStack Master Changed
- SwitchStack Data Ring Broken
- SwitchStack Member Number Changed
- SwitchStack Power Redundancy Lost

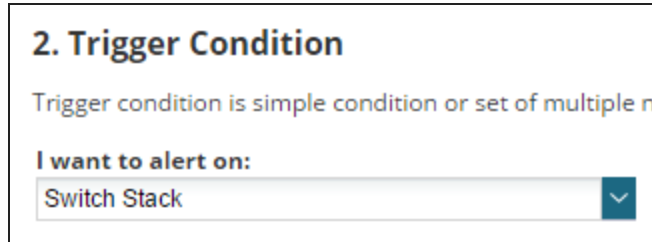
 Not all out-of-the-box alerts are turned on by default.

Create alerts based on SwitchStack events

You can [configure additional notifications](#) based on SwitchStack events. For example, you can specify that when a stack ring fails, you want to receive an email with details.

 Out-of-the-box alerts cover the most frequent issues. Review available alerts and [duplicate and edit the alerts](#) if you only need small adjustments.

1. Select Alerts & Activity > Alerts, and click Manage Alerts.
2. Click Add New Alert.
3. On Trigger Condition, select the SwitchStack item you want to alert on.



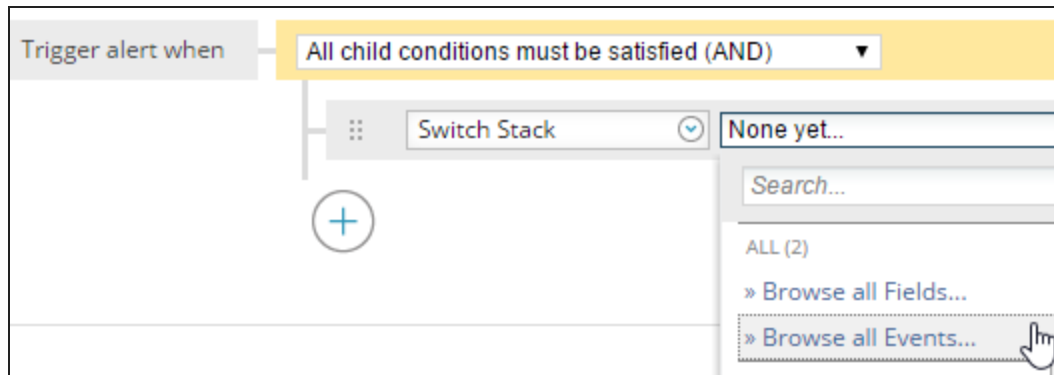
2. Trigger Condition

Trigger condition is simple condition or set of multiple n

I want to alert on:

Switch Stack

4. In Trigger alert when, select a condition, click the arrow in the second box next to the selected SwitchStack object, and select Browse all events.



Trigger alert when

All child conditions must be satisfied (AND)

Switch Stack

None yet...

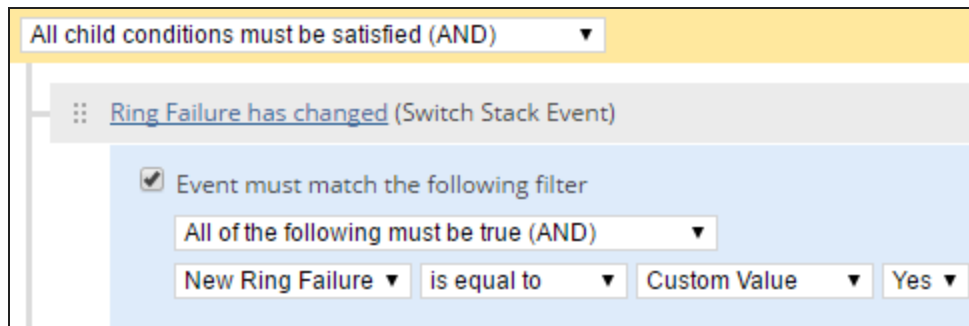
Search...

ALL (2)

» Browse all Fields...

» Browse all Events...

5. Select the event you want to alert on and if necessary, complete the trigger condition.
For example, if you want to be notified about a SwitchStack ring failure, select the Ring Failure event, select Event must match the filter, and then select New Ring Failure is equal to Yes.



All child conditions must be satisfied (AND)

Ring Failure has changed (Switch Stack Event)

☒ Event must match the following filter

All of the following must be true (AND)

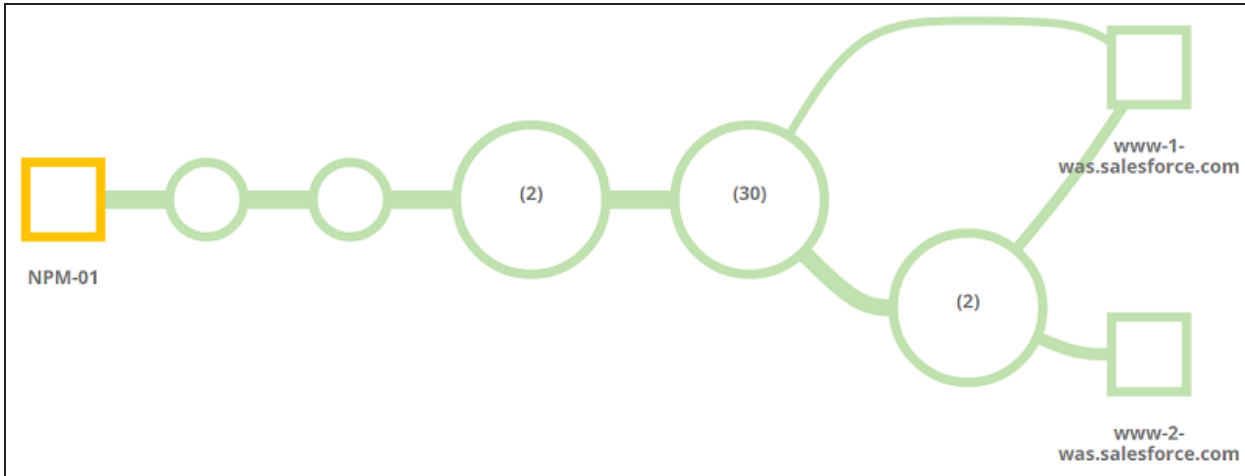
New Ring Failure is equal to Custom Value Yes

6. [Specify the trigger action](#) and complete the wizard.

After the trigger condition occurs, you will be notified about it both by the event and the trigger action you specified.

Discover your network paths

SolarWinds NPM 12.0 introduces a new feature called NetPath™. NetPath™ helps you identify network problems faster by automatically creating a map of the problem area, and enriching it with a wide variety of supporting information. NetPath™ displays the performance details of devices inside and outside of your network.



Key features of NetPath™

- NetPath™ discovers the hop-by-hop network path.
- NetPath™ quantifies the performance of each link and node along the path.
- NetPath™ isolates the node or connection that is decreasing end-to-end performance.
- If the issue is external, NetPath™ identifies the name of the company that owns the node and displays their contact information.
- If the issue is internal, NetPath™ incorporates data from SolarWinds NPM, NCM, and NTA about your on-premises gear.

How does NetPath™ work?

NetPath™ uses distributed monitoring and path analysis to discover how applications are delivered through the network to your users. To use NetPath™:

1. You deploy agents on Windows computers that act as synthetic users. The agents use advanced probing to discover and test the network path that traffic takes to any network endpoint, such as your local file print server, your website, or external websites.
2. After discovering the path and quantifying the performance of each hop and connection, NetPath enriches the picture with additional data about Internet nodes. If you are monitoring non-Internet nodes with Orion, NetPath™ incorporates that data too.
3. The result is a clear end-to-end map of how applications are delivered to your users, including your network, the network of your provider, and any other networks you depend on.

NetPath™ answers the following questions:


- How well is my network delivering applications to my users?
- Are the paths to key applications or users down?
- Where is the network problem and who is responsible for it?

NetPath requirements

Probe computer

Probes are the source of network paths, and the paths are discovered by probes.

You [create a probe](#) on a source computer, which must meet the following requirements:

TYPE	REQUIREMENTS
Operating system (64-bit only)	Windows Server 2008 R2 SP1 Windows Server 2012 Windows Server 2012 R2 Windows 7 Windows 8 Windows 8.1 Windows 10 Professional and Enterprise <div> Windows 10 Home edition is not supported.</div>
CPU cores	2 CPU cores for 20 paths +1 CPU core per 10 additional paths
Hard drive space	1 GB
RAM	2 GB

Orion integration

NTA 4.2 and NCM 7.4.1 are the minimum required versions to use the [Orion integration features with NetPath](#).

Ports

Open the following ports on your firewall for network connectivity used by NetPath™:

PORT OR CODE	SOURCE	DESTINATION	PROTOCOL	DESCRIPTION
17778	NetPath™ probe	Orion polling	TCP	Used to send information back to your SolarWinds Orion server.

PORT OR CODE	SOURCE	DESTINATION	PROTOCOL	DESCRIPTION
		engine		
11	Networking devices along your path	NetPath™ probe	ICMP	Used by the NetPath™ probe to discover network paths.
User configured	NetPath™ probe	Endpoint service	TCP	Any ports of the monitored services that are assigned to the probe. Used by the NetPath™ probe to discover service status.
43	NPM polling engine	BGP data providers	TCP	Used by NetPath™ to query IP ownership and other information about the discovered IP addresses.

Database storage

When calculating the size requirements in SQL Server for NetPath™, you must account for the probing interval and the complexity of the network path from the probe to the monitored service. The complexity of the path is divided into three groups:

- Internal: services with fewer than 10 hops between the probe and the monitored service.
- Intermediate: multiple paths ending in a single endpoint node. Examples are github.com, linked.com, and visualstudio.com.
- Complex: multiple paths (over 20) ending in multiple endpoint nodes. Examples are google.com and yahoo.com.

This table provides an estimate in megabytes (MB) of the amount of storage consumed by SQL Server over a 30-day period (the default retention time) when monitoring a single service.

INTERVAL (IN MINUTES)	INTERNAL (IN MB)	INTERMEDIATE (IN MB)	COMPLEX (IN MB)
1	520	1105	1615
2	325	645	1145
3	200	445	915
4	170	350	750
5	135	265	480
10	80	175	470

Example storage requirement calculation

Your monitoring setup contains the following:

- Five internal monitors with a one-minute interval.
- Three intermediate monitors with a five-minute interval.
- Four complex monitors with a ten-minute interval.

The total storage requirement for SQL Server can be calculated as:

$(5 \times 520) + (3 \times 265) + (4 \times 470) = 5275$ MB over a 30-day time period.

Cloud environment

When you place a probe in a public cloud, consider the following additional requirements:

PROVIDER	REQUIREMENTS
Amazon	<ul style="list-style-type: none"> ■ Security group must be enabled on instances that host NetPath™ probes to allow inbound ICMP packets. ■ Probing services that host on Amazon Web Services (AWS) instances within the same cloud networks may not work.
Azure	<ul style="list-style-type: none"> ■ Private Internet Protocol (PIP) must be enabled on instances that host NetPath™ probes. ■ Probing may work within VNET, but may not work if the path crosses the Azure Load Balancer.

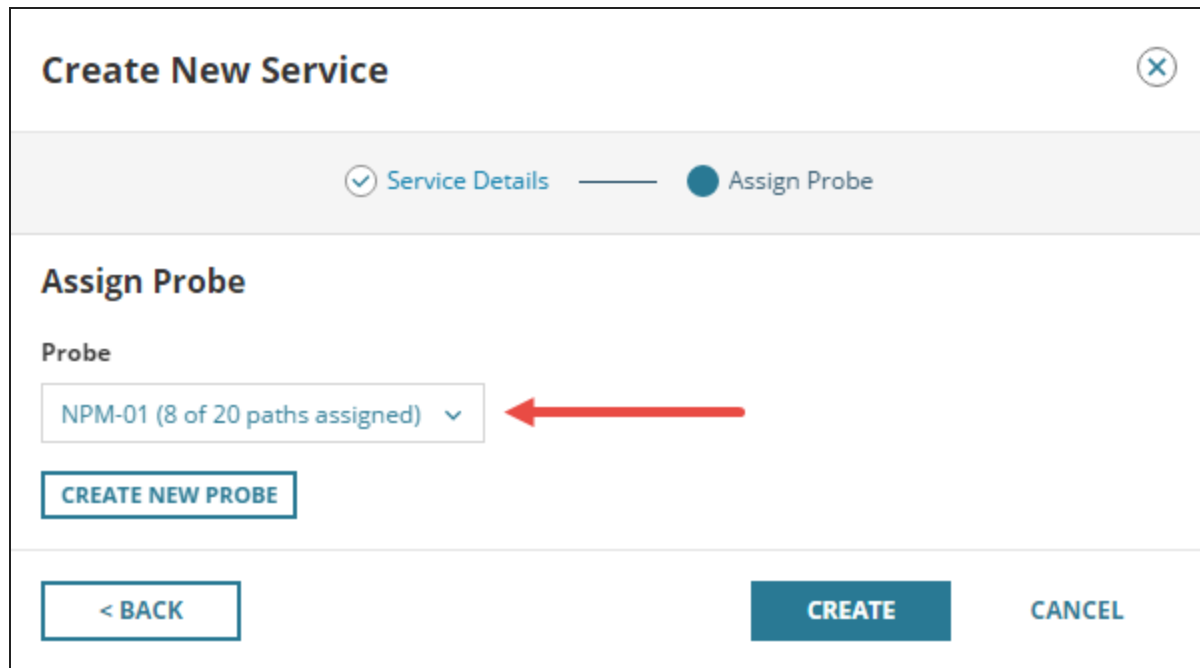
Scalability

The scalability of NetPath™ depends on the complexity of the paths you are monitoring, and the interval at which you are monitoring them.

In most network environments:

- You can add up to 100 paths per polling engine.
- You can add 10 - 20 paths per probe.

NetPath™ calculates the recommended path count based on the performance of each probe, and displays it each time you deploy a new path to the probe.



The screenshot shows a 'Create New Service' dialog box with a close button (X) in the top right corner. Below the title bar, there are two tabs: 'Service Details' (selected with a checkmark) and 'Assign Probe' (indicated by a blue dot). The 'Assign Probe' section has a title 'Assign Probe' and a label 'Probe'. Below the label is a dropdown menu showing 'NPM-01 (8 of 20 paths assigned)' with a downward arrow. A red arrow points to this dropdown menu. Below the dropdown is a button labeled 'CREATE NEW PROBE'. At the bottom of the dialog, there are three buttons: '< BACK', 'CREATE', and 'CANCEL'.

Create a service

A service is the destination to which you are mapping. It represents an application, and SolarWinds recommends deploying a service for the most important applications that your users rely on. This can be any TCP-based network service, such as salesforce.com, Microsoft Exchange, Office365, or a file server.


NetPath™ services are monitored by probes. Orion automatically installs a probe on each polling engine, and you can install a probe on any Windows computer. No other software is required on the path.

Create a new service


1. Click My Dashboards > Network > NetPath Services.
2. Click Create New Service.

3. Enter the service details of the target destination of your network path. The service must be TCP-based.

- a. Enter a host name or IP address and port.

 SolarWinds recommends using the same information that your users access the application by. For example, if they access your internal site by a host name rather than an IP address, enter the host name in NetPath™. That way NetPath™ gets the same service as your users.

- b. Enter the probing interval in minutes.

 SolarWinds recommends starting with a 10-minute interval. See the Probing interval section below to learn how to adjust the probing interval.

- c. Click Next.

4. Select an existing probe from the list, or [Create a probe](#) to use a new source.

5. Click Create.

Probing interval

This value determines how often and how long information is polled from the network path. If the value is too low, NetPath™ does not complete the probe and the network path may not show all routes. If the value is too high, the information may not update as frequently as you like.

- If you probe more frequently, the data updates quicker but accuracy is lost. If this happens, NetPath™ identifies it as an issue on the probe displayed in the graph.
- If you probe less frequently, the data updates more slowly but the accuracy of the data increases.

SolarWinds recommends starting with a probing interval of 10 minutes, which is appropriate for most paths. You can adjust the value from there to suit your needs.


Is your network path internal? Does it contain fewer than 10 nodes? If so, you can decrease the interval for more frequent data updates.

Is your network path external and does it contain internet connections? Does it contain more than 10 nodes? If so, you can increase the interval for less load strain on the Orion server, your nodes, and the network. A larger value also saves storage space by writing less NetPath™ data to the database.

Create a probe


NetPath™ services are monitored by probes. Orion automatically installs a probe on each polling engine, and you can install a probe on any Windows computer. No other software is required on the path.

A probe is the source you are testing from. It is always the start of the path. Think of a probe as a representative of a user. SolarWinds recommends deploying probes where you have users, for example at each of your office locations.

 The probe must be a Windows computer.

Create a probe

You can create a probe when you [create a service](#), or while assigning an additional probe after you create the service:

1. Click My Dashboards > Network > NetPath Services.
2. Click  next to an entry in the NetPath Services list.
3. Click Create New Probe.
4. Enter the required information on the Create New Probe window.

 Enter the credentials that can be used to log in to the computer and install the software.

5. Click Create.
6. Select the probe from the list.
7. Click Assign.

Assign additional probes

Click  next to an entry in the NetPath™ Services list to assign another probe to the service.

Probe troubleshooting


If you are creating a probe on an existing Orion Agent, you must enter the primary polling IP address used by Orion for that device.

Check the probe status

If you have other issues with probe deployment, you can check the probe status.

Probes are listed in the Manage Agents section of Agent Management. The NetPath™ probe relies on the Agent infrastructure built into Orion and used for things like QoE and SAM Agents. NetPath™ is an additional plugin in this agent framework.

1. Click Settings > All Settings.
2. Under Node & Group Management, click Manage Agents.
3. Locate the probe in the Agent/Node list by its host name, and select it.
4. Verify the Agent Status is Running, and that the Connection Status is Connected.

 If the Agent is not running or connected, see the Probe troubleshooting section below.

5. Click More Actions > View installed agent plugins.
6. Verify the NetPath™ Agent Plugin is installed.

You can also click Edit Settings to change the configuration of the probe, or Delete to remove it.

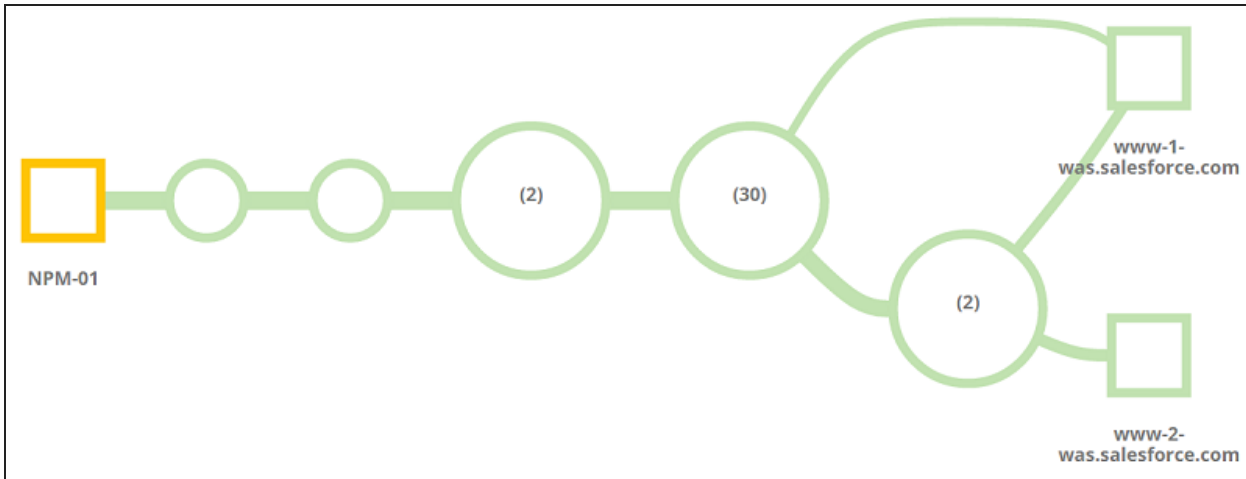
View a network path

1. Click My Dashboards > Network > NetPath Services. This view displays a list of created network services.

2. Expand a service, and click one of the associated probes to see the network path from that probe to the expanded service.

Path layout

The source is on the left and the destination is on the right. The network path is everything in the middle.

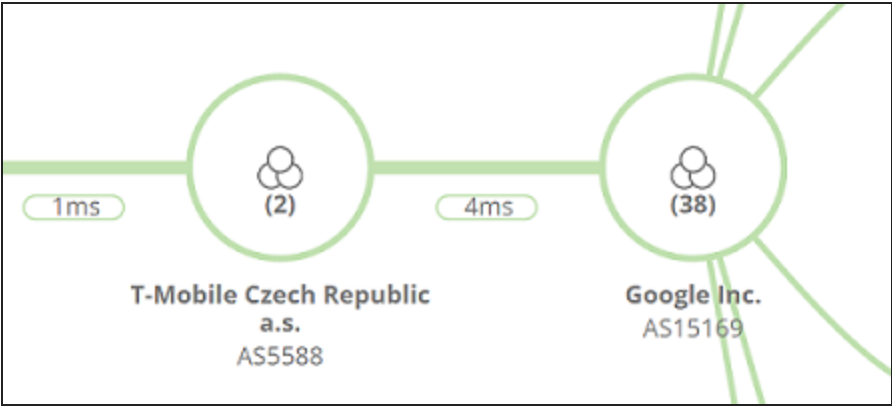


Use the controls in the upper left to change the zoom, detail levels of the path, and the amount of information displayed. You can also use your mouse to pan and zoom.



Objects in the network path include nodes, connections, and interfaces. Point to an object for a summary, and click it for details.

NetPath™ groups nodes into networks represented as larger circles. In the example below, the path goes through two (2) nodes in T-Mobile's network and 38 (38) nodes in Google's network.



Click the network to show the nodes that comprise it, and click the X on the Expanded filter to collapse it.

NPM-01 to Google | Network Path
SOURCE:NPM-01 | DESTINATION:www.google.com | PORT:443

+

-

⌵

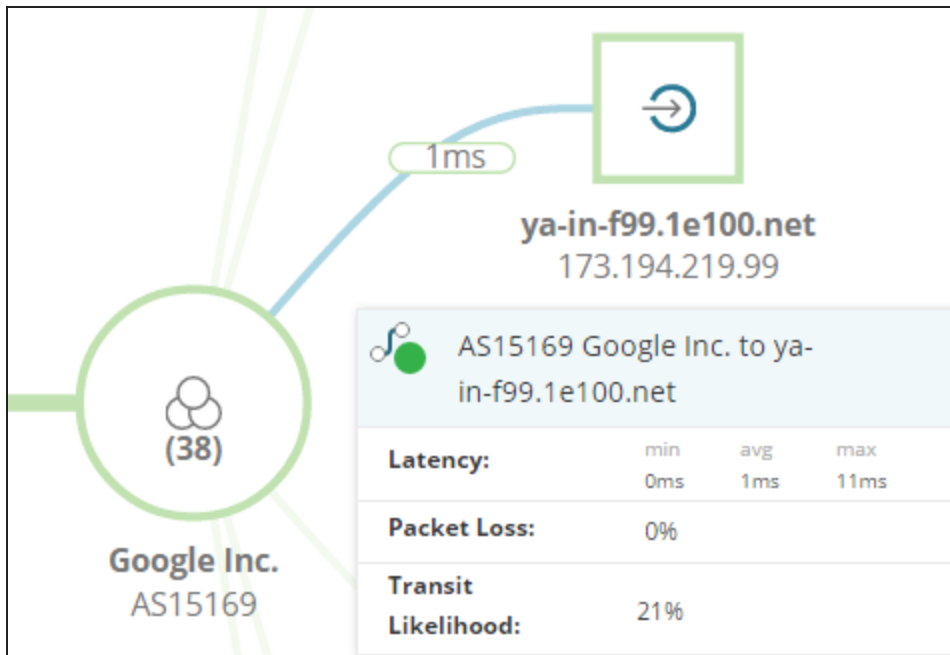
EXPANDED: Google Inc. (40)

The node information is cumulative from the source to that node. When you point to or click a node, the displayed metrics answer the question, “what is the performance between the source, along the path, up to this node?”

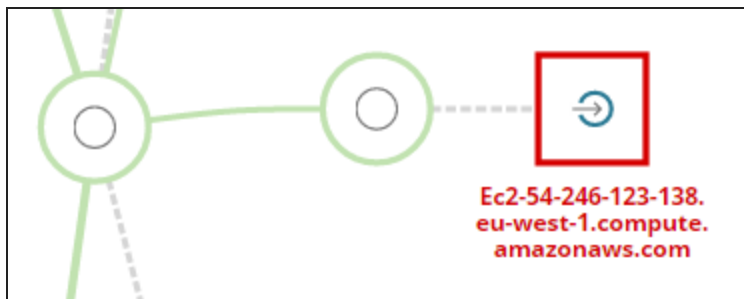
ya-in-f99.1e100.net
173.194.219.99

ya-in-f99.1e100.net 173.194.219.99			
Latency:	min	avg	max
	120ms	124ms	144ms
Packet Loss:	0%		
Owned by:	Google Inc.		
Prefix:	173.194.219.0/24		
Originated by:	AS15169 (Google Inc.)		

A connection between nodes shows latency and packet loss between its two nodes. When you point to or click a link, the displayed metrics answer the question, “what is the performance of this specific link?”



A dotted line illustrates a broken connection to a host that is unreachable. This means that traffic reached the green node, is destined for the endpoint connected with the dashed line, but does not make it.

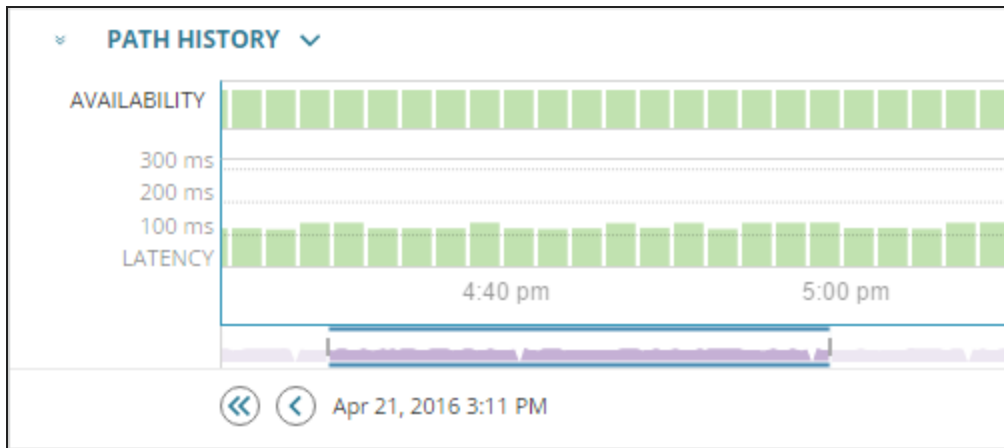


Use the green, yellow, and red color coding to identify the nodes and connections that may be performing poorly and affecting the end-to-end connection. If you confirm that a service provider is responsible for the outage, you can contact them to resolve the issue.

Path history

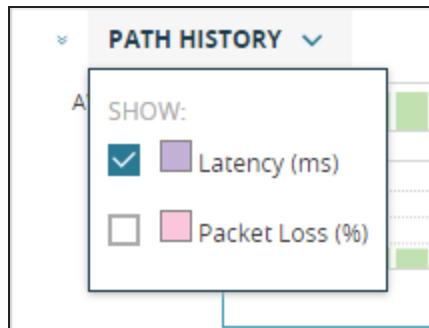
The chart on the bottom shows metrics for the end-to-end performance. Select an interval to see the network path and its performance that resulted in that end-to-end performance.

Think of this as your network time machine. You can compare performance metrics from today or a previous time.



Available actions in the path history

- Click a bar in the chart to load the network path from that date and time.
- Click the single arrows, or press the Left and Right Arrow keys, to move one interval at a time.
- Click the double arrows to move to the beginning or the end of the displayed history window.
- Drag the bottom slider to change the history window.
- Click Path History to show or hide Latency and Packet Loss in the chart.

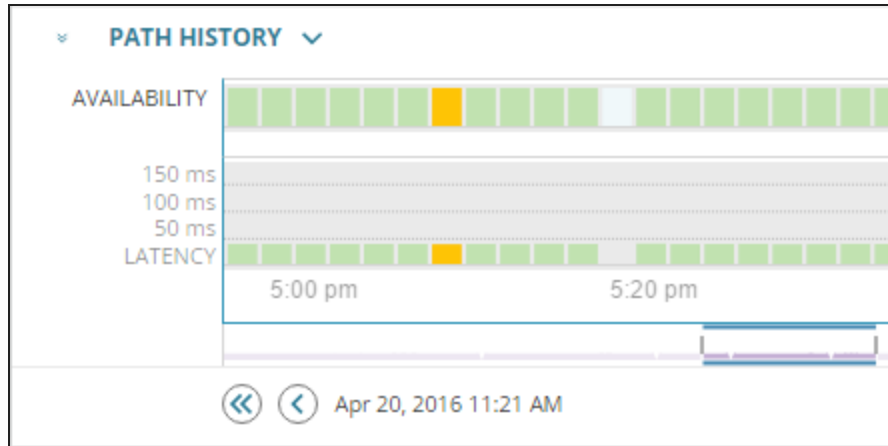


Troubleshoot a service with external path data

You can use NetPath™ to diagnose a slow connection to an external service. This example uses amazon.com.

1. Click My Dashboards > Network > NetPath Services.
2. Expand the service that your users reported as slow or unreachable.
3. Click the probe from the office or location that reported the issue.

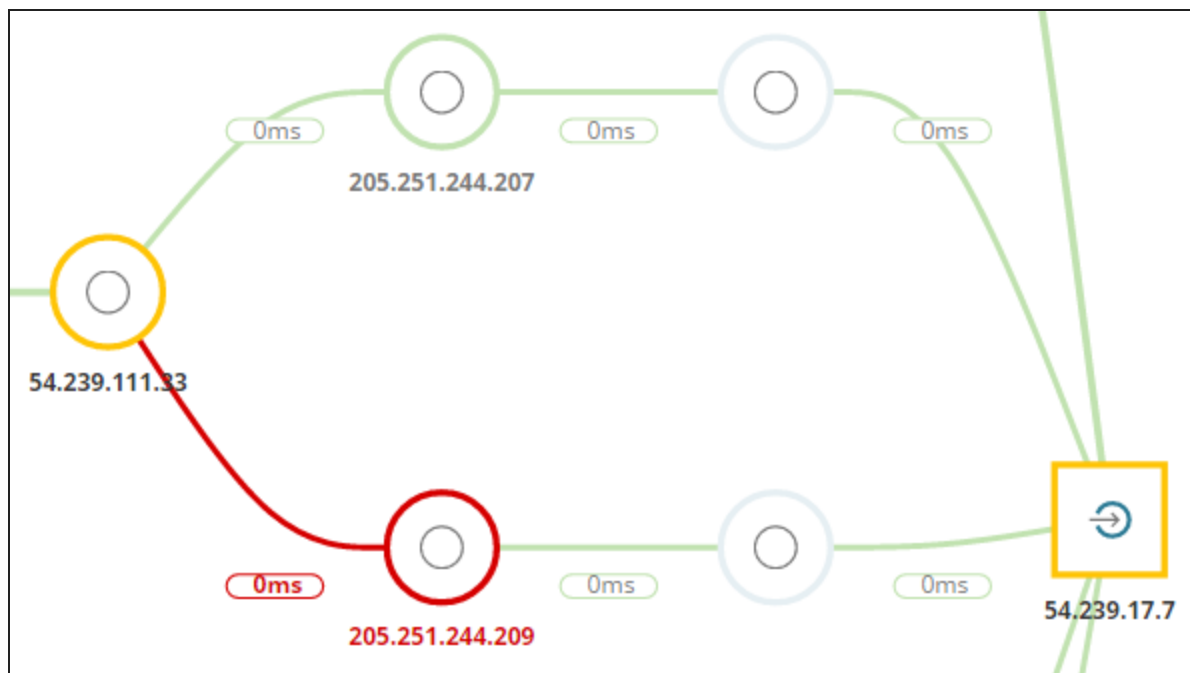
4. Under Path History, locate the date and time for when your users reported the issue. Here, there is a yellow warning entry at 5:09 p.m. on April 20.



5. Click the yellow bar at 5:09 p.m. in the chart.
6. The problem is in Amazon's network. Click the red Amazon node to expand it.

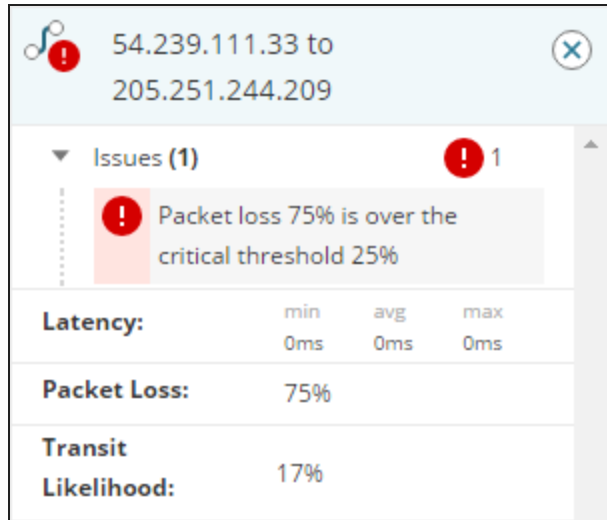


7. Although Amazon's network is large and complex, you should investigate the red and yellow areas.



8. Click the red connection between the two nodes to open the inspector panel.

- Expand the Issues section to see that packet loss is over the critical threshold, and that it is 17% likely that transit passed through this link.

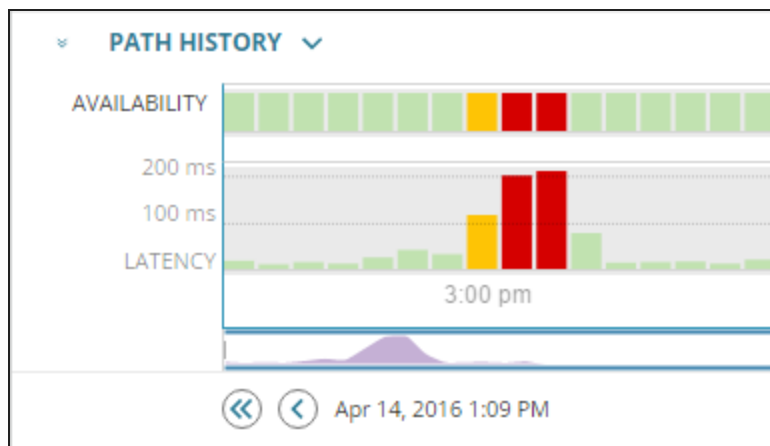


- Click the red 205.251.244.209 node to open the inspector panel.
- Use the phone number or email address to contact the service provider and report the issue.
Present the following information to resolve the issue:
 - IP addresses of the nodes in question (54.239.111.33 and 205.251.244.209 in this case)
 - Date, time, and duration of the performance issue
 - Latency and packet loss information

Troubleshoot my network with Orion path data

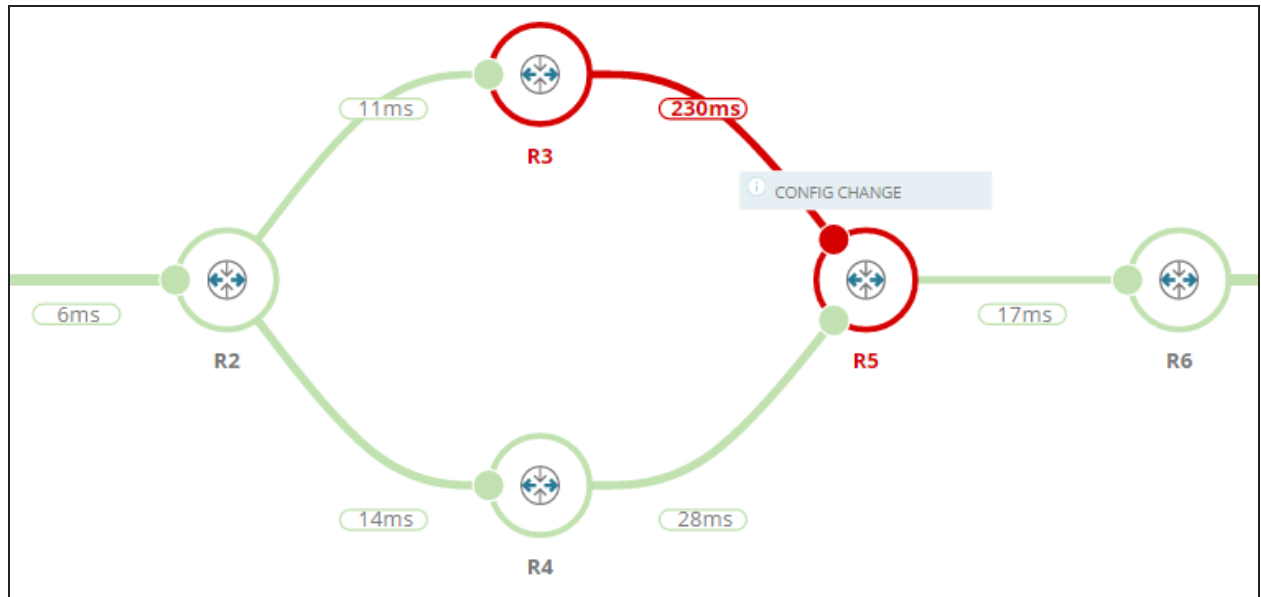
You can use NetPath™ to diagnose a slow connection caused by your internal network. This example shows a node that stopped working properly after a change to its config file.

- Click My Dashboards > Network > NetPath Services.
- Expand the service that your users reported as slow or unreachable.
- Click the probe from the office or location that reported the issue.
- Under Path History, locate the date and time for when your users reported the issue. Here, there is a red critical entry at 3:26 p.m. on April 14.

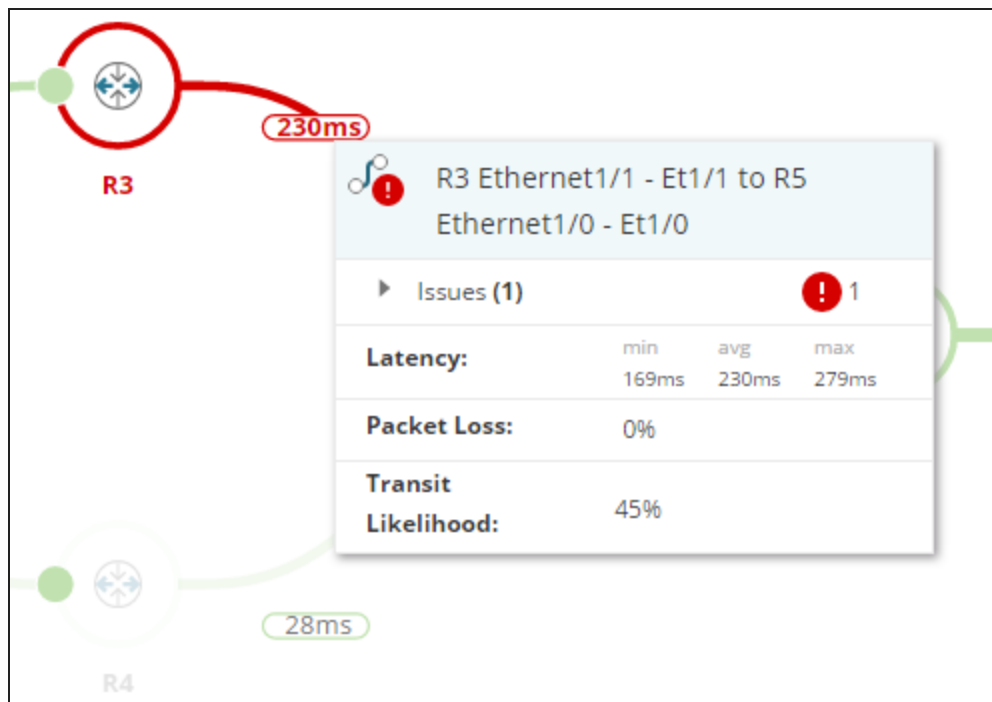


- Click the red bar at 3:26 p.m. in the chart.

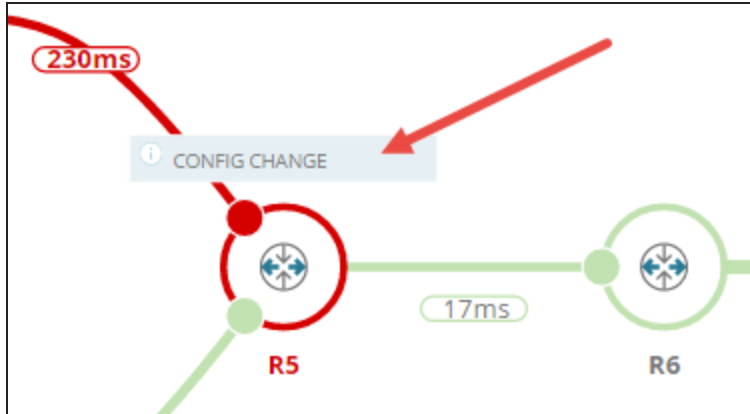
6. The problem is in the internal network. There is a high latency between nodes R3 and R5.



7. Point to the red connection between the two nodes to see that Transit Likelihood is 45%. This means that just under half of your users are likely to experience the problem.



8. NCM is installed, so the [Orion integration with NetPath](#) displays information about a config change to node R5. Click the Config Change notification.



9. In the config comparison window, scroll down until you see the highlighted change.

72	!	!
73	interface Ethernet1/0	interface Ethernet1/0
74	ip address 10.0.35.5 255.255.255.0	ip address 10.0.35.5 255.255.255.0
75	ip flow ingress	ip flow ingress
76	ip flow egress	ip flow egress
77	duplex half	duplex half
78		traffic-shape rate 1000000 25000 25000 1000
79	!	!

10. A new command was added on line 78 for interface Ethernet1/0. This is the problem. Note the change, and close the config comparison window.
11. Use NCM to revert the config file, or log in to the device and remove the incorrect configuration.

Orion integration with NetPath

NPM integration

NetPath™ is a feature of NPM, and by default displays NPM data and issues.

On the internal portion of the network path, you can:

- See NPM data such as CPU, RAM, interface utilization, and more included in the graph.
- Click a monitored device and go to its Node Details page.
- Click an unmonitored device and add it to Orion to see more data.

NTA integration

NetPath™ uses data from NPM to display information about your internal nodes on the network path, such as bandwidth used for the interface. But what is using that bandwidth?

 NetPath™ and NTA integration requires NTA 4.2 or later.

If you are exporting flow data from those nodes and monitoring it with NTA, NetPath™ displays additional information to identify what is using the most ingress and egress bandwidth.

Click the node or interface in the network path to open the inspector panel, where you can:

- View the top three conversations.
- Select ingress or egress.
- Click a conversation name to view details about that conversation.

NCM integration

NetPath™ displays additional information about NCM nodes with backed-up config files. If traffic through an NCM node was affected after a config change, NetPath™ notifies you that the two events may be correlated.

 NetPath™ and NCM integration requires NCM 7.4.1 or later.

NetPath™ highlights config-related issues on the path, and provides quick access to the configuration data for nodes on the path.

Click the node in the network path to open the inspector panel, where you can:

- Click Commands > View Current to see the config for the device.
- Click Commands > Compare to see two configs side by side for comparison.

View monitored objects on maps

Maps in the Orion Web Console can show monitored nodes, interfaces and volumes, SAM applications and components, and network links.

Open Street Map

[Display nodes](#) on maps powered by Open Street Map.

Network Maps

Create customized maps in Network Atlas, including [wireless heat maps](#), and display them in the Orion Web Console.

Wireless Heat Maps


In the Network Atlas, you can also [create wireless heat maps](#) to visualize the signal strength provided by your wireless access points.

Display nodes in the Worldwide Map of Orion Nodes resource

Nodes and groups that contain information about their location in the OpenStreet format are displayed automatically. See [Place nodes automatically on the Worldwide Map](#)

Objects with the same position are displayed as one location.


Although there is one Worldwide map, you can add the Worldwide Map resource to multiple views, and display different objects and information on each view. For example, you can apply different zoom levels, use different titles and subtitles, or center the map on different coordinates.

 If you cannot see the Worldwide Map resource on a view, add the resource. See [Add resources and columns to views, and define subviews](#).

Add nodes manually

Add a new location into the map, and define the nodes positioned in the location.


1. Click Manage Map in the Worldwide Map resource.
2. Click Place Nodes on the Map Manually, and click into the map where you want to place the nodes.
3. Use the Grouping and Search tools to select nodes which you want to place on the map.

 Click > next to a node group to expand a list of all nodes in the group.

4. Provide a name for the location.
5. Click Place on Map.
6. Click Submit.

If you want to further edit the map, click Save and Continue.

Edit the position of locations


 If the exact position is not known or important, you can drag locations to their positions.

1. Click Manage Map in the Worldwide Map resource.
2. Click a map location, and click Edit Location.
3. Provide the Latitude and Longitude of the new location, and click Save.
4. Click Submit.

If you want to further edit the map, click Save and Continue.

Add or remove nodes in locations, or rename locations

1. Click Manage Map in the Worldwide Map resource.
2. Click the map location you want to edit, and click Edit at the top right of the list of nodes at the selected map location.
3. Add or remove nodes in the location.
 - Select nodes to be added in the Available Objects section.
 - To remove nodes, click x next to the node in the Selected Objects section.

 If you want to rename the location, type the new name in the Name of Location field at the bottom of the Available Objects section.

4. Click Save Changes.
5. To apply your changes in the resource, click Submit or Save and Continue if you want to further edit your worldwide map.


Delete locations

1. Click Manage Map in the Worldwide Map resource.
2. Select the map location.
3. Click Remove from Map, and then confirm the map location removal.
4. Click Submit.

If you want to further edit the map, click Save and Continue.

Place nodes automatically on the Worldwide Map


If your devices contain information about their location in the OpenStreetMap format, they can be added into the Worldwide Map resource automatically.

 You can specify the position for automatic geolocation with custom properties. See [Place objects into the map using custom properties](#).


Objects with the same position appear as one location in the map.

To verify whether the automatic placement of objects is enabled:

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. In the Product Specific Settings, click Web Console Settings.
4. Scroll down to Worldwide Map Settings and make sure Automatic Geolocation is selected.

 Locations will display in the Worldwide Map resource within an hour after you select this option.

5. Click Submit to apply the current settings.

 Automatic geolocation does not change locations for manually placed objects. If you move an automatically placed location, its position will not be updated if you change the values for longitude and latitude.


In what format should the location on a Cisco device be configured?

You can use any format the mapquest API is able to parse.

FORMAT	EXAMPLE
city (AA5), state (AA3)	city (AA5), state (AA3)
city, state, postalCode	Lancaster, PA, 17601
postalCode	17601
street, city, state	300 Granite Run Dr, Lancaster, PA
street, city, state, postalCode	300 Granite Run Dr, Lancaster, PA, 17601
street, postalCode	300 Granite Run Dr, 17601
latLng	40.07546,-76.329999

Place objects into the map using custom properties

If you have longitude and latitude for your nodes or groups defined as custom properties, you can use the coordinates to automatically place the nodes on the WorldWide Map.

 You can [create the custom properties](#) using the Longitude and Latitude property templates.

1. [Export the values for the custom properties](#) Longitude and Latitude.
 - a. Click Settings > All Settings, and then click Manage Custom Properties.
 - b. Select Longitude and Latitude, click Export Values, and click Export.

2. **Import the .csv file** with longitude and latitude custom properties, and match these to Latitude and Longitude (World Map) column.
 - a. In the Custom Property Editor, click Import Values, select the export file with Longitude and Latitude.
 - b. Clear the Remove unchanged rows box, and click Next.

i If the box is selected, only the data you changed manually in the exported file will be imported. After an automatic export, there are no changes, and thus no data will be imported.

- c. Match Longitude and Latitude to the World Map columns.

Import Custom Properties

SELECT FILE **MATCH COLUMNS**

MATCH THE SPREADSHEET COLUMNS ON THE LEFT WITH ORION DATABASE COLUMNS ON THE RIGHT:

At least one column must be used as a reference for matching values to Orion objects (for example, IP address, MAC address). Only custom properties will be imported. [Learn more about matching columns](#)

⚠ Import will override existing custom property values in the Orion database where there is a match on selected columns

SPREADSHEET COLUMN	RELATIONSHIP	ORION DATABASE COLUMN
Caption	matches	Caption
IP_Address	matches	IP_Address
Latitude	imports to	Latitude (World Map)
Longitude	imports to	Longitude (World Map)

- d. Click Import.
3. Optional: Verify that the values were imported successfully.
 - a. Click Settings > All Settings, and click Manage Custom Properties.
 - b. Select Longitude and Latitude and click View / Edit Values.
 - c. Add the Longitude (World Map) and Latitude (World Map) columns.

+ ADD CUSTOM PROPERTY

IP_Address

Sort Ascending
Sort Descending
Columns
Filters

OrionIdColumn
OrionIdPrefix
Percent Loss
Percent Memory Available
Status
☒ Latitude (World Map)
☒ Longitude (World Map)
City

The values for Longitude (World Map) should match the Longitude values, and values for Latitude (World Map) should match the Latitude values.

You can now see the nodes in the Worldwide Map, as specified by the Longitude and Latitude (World Map) properties.

Network Atlas

Network Atlas is an application for creating custom maps and network diagrams. It is preinstalled with your Orion Platform product.

Maps provide a graphical depiction of the network. You can export or print maps, and use them to document your network. You can also view Network Atlas maps in the Orion Web Console.

What can you see on maps?

- Monitored SolarWinds NPM nodes, interfaces, and volumes, SAM applications and components, nested maps, and network links
- The coverage provided by your wireless access points and wireless clients connected to the access points

What customization options are there?

- Customize the map background with default colors, textures, or images. Add custom background graphics, such as floor plans.
- Link dynamic real-time weather or natural disaster maps to your network maps as the background.
- Customize the shape, size, color, and style of map links to illustrate the status of the relative bandwidth of associated objects.
- Select a graphical style for objects to reflect the network status on maps.
- Nest maps, so that you can drill down to reveal increasing levels of detail, and the status of nested map child objects may be bubbled up to the parent map. You can for example nest floor maps into a map of a building, and be notified if devices on the floor map are down.


Install Network Atlas


Network Atlas is pre-installed on Orion EOC and SolarWinds NPM, and it can be run as a local application on those Orion servers.

Users can also run Network Atlas as a standalone application on a remote computer.

Network Atlas Requirements

Network Atlas users must have the Map Management rights in SolarWinds NPM or in Orion EOC.


 The user logged in to Network Atlas must be able to access the Network Atlas synchronization folder to ensure synchronization with the SolarWinds Orion database.

Hardware/ Software	Requirements
Operating System	<div data-bbox="305 1753 768 1837">Windows Server 2008 R2 SP1 Windows Server 2012 and 2012 R2</div> <div data-bbox="310 1864 1511 1927"> Windows Server 2012 R2 Essentials is not supported.</div>


HARDWARE/ SOFTWARE	REQUIREMENTS
Memory	1 GB
Hard Drive Space	150 MB
Ports	Remote instances of Network Atlas require TCP on port 17777 to either the SolarWinds NPM or the Orion EOC server.
.NET Framework	.NET 4.5

Install Network Atlas on a remote computer

1. Log in to your SolarWinds NPM or Orion EOC server.
2. Start the Orion Web Console in the SolarWinds Orion program folder.
3. In the Map resource, click Download Network Atlas.

 If you do not see the download link in the Map resource, click Edit, select Show Network Atlas Download Link, and click Submit.


4. Save the installer (`NetworkAtlas.exe`) on the remote computer.
5. Run the installer on the remote computer, and click Next on the Welcome window.

 If you have previously installed Network Atlas, you may be prompted to change, repair or remove your installation. Click Repair, click Repair again on the Ready to repair window, and complete the Setup Wizard.

6. Accept the terms in the license agreement, and click Next.
7. Provide an appropriate installation destination folder, and click Next.
8. Click Install on the Ready to Install window.
9. Click Finish when the Setup Wizard completes.

See [Create network maps](#).

Start Network Atlas

 Users must have the Map Management right in SolarWinds NPM or in Orion EOC.

1. Log in to the computer hosting your Network Atlas installation.
2. Start Network Atlas in the SolarWinds program folder.
3. Connect to your primary Orion server:
 - a. Provide your Orion Web Console user name and password.
 - b. Provide the IP address or hostname of your primary Orion server in the Address field.
 - c. If you are connecting to an SolarWinds NPM server, select Orion as the Connect To target.
 - d. If you are connecting to an Orion EOC server, select EOC as the Connect To target.
 - e. Click Connect.

4. Now on the Network Atlas Welcome screen, select what map you want to open:
 - To open a recent map, select it in the Open Recent section.
 - To open a map available in a certain location, click Browse and navigate to the map.
 - To create a new network map, click Network Map in the Create New section. See [Create network maps](#).
 - To create a wireless heat map, click Wireless Heat Map in the Create New section. See [Create wireless heat maps](#).

Create network maps

Before you start creating maps, prepare a map management strategy. Consider the following recommendations:

- Map only static objects. If objects move, you need to adjust their location on maps, and it is difficult to keep maps up-to-date.
- Build maps to match the column width of your Orion Web Console views. Rescaling maps in views results in distorting of icons and texts.

To create a network map:

1. Start the Network Atlas in the SolarWinds program folder.
2. Provide your Orion Web Console credentials.
3. If you are launching Network Atlas on the local computer, type localhost into Address. If you are starting Network Atlas on a remote computer, provide the IP address of the main polling engine.
4. Click Connect.
5. Click Network Map in the Create New section.




A new empty network map will open in the Network Atlas.

Add objects on a map

Any objects monitored by SolarWinds NPM or SAM may be added to a Network Atlas map, such as:

- SolarWinds NPM nodes, interfaces, volumes, and Universal Device Pollers (UnDPs)
- SAM applications and components
- VoIP & Network Quality Manager operations
- Network Atlas maps
- Network links

To add objects on a map:

1. If you are creating a new map, click the Network Atlas button () and click New Map.
2. If you are adding objects to an existing map:
 - a. Click the Network Atlas button ()
 - b. Click Open Map.
 - c. Navigate to your existing map, and click Open.
3. Expand and navigate the node tree in the left pane to locate the network nodes and monitored objects you want to add to your map.
4. Drag selected objects onto the drawing area.
 - To add all the objects of a type on a node to your map, click + next to the node name to reveal all its associated monitored network objects, and drag all objects in the object group onto the drawing area.
 - A checkmark () next to a node or network resource indicates you have already added it to your map.
 - To view details about a map object, hover over it with the mouse pointer.
 - To locate a specific map object in your map, click its network resource in the left pane. This selects the map object.


Connect objects on maps automatically with ConnectNow

Using the ConnectNow tool, Network Atlas can automatically draw lines between directly connected nodes on your network.


ConnectNow displays connections based on data polled for nodes with enabled L2 and L3 topology pollers, and for unidentified nodes.

An unidentified node is a node that was found on the network but which is not managed by Orion. These devices might be switches, hubs, routers, or other devices without names or addresses.

Unidentified nodes can be virtual, generated to signify an indirect connection in your map. For example, when a topology calculation cannot find any direct connections between two nodes, an unidentified node is generated between the two known nodes.

- 
- The ConnectNow tool cannot draw indirect connections between nodes. For example, if nodes A and C are connected indirectly through node B, you must manually add node B to the map to create the connections.
 - Orion Enterprise Operations Console (EOC) does not support ConnectNow.

Connect objects on maps automatically using ConnectNow

1. Add the nodes to an open network map.
See [Add objects on a map](#).
2. Click ConnectNow () in the Home ribbon.

Update the Topology



ConnectNow displays data stored in the TopologyConnections database table. By default, the data are re-calculated every 30 minutes. You can update the data manually.

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. In the Node & Group Management grouping, click Manage Nodes.
4. In the More Actions drop-down list, select Update Topology.

The values in the TopologyConnections table will be re-calculated and your topologies will be updated.


Connect objects on maps manually

You can represent network links in your map by drawing lines between map objects. If a connected object is down, any connected links change color to red.

1. Make sure the Home ribbon is selected.
2. Click Straight () or Curved Line () in the Lines group, as appropriate.
3. Click an object with the line drawing tool to begin drawing the link
4. Click and drag as needed to set optional anchor points along the link path.
5. Click a second object to finish drawing the link.
6. If you want the links connecting your mapped objects to communicate the status of connected interfaces:
 - a. Right-click a link, and select Properties.
 - b. Select Status in the left pane of the Link Properties page.
 - c. Drag the appropriate interface objects from the left pane of the Network Atlas window to the link status assignment areas.

Reshape map links

You can use anchor points to change the shape of object links on your map. Use multiple anchor points to create more complex shapes and curves.


1. Select  in the Tools group, or click the middle mouse button.
2. Click and drag the link you want to reshape.

Configure display of connections on maps

Links created on Network Atlas maps are not merely connectors between network objects. They can display status of the connection, the link speed, or utilization.

1. Right-click a link, and select Properties.
2. Click Status and review the objects from which the link gets its status. To change the objects, drag objects from the Network Atlas navigation tree to the appropriate endpoint box.
3. Click Appearance and set the default width and style for the link. Select the color for links that are UP. Down links are always red.

4. Click Hyperlink to specify what should open when you click the link in the Orion Web Console.
5. To add a label, right-click a link, and select Add Label. A default label appears. Edit the label text or move the link label.
6. To specify what should be displayed for connections:
 - a. Expand Connection Display Options.
 - b. To display the link speed, select Show Link Speed.
 - c. To show the link utilization in percent, select Link Utilization.

 To hide all labels for the connections, clear the Include Link Labels, and click Don't Show Additional Info.

You can set interfaces through which linked objects are connected. Links can then display the status, speed or link utilization of the connection. Interface states and performance data are determined from SolarWinds NPM polling data.


Interface performance information in maps can be communicated using the interface status or performance:

- [Determine interface status in connections](#)
- [Specify interfaces that determine the status of connections on maps](#)
- [Display interface performance in map links](#)

Determine interface status in connections

Connections are shown as either solid or dotted lines. A solid line indicates that the connection is UP. A dotted line indicates that the connection is DOWN.

The connection status depends on the status of interfaces at both ends of the connection.

 The connection status is only shown as either UP or DOWN. To emphasize potential problems, DOWN status is granted a higher priority.

The following table shows how interface states are reflected in the status of a connection between NodeA, with InterfaceA, and NodeB, with InterfaceB.

		InterfaceB Status		
		UP	DOWN	UNKNOWN
InterfaceA Status	UP	UP	DOWN	UP
	DOWN	DOWN	DOWN	DOWN
	UNKNOWN	UP	DOWN	DOWN

Specify interfaces that determine the status of connections on maps

1. Right-click a link in a map, and select Properties.
2. Select Status in the left pane of the Link Properties page.

3. Drag the interface objects from the left pane of the Network Atlas window to the link status assignment areas.

Display interface performance in map links

Map links can show either interface utilization or interface connection speed. A legend is available to interpret colors representing interface performance data.

1. Expand Connection Display Options in the bottom left pane.
2. Select display options:
 - Show Link Speed provides interface connection speed information in colored links.
 - Show Link Utilization provides interface utilization information in colored links. This option is default on new maps.



 Utilization data is not shown for manually created links.

- Don't Show Additional Info provides only interface UP/DOWN status information on device links. This is the default option for previously created maps.
- Include Link Labels enables or disables displaying connection labels.

Add a background


You can select colors, textures, and locally-hosted or Internet-hosted images to serve as your map backgrounds.

- [Select a background color](#)
- [Select a background texture](#)
- [Select a background image](#)


 To clear the current map background, click Home, and click Background > Clear Background (.


Select a background color

Network Atlas supports 24-bit color backgrounds.

1. Click Home.
2. Click Background > Background Color (.
3. Select a color from the palette, or click More Colors to select a custom color.

Select a background texture

1. Click Home.
2. Click Background > Background Texture (.
3. Enter the Width and Height of your map in the Map Size in Pixels area.

 The default values are the smallest area bounding the existing map objects and labels.


4. Select a texture, and click OK.

Select a background image

Add images accessible on the hard drive or on the Internet as the background for your maps.

Requirements and recommendations

- Files used for linked backgrounds must be continuously accessible by URL reference.
- Files used for static backgrounds must be available within the local file system.
- To ensure optimal quality of images, plan graphics to display at full size in the Orion Web Console.
- When determining map size and resolution, consider web page layouts and display screen resolutions.

 Example backgrounds are in the `NetworkAtlas Backgrounds` folder located in your default shared documents folder.


Supported formats

- Graphics Interchange Format (.gif, non-animated)
- Tagged Image File Format (.tiff)
- Joint Photographic Experts Group (.jpg)
- Microsoft Windows Bitmap (.bmp)
- Portable Network Graphics (.png)

Linked backgrounds are updated when you access the map, or refresh the browser page.

Add an image as the background

1. Open the map in the Network Atlas, and click Home.
2. To use a background image the disk, click Background > Background Image, and navigate to the image.
3. To use a background image from the Internet:
 - a. Click Background > Linked Background.
 - b. Type the URL of the image.
 - c. Click Validate.
 - d. Click OK.



- In the web console, map background images linked from the Internet are refreshed with the Orion Web Console refresh.
- If the SolarWinds Orion server is behind a web proxy which requires authentication, you cannot link directly to the background image. A workaround is to write a script that periodically downloads the image and saves it to a folder on the web server. You can specify the saved image as the linked background image.

Add a dynamic background for a map

Weather conditions can affect availability of a certain location. You can add weather maps displaying the current weather as a background for maps.

1. Navigate to the page which you want to link as the background, and copy the static link.
2. Open the map in the Network Atlas.
3. Click Linked Background, and paste the URL.
4. Validate the URL, and click OK.

The dynamic map will now display as the map background.



When you add the map to the Orion Web Console, the map will refresh every time the Orion Web Console refreshes.

Clear the background

To clear the current map background, click Home, and click Background > Clear Background (✖).

Save maps

Network Atlas saves your maps directly to the server to which you are connected.

1. Click the Network Atlas button () and click Save.
2. If you are saving the map for the first time, name the map, and click OK.
3. If you want to save your map to your hard drive:
 - a. Click  > Export > Export Map.
 - b. Navigate to a location on your hard drive.
 - c. Provide a File name, and click Save.


Open maps

Maps are loaded from the Orion server to which you are connected. They appear in the left pane of the Network Atlas window.

1. Click + to expand the Maps group in the left pane of the Network Atlas window.
2. Double-click the map you want to open.

Create wireless heat maps

Wireless heat maps help you visualize wireless signal coverage on a building floor plan.

 Wireless heat maps are only supported for Cisco wireless controllers. The wireless controllers you want to see on wireless heat maps must be managed in SolarWinds NPM.

Before you begin

- Obtain an image of the wireless coverage area, such as a floor plan.
- Find at least one measurement of the distance between two points on the image, such as the length of a conference room.
- Choose the physical location of access points to accurately place them on the map.

To create wireless heat maps:

1. Start Network Atlas in your SolarWinds program folder.
2. On the Welcome to Orion Network Atlas page, click Wireless Heat Map in the Create New section.
3. Enter a name for the new map.
4. [Set a floor plan as the background.](#)
5. [Set the wireless heat map scale.](#)
6. [Add wireless access points.](#)
7. Optional: [Improve the accuracy of wireless heat maps by taking samples of the signal strength on real devices.](#)
8. Click Generate to display wireless signal coverage.

See also [Display wireless heat maps in the Orion Web Console.](#)


Disable the wireless heat map poller

The wireless heat map poller collects information about the signal strength on monitored access points. By default, this poller is disabled on your devices because of performance issues.


Network Atlas enables the wireless heat map poller on wireless controllers used in wireless maps because the information collected by the poller is required for including access points into wireless heat maps.

When do I need to disable the wireless heat map poller?

If you experience performance issues when working with wireless heat maps, disable the wireless heat map poller on the devices.

 Disabling the poller resolves performance issues, but your wireless heat maps will no longer be updated. The Orion Web Console resources and the Network Atlas will both display the last status generated before you disabled the wireless heat map poller.

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. In the Node & Group Management grouping, click Manage Pollers.
4. Locate the wireless heat map poller in the pollers table, and click the item in the Assignments column, such as 1 Node. Clicking the assignments link opens the Assign Wireless Heat Map to Nodes view.
5. Select all nodes for which you want to disable the poller, and then click Off: Disable Poller in the table title.

 Clicking the grey Off icon for the nodes in the Poller Status column disables the poller for the nodes. The icon will turn to green On, and the poller will be disabled.


Set a floor plan as the background

The floor plan should reflect the real dispositions of the office or buildings on the map, so that you can correctly position the wireless access points and reflect the wireless signal coverage on your map.

Requirements:

The floor plan must be a graphic file in one of the following graphics formats:

- Graphics Interchange Format (.gif, non-animated)
- Tagged Image File Format (.tiff)
- Joint Photographic Experts Group (.jpg)
- Microsoft Windows Bitmap (.bmp)
- Portable Network Graphics (.png)

 To ensure the readability of wireless heat maps, use black and white images.


To set a background for wireless heat maps:

1. Create the wireless heat map in the Network Atlas.
2. Click Background Image on the Home ribbon.
3. Navigate to the floor plan image, select the image, and click Open.

The floor plan will appear as the background for your heat map.


Set the wireless heat map scale

The correct scale is necessary for an accurate display of the wireless coverage provided by your wireless access point.

 You can use online maps, such as the full version of Google Maps, to measure your office building. Locate the building on Google Maps, right-click one wall, and measure the distance to the other wall of the building.

Requirements

- You have already inserted a background image for your wireless heat map (a floor plan).
- You know the distance of two objects displayed on the background image.

 To minimize error, set the scale for the longest distance possible, such as the building or floor length.

To set the map scale:

1. Create the wireless heat map in the Network Atlas.
2. Click Set Scale in the Home ribbon. A blue line segment with squares as end points will appear in the plan.
3. Drag endpoints of the segment to the objects on the map whose distance you know.

4. Fill in the distance between the endpoints into the appropriate field, and select the units (feet or meters).

Example: In floor plans, you usually know the dimensions of individual rooms. Drag and drop the line segment endpoints so that the endpoints are located on the opposite walls, and fill in the width of the room.

5. Click Set Scale to apply the scale to the wireless heat map.

Add wireless access points

To generate a wireless heat map, add wireless access points used by client devices into the map.

Requirements

- The wireless LAN controllers must already be managed in your Orion Platform product.
- Only Cisco controllers are supported.
- The wireless heat map poller must be enabled on the wireless LAN controllers that you use in the map.

To add wireless access points:

1. Create a wireless heat map in the Network Atlas.
2. Go to the navigation tree on the left of the Network Atlas main screen.
3. Locate the wireless access points that you want to add to the map.



To find access points on a node, navigate to Orion Objects > vendor name, such as Cisco > appropriate node > Wireless Access Points.

4. Drag the access points to their location on the map.

The selected access points will appear on the map. You can now generate the map.



To make the map more accurate, take signal samples.

Improve the accuracy of wireless heat maps by taking samples of the signal strength on real devices

Wireless heat maps display the ideal wireless signal coverage, they do not count with physical obstacles, such as office walls. To make wireless heat maps more real, measure the signal strength on real devices, such as cell phones, laptops, or tablets connected to your wireless network. The measured values are stored as signal samples and used for calculating the signal coverage on wireless heat maps.

Signal samples represent the signal strength measured in a specified location.



Take signal samples in places where you expect the signal to be blocked by walls or other obstacles, or in places where the signal strength does not correspond with your heat map.


Take signal samples with cell phones, because polling the signal is usually faster for them.

Simple signal samples

Take a wireless device, walk it to a certain location, and take a signal sample there. Then, walk the device to another location, and take another signal sample. This procedure is called "walking edition" because it requires you to walk through the office.

Multiple signal samples

If you have multiple devices connected to your wireless access points, take multiple signal samples at once (called "sitting edition" because you can do it sitting at your desk).

 Signal samples stay in the map and influence the calculation of wireless heat maps even after the client moves from its position. When you move access points in a map, the signal samples might not be accurate any more. Delete obsolete signal samples, and add new ones.

Requirements

- You need to have a [wireless heat map created](#) and open in the Network Atlas.
- You need to have [wireless access points added](#) into the map.
- You need to have clients, such as cellular phones, tablets, laptops, connected to the access points positioned in your wireless heat maps.

Take simple signal samples

1. Click Take Signal Sample in the Home ribbon. The Signal Sample wizard will display on the right side of the Network Atlas screen as a tab.
2. Walk your device to the location where you want to measure the wireless signal strength and click Next.
3. Select the wireless client (cellular phone, laptop, or tablet) in the drop-down list, and click Next.
4. Drag the client into its current location on the map, and click Next. Network Atlas will start measuring the wireless signal strength in the spot. It can take a few minutes, depending on the device.
5. To add another signal sample, click Repeat, walk the device to a new location, and repeat steps 3 - 4.
6. To apply the measured signal strength to the heat map, click Generate Map.
7. Network Atlas will regenerate the map. Click Close to hide the Signal Sample wizard tab.

Take multiple signal samples at the same time

1. Click Take Signal Sample in the Home ribbon. The Signal Sample wizard will display on the right side of the Network Atlas screen as a tab.
2. Click Use Multiple Devices to Take Signal Samples.
3. Drag the clients to their positions on the wireless heat map, and click Next.



- If there are too many devices, use the search box to find the devices you want to use for creating signal samples.
- Measuring the wireless signal strength can take a few minutes.
- If the signal measuring fails, you can either repeat the measurement for the device, or restart the wizard.

4. Network Atlas will automatically regenerate the map according to the defined signal samples. Click Close to hide the Signal Sample wizard tab.

Troubleshoot wireless heat maps

If your wireless signal coverage on your wireless heat maps is not as expected, you can take the following troubleshooting measures.

- Make sure that the map scale you have entered is precise.
- Make sure that your access points are located correctly.
- Verify that signal samples are up-to-date.
- The signal samples stay in the map even after the device you measured the signal strength on moves away. If you change the position of your access points, or the dispositions of your office, the signal samples might not be accurate and could affect the calculated wireless heat map.

- Delete obsolete signal samples.

To delete a signal sample, open the wireless heat map in the Network Atlas, select the signal sample, and press the Delete key.

- Add new signal samples. See [Improve the accuracy of wireless heat maps by taking samples of the signal strength on real devices](#).

Advanced mapping techniques

- [Zoom in and out of a map](#)
- [Create nested maps](#)
- [Display the status of child objects on maps, and change metric thresholds](#)
- [Add independent map objects and floating labels](#)
- [Change the appearance of map objects](#)
- [Customize the width, color, and line styles of network links in maps](#)
- [Customize labels](#)
- [Customize the page that opens when you click on a map object](#)
- [Link or embed maps in web pages using the map URL](#)

Zoom in and out of a map

Zoom into a map to enlarge details or to zoom out to reduce its size. Zoom level is a visual aid, and it is not saved with the map.

Use any of the following methods:

- Press and hold CTRL while rotating the mouse wheel button.
- Click the Zoom slider on the status bar, and then slide the zoom control to the zoom level you want.
- Click View, and select the type of zoom you want to use from the Zoom group.

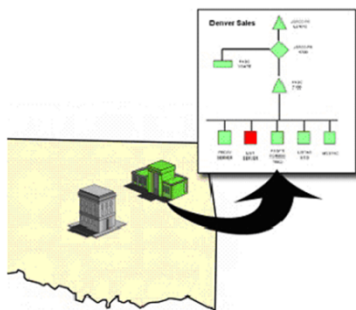
Create nested maps

Nested maps allow you to navigate through a map to see multiple levels of detail.

For example, a map of the United States can include an icon for a child map of Oklahoma. You can then click the Oklahoma object to open the child map.



The map of Oklahoma can become a parent map to a network diagram.



Each child map can include a view of the objects, either devices or other maps, deployed on it.

Click any nested object to view the next level of map detail, until you reach the final network device and see all available network information.

i The total number of objects on a map, including objects on child maps, affects how fast the map loads in the Orion Web Console. If your maps load slowly, decrease the number of map objects.

1. Create all maps to be nested in the Network Atlas.
2. Open the parent map, and drag a map from the Maps group onto the parent map.
3. Position the new map object on the parent map, and save the map.

4. If you want the status of a child map to also indicate the status of its child objects, complete the following steps:
 - a. Right-click the child map icon on the map, and select Properties.
 - b. Select Include Child Status on the Status properties page, and click OK.

The object status icon now includes the secondary status indicator.

Display the status of child objects on maps, and change metric thresholds


The status of a map object icon reflects its current state, such as up or down. You can add a secondary status indicator to a map object to reflect metrics such as response time, CPU load, or the state of any child objects. This secondary status indicator appears at the bottom right corner of the status icon.

To add the secondary status indicator:

1. Right-click the map object, and select Properties.
2. Select Include Child Status on the Status properties page, and click OK.

To change the thresholds of the metrics:

1. Right-click the map object, and select Properties.
2. Click Metrics to view the Metrics properties page.
3. To change the warning or critical threshold for a metric, click the threshold value, and type a new value.
4. To ignore a metric, clear the metric.
5. Click OK.

-  ■ The secondary status indicator respects the Orion Web Console Status Rollup Mode setting for displaying status.
- All child objects and selected metric thresholds are taken into account to determine secondary status.

Add independent map objects and floating labels

Independent objects and floating labels do not have associations to network nodes or resources.

To add an independent object:

1. Click Home.
2. Click Add Object in the Objects group to add a gray map object to the map.


To add an independent label:

1. Click Home.
2. Click Add Label in the Labels group. A label is added to the map.

Change the appearance of map objects

Changing the graphics that represent map objects allows you to increase the information density of your map without increasing the map complexity.

Set the default representations of map objects

1. Click the Orion Network Atlas button , and click Network Atlas Settings.
2. Click Graphic Styles in the left column.
3. Select an appropriate default style for each available map object.

For example, you can set an object icon to visually designate the type of the monitored device. You can then select a status style, such as 3D Pad Underneath, to illustrate the object status.

Change the representation of single map objects


1. Right-click a map object, and select Properties.
2. Click Appearance in the left column of the Properties page.
3. If you want the map object to appear as a fixed-size, LED-type graphic, complete these steps:
 - a. Select Orion LED Status Icon.
 - b. Select a style from the Orion LED Status Icon Style list, and click OK.
4. If you want the map object to appear as a scalable shape, complete these steps:
 - a. Select Shape.
 - b. Select a style from the Shape Style list, and click OK.
 - c. Drag a corner handle on the map object to resize the shape.
5. If you want the map object to appear as a scalable graphic, complete these steps:
 - a. Select Graphic.
 - b. Click Select Graphic, select an appropriate graphic, and click OK.
 - c. Select a status style from the Graphic Style list, and click OK.
 - d. Drag a corner handle on the map object to resize the graphic.


Paste custom icons from the Windows clipboard

You can paste graphics from the Windows clipboard into Network Atlas maps, and display an overlay behind them to depict their status.

Icons that you paste into Network Atlas are saved to the SolarWinds Orion database, and made available for reuse in other maps under the "Imported" icon grouping. Pasted icons saved to the SolarWinds Orion database can be used by remote instances of Network Atlas.

1. Open the icon image in a graphics program, such as Visio or Photoshop.
2. Copy the image to the Windows clipboard with the Copy command.
3. Open the appropriate map in Network Atlas.
4. Paste the image as a new object following these steps:
 - a. Right-click on the map and then click Paste.
 - b. Select Paste the Image From the Clipboard as a New Object.
 - c. Enter a name for the image.
 - d. Click OK.

 The added icons are also saved on the SolarWinds Orion server in the path

 %APPDATA%\SolarWinds\NetworkAtlas\Maps\Orion\<orion server address>\NetObjects\Imported.
%APPDATA% is typically located in C:\Users\<logged on user>\AppData\Roaming

Delete a custom icon

1. Determine which file on the SolarWinds Orion server contains the icon (for example, `mypicture.wmf`).
2. Add `.del` to the file name (for example, `mypicture.wmf.del`).
3. Start Network Atlas on the SolarWinds Orion server to delete the icons from the database.

Add custom icons from graphics files

The custom graphic files must meet the following requirements:

- Supported image formats: Windows Media File (`.wmf`) or Graphics Interchange Format (`.gif`).
- Name the graphic files according to their roles.
- The file name must not contain any other dash (-) characters other than depicted in this table.

ROLE	FILE NAME
Critical status	<code>iconName-critical.gif</code>
Down status	<code>iconName-down.gif</code>
External status	<code>iconName-external.gif</code>
Icon with no status	<code>iconName.gif</code>
Unknown status	<code>iconName-unknown.gif</code>
Unmanaged status	<code>iconName-unmanaged.gif</code>
Unplugged status	<code>iconName-unplugged.gif</code>
Unreachable status	<code>iconName-unreachable.gif</code>
Up status	<code>iconName-up.gif</code>
Warning status	<code>iconName-warning.gif</code>

Add custom icons from graphics files

1. Prepare the icons and save them as `.gif` or `.wmi` files.
2. On your SolarWinds NPM server, paste the icons into the following folder:
%APPDATA%\SolarWinds\NetworkAtlas\Maps\Orion\<orion server address>\NetObjects\User Graphics.
%APPDATA% is typically located in C:\Users\<logged on user>\AppData\Roaming
3. Start Network Atlas on the SolarWinds NPM server.
You can now assign the custom icons to objects on Network Atlas maps.


Assign a custom icon to an object

1. Right-click the object on the map, and then click Select Graphic.
2. Select User Graphics in the left pane.
3. Select the graphic image, and click OK.

The custom icon will display on the map.

Customize the width, color, and line styles of network links in maps

1. Right-click a link, and select Properties.
2. Select Appearance in the left column of the Properties page.
3. Select a line width in pixels from the Width list.
4. Select a line color from the Color list.
5. Select a line style from the Style> list.
6. Click OK.

 The color setting only changes the color of links that have the Up status.

Customize labels

 To move a label, drag it to the new location.

Edit a label text

1. Double-click the label.
2. Press <SHIFT>+<ENTER> to separate multiple lines within the same label.

Customize text attributes, borders, and background colors

1. Right-click the label, and select Properties.
2. Select Appearance in the left column of the Properties page.
3. To change the font attributes, click the ... button, select the font attributes, and click OK.
4. To change the text alignment, select an alignment from the Text Alignment list.
5. To change the text color, click the Text Color box, and select a color.
6. To add a label border, select the border width in pixels from the Border Width list.
7. To change the label border color, click the Border Color box, and select a color.
8. To remove label borders, select **0** from the Border Width list.
9. To add a label background, clear Transparent Background.
10. To change the label background color, click the Background Color box, and select a color.
11. To remove a label background, select Transparent Background.
12. Click OK.

Customize the page that opens when you click on a map object

By default, map objects are linked to the most relevant details page for the object. Customize the URL hyperlink to link to external web sites and pages.

1. Right-click the map object, and select Edit Hyperlink.
2. To link to the relevant Orion page for the map object, select Logical Page in Orion.
3. To link to a custom URL, select Manually Set Address, and type the URL.
4. Click OK.

Link or embed maps in web pages using the map URL

The map URL is in the form:

```
http://orionServer/Orion/NetPerfMon/MapView.aspx?Map=mapName
```

orionServer

This is the IP address or host name of your SolarWinds NPM server.

mapName

This is the display name of the map. If the name contains space characters, substitute %20 for the spaces when specifying the name.

Customize map tooltips

When you hover over map objects in the Orion Web Console, a tooltip with the current identification and status of the object appears.

Customize tooltips for all map object types in the Orion Web Console to display additional information using alert variables, custom properties, and other text.



- Tooltip customizations are global, and affect all maps.
- Orion EOC does not support custom web console tooltips.
- To enter a carriage return, use \${CR}.

Add additional information to map object tooltips

1. Log in to the Orion Web Console as an administrator.
2. Locate the Map resource, and click Edit.
3. Click Customize Map Tooltips.
4. Type the variables and any text in the text field for the map object type.
5. Click Submit.

Set when a map is displayed as Up on parent maps using the Up status threshold

The UP status threshold is the percentage of map objects that must be in an up state on a given map for the map to be represented as up on the parent map.

1. Right-click any empty portion of the map, and select Map Properties.
2. Slide the Map Status Will Be UP slider to configure the up state threshold on the Map Properties page.

Display restricted nodes for users with account limitations

If Orion Web Console users have account limitations that prevent them from seeing network nodes, set whether the users should see the restricted nodes on maps.


Users with restricted access to the nodes will only see the restricted nodes, but cannot retrieve any additional information about the nodes.

Hide nodes from users who have account limitations

1. Right-click any empty portion of the map, and select Map Properties.
2. Select Remove Nodes That Users Do Not Have Permission to View.

Reveal nodes to all users

1. Right-click any empty portion of the map, and select Map Properties.
2. Select Allow All Users to View All Nodes On This Map.

 Users with account limitations, but with the permission to run and use the Network Atlas can change this setting in the map. To prevent this, do not give node management permissions to users who have account limitations.

Advanced map layouts

- [Position map objects](#)
- [Display grid](#)
- [Align map objects](#)
- [Distribute map objects](#)
- [Arrange map objects according to a layout style](#)

Position map objects

Drag objects from the tree on the left to the appropriate position on the map.

To nudge a map object, select the object, and press <Ctrl> + <arrow>.

To reposition a map object:


1. Click the map object.
2. Click the Edit ribbon.
3. In the Size & Position area, enter the X and Y coordinates.

 Map center is designated as (x,y) = (0,0).

Display grid

A grid guide helps you maintain structural and spatial relationships as you arrange your map objects.

Grids are neither saved with a map, nor displayed in the Orion Web Console.







1. Click the View ribbon.
2. Click Show Grid  in the Grid group.

Customize grid

1. Click View.
2. To display grid lines, click Grid Option > Grid Lines.
3. To display grid points, click Grid Options > Grid Points.
4. To change the grid size, click Grid Options > Grid Size, and select a grid size.



Align map objects

1. Click the Edit ribbon.
2. Select the map objects you want to align.
3. Click the button in the Align group to arrange the object.

BUTTON	FUNCTION	DESCRIPTION
	Align Left	Aligns all selected objects on the left edge of the group
	Align Right	Aligns all selected objects on the right edge of the group
	Align Bottom	Aligns all selected objects on the bottom edge of the group
	Align Top	Aligns all selected objects on the top edge of the group
	Center Vertically	Centers all selected objects vertically
	Center Horizontally	Centers all selected objects horizontally








Distribute map objects

1. Click Edit.
2. Select the map objects you want to distribute.
3. Click the appropriate button in the Distribute group to arrange the selected objects.

BUTTON	FUNCTION	DESCRIPTION
	Distribute Horizontally	Distributes all objects so that they are equidistant from the left edge of the leftmost object to the right edge of the rightmost object
	Distribute Vertically	Distributes all objects so that they are equidistant from the top edge of the topmost object to the bottom edge of the bottommost object

Arrange map objects according to a layout style

1. Click Edit.
2. Click a layout style from the AutoArrange group.

BUTTON	FUNCTION	DESCRIPTION
	Circular	Emphasizes the clusters inherent in the topology of a map. It emphasizes prominent links between main objects and its peripherals. Object groups have radial placements. Use circular layouts for maps containing ring and star network topologies.
	Symmetrical	Emphasizes the symmetrical patterns inherent in the map topology. It emphasizes an even distribution of objects, and minimizes edge crossings. Object groups have star spiral placements. Use symmetrical layouts for maps that have fairly homogenous or uniform clusters.
	Hierarchical	Emphasizes mapped dependency relationships by placing objects at different levels. Use hierarchical layouts to depict data dependencies.
	Orthogonal	Emphasizes compact drawings, and uses only horizontal and vertical edges. Objects are enlarged if necessary to provide enough space for edge connections. Use orthogonal layouts for maps that need to depict multiple clusters in a space-efficient manner.
	Tree	Emphasizes parent and child relationships. Child objects are arranged farther from the root object than their parent objects. Use tree layouts for maps that have a central control object.
	Reorganize	Moves all mapped objects back to the center of the map view.
	Arrange Labels	Restores the default relative position of all object labels.

Display Network Atlas maps in the Orion Web Console


To see a graphical overview of devices on your network, [create a Network Atlas map](#), [add the Map resource](#) on the view, and specify the map you want to see in the resource.

1. Log in to the Orion Web Console as an administrator.
2. Click Edit in the Map resource.
3. Select your map from the Select Map list.
4. Click Submit.

The selected map will now appear in the Map resource.

Display wireless heat maps in the Orion Web Console

1. [Create](#) the wireless heat map in the Network Atlas.
2. Log in to the Orion Web Console.
3. To open a wireless heat map, use one of the following options:
 - Go to the All Wireless Heat Maps resource, and click the thumbnail for the map. The map will open in the Wireless Heat Map view that includes all resources specific for wireless heat maps.


 By default, the All Wireless Heat Maps resource is available on the NPM Summary view.
 - Add the Map resource on the view, click Edit, select the map in the list, and click Submit. See [Add resources and columns to views, and define subviews](#) for more details about adding the resource.


Change the time and frequency for regenerating the map

By default, the wireless heat map is regenerated once a day, and the information about clients connected to wireless access points is collected every 5 minutes.

1. Click Settings > All Settings.
2. In the Thresholds & Polling grouping, click Polling Settings.
3. Scroll down to the Wireless Heat Map.
4. Adjust the time when wireless heat maps should be regenerated in Map Generation Start Time.
5. Specify how often the information about clients connected to wireless access points should be collected in Default Client Signal Strength Poll Interval.
6. Click Submit.


View the location of clients connected to access points in maps

 To be able to view clients in a wireless heat map, you must add at least three access points and one signal sample, or four access points into the map.

 Viewing the location of connected clients is supported only for Cisco access points with CleanAir technology.

1. Create a wireless heat map in the Network Atlas. See [Create wireless heat maps](#).
2. Log in to the Orion Web Console, and open the wireless heat map in the Wireless Heat Map resource. See [Display wireless heat maps in the Orion Web Console](#).
3. Make sure the Show Connected Wireless Clients option is selected.

You should now be able to see clients connected to access points available on the map.

 If you cannot see a client on the map, its position might be calculated outside of the selected map. To verify this, consult the Displaying item in the legend. If the map shows less clients than are actually connected, such as one out of three, it means that the remaining clients are either outside of the map, or filtered out.

Limit the number of clients displayed on the map

Too many clients on the map might make the map crowded, and could also cause performance issues. A wireless heat map can show a maximum of 100 clients.

1. Go to the Map resource.
2. Click Select Which Clients to Show
3. Click + next to Select Wireless Clients To Be Specified.
4. Define how the displayed clients should be selected:

Random selection of all clients

- a. Select Show Every Client Connected to Any AP on the Map.
- b. To limit the number of clients, select the Limit the Number of Clients To box, and enter the number of clients to be shown on the map (1 - 100).

Clients connected to an AP

- a. Select Only Show Clients Connected to a Specific AP.
- b. Select a Wireless AP.
- c. To limit the number of clients, select the Limit the Number of Clients To box, and enter the number of clients to be shown on the map (1 - 100).

Select which clients to show

- a. Select Let Me Pick Specific Clients to Show.
 - b. Use the Group and Search by filters, and select the clients to be displayed on the map.
5. Click Submit to apply your settings.

Use alerts to monitor your environment

An alert is an automated notification that a network event has occurred, such as a server becoming unresponsive. The network event that triggers an alert is determined by conditions you set up when you configure your alert. You can schedule alerts to monitor your network during a specific time period, and create alerts that notify different people based on how long the alert has been triggered.

The types of events for which you can create alerts vary, depending on the Orion Platform products you have installed. For example, you can create an alert to notify you if a node in a specific location goes down or if the network response time is too slow when you have NPM. If you have installed SAM, you can receive alerts about application response times or when your Exchange mailbox database is almost full.

You can create alerts for any monitored object. You can alert against volumes and nodes with most Orion Platform products.

Use the following topics to get started if you have never used Orion Platform products:

- [Alert preconfiguration tasks](#)
- [Best practices and tips for alerting](#)
- [Navigate to the Alert Manager](#)
- [Create new alerts to monitor your environment](#)
- [Alert me when a server goes down](#)


You can also view our [Alert Lab](#) on [thwack](#) for community-based alert information.

Alert preconfiguration tasks

Some alerts require extra configuration, separate software installations, or information that you may need to request from other departments.

Alert actions that require set up before creating or configuring alerts include:

- [Send an email or page](#)
- [Dial a paging or SMS service](#)
- [Play a sound when an alert is triggered](#)
- [Send an SNMP trap](#)
- [Use the speech synthesizer to read alerts](#)

 Monitored objects in the SolarWinds Orion database must exist before creating or configuring alerts. Monitored objects can include items such as nodes, databases, and applications.

Configure the default information in the email action

The information you provide in the default email action is used to populate the Send an Email/Page action. You can still customize individual email actions if you configure the default email action.



- Separate email addresses with a semicolon.
- All email actions require a designated SMTP server.

1. Click Settings > All Settings in the menu bar.
2. Click Configure Default Send Email Action.
3. Under the Default Recipients heading, provide the email addresses of all default recipients for any email alert action, like the following:
`email@company.com; email2@company.com; distro1ist@company.com`
4. Provide the default sender and reply address.
5. Enter the default SMTP server information.



Selecting SSL encryption automatically changes the SMTP port number to 465.

Best practices and tips for alerting

Use these best practices and tips to help you configure and test your alerts.

Use the out-of-the-box alerts as templates

SolarWinds recommends using the alerts that are included when you install the product as templates for your new alerts.

Find an alert that is similar to one you want to create and then click Duplicate & Edit in the menu bar. Fields are pre-populated so you can skip to specific parts of the Alert Wizard where there is data you want to change.

Enable out-of-the-box alerts

If there are out-of-the-box alerts that match your monitoring needs, enable them in your environment. You can customize the alert actions for those alerts. If you want to modify the conditions, use the alert as a template.

Restrict who receives alerts

During your initial evaluation and testing, send alerts to a few people instead of to a large distribution list. This can prevent overloading your email server while you fine-tune your alerts.

Plan which devices to monitor

To reduce the number of alerts sent out, consider which devices are most important. For example, you may want to receive alerts only for mission-critical interfaces instead of every interface on a device.

Establish dependencies

Establish dependencies to prevent you from receiving duplicate alerts that stem from a single network event. For example, you may want to be emailed if servers in your server farm go down, but if the router goes down and the servers can no longer be polled, you do not want to receive notifications for all of your servers.

Navigate to the Alert Manager


Use the Alert Manager to create, edit, delete, enable, or disable alerts. You can access the Alert Manager in one of three ways:

- Settings Page (Recommended)
 - Click Settings > All Settings in the menu bar. Under Alerts & Reports, click Manage Alerts.
- Active Alerts Details
 - From the Active Alerts Details page, click Manage Alerts in the Management resource.
- Node Details
 - On the Node Details page, navigate to the All Alerts this Object can trigger resource, and then click Manage Alerts.

Create new alerts to monitor your environment

[Navigate to the Alert Manager](#) to create a completely new alert definition, or duplicate an alert that is similar to the alert you want to create.

1. Enter the [alert properties](#), which includes who can view the alert, severity, and how frequently the alert conditions are evaluated.
2. Define [the conditions must exist to trigger the alert](#).
3. Define [what event occurs to reset the alert](#).
4. [Schedule](#) when you want the alert to monitor your environment.
5. Define [what happens when an alert is triggered](#).
6. Define [what happens when the alert is reset](#).
7. [Review](#) your alert, including the number of alerts that will be triggered based on the conditions you defined.

 You can skip to different steps if you clicked Duplicate & Edit or if you are editing a saved alert.


Once you have created an alert, it is added to the list of available alerts in the Alert Manager. When the alert is enabled, it immediately monitors your environment for the conditions necessary to trigger it.

Set alert properties

After creating a new alert, use the Alert Properties to describe the alert, including which users can view the alert.

Name of alert definition

This is a required field. The name is displayed in the Alert Manager and can be used to sort your alerts. If you intend to create a large number of alerts, consider a naming convention that allows you to quickly scan through them.

 SolarWinds recommends a name that describes the condition and most visible alert action. For example, you can use "Email NetAdmins when router goes down" as the name of an alert.

Description of alert definition


Describe the alert. This is displayed on the Manage Alerts page, so important information should be near the front.

Enabled (On/Off)

Choose to evaluate the alert immediately after it is created and saved. The alert is enabled. If you are in the process of refining your alert, you may want to disable this alert until it is ready for use.

Evaluation Frequency

Set how frequently you want to evaluate the conditions. If you choose to alert on an event, such as a changed IP address, the condition is not evaluated by frequency, but by when the change is reported based on the polling interval.


 SolarWinds recommends using intervals longer than one minute to evaluate alert conditions. Shorter frequencies can negatively impact your network performance or computing resources.

Severity of Alert

Control how the alert in the Active Alerts resource looks, and use the severity to group or filter alerts more easily.

Alert Custom Properties

Use custom properties to organize your alerts. For example, you can create a "Responsible Team" custom property and use it to help audit who receives specific alerts.

 You must [create a custom property](#) for alerts before you can use it in an alert.


Alert Limitation Category

Restrict who can view the alerts. For example, managed service providers can restrict alerts to their specific customers. Create a new alert limitation by editing or creating a user account.

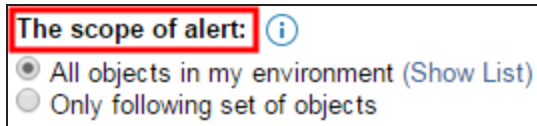
Define the conditions that must exist to trigger an alert

The trigger condition is the most complex step in creating an alert. Before you begin, you may want to revisit the [Best practices and tips for alerting](#). To see an example of completed trigger conditions, see the [Alert me when a server goes down](#) topic.

Trigger conditions are built using child conditions that are evaluated in order. Child conditions are represented as a line item under the Actual Trigger Condition. You can have multiple trigger condition blocks with multiple child conditions.

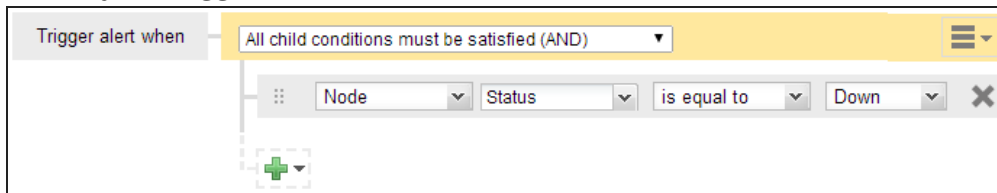
 Filter your environment to only display the objects you want to monitor in The scope of alert. Use the Show List link to view all of the objects that the alert monitors.

1. Choose what objects you want to monitor in the I want to alert on field.
2. Establish how much of your environment you want to monitor in The scope of alert.




You can monitor all objects in your environment or filter your environment to a specific set of objects.


3. Create your trigger condition.



- a. Choose if the child conditions must be true or false to trigger the alert.
 - All child conditions must be satisfied (AND) - Every child condition must be met
 - At least one child condition must be satisfied (OR) - At least one child condition must be true
 - All child conditions must NOT be satisfied - Every child condition must be false
 - At least one child condition must NOT be satisfied - At least one child condition must be false
- b. Click the + sign to add child conditions.
 - Add Single Value Comparison (Recommended) - The child condition evaluates a single field, like Status
 - Add Double Value Comparison - The child condition evaluates two conditions, such as Status and OS
 - Add And/Or block - Adds a sub condition block

 Use the X at the end of each child condition to delete it, or use the drop-down menu at the top of the block to delete the entire condition.

- c. Select the object you want the child condition to evaluate, and then select which field you want to evaluate. In the example screenshot, the object is "Node" and the field is "Status".

 You can evaluate objects based on variables or macros.

- d. Select how you want to compare the polled value of the field to the value entered here, and then enter the value. In the example screenshot, the comparison is "is equal to" and the value is "Down".

- e. To use more complex conditions, such as evaluating when an application on a specific server is down and a different application on another server is down, enable complex conditions under Advanced options.
See [Building Complex Conditions](#) for more information, or visit [thwack](#), SolarWinds' community website, for support from other users.
- f. Choose how long the condition must exist before an alert is triggered. This prevents receiving alerts when the alert condition, such as high CPU utilization, occurs briefly or only once during a certain time period.
 - Send an alert immediately when the condition is met by clearing any selection for Condition must exist for more than.
 - Wait before sending an alert by selecting Condition must exist for more than, and entering how long the condition must exist. This option prevents multiple alerts firing if the condition is temporary.


If you have successfully created an alert condition, you can move to the next step in the alert wizard. The Summary step evaluates the conditions against your environment and returns how many objects will trigger the alert.

Define the conditions that must exist to reset an alert

Use the reset condition to define what must occur to remove an alert instance from the active alerts list. For example, the "Email me when a Node goes down" alert automatically resets when the node comes back up. You can use the built-in reset conditions or create your own.

When reset conditions are met, the alert is removed from Active Alerts. You can also add actions that occur when the reset conditions are met.

For example, you can create an alert that triggers when nodes in your lab go down. If node 192.168.4.32 goes down, the alert fires for that specific instance of the trigger condition and any escalation levels you create continue until you reset the alert. After the alert is reset, all trigger actions stop and a new alert fires the next time node 192.168.4.32 goes down. If you have created reset actions, the reset actions fire.

 When the alert is reset, escalation actions are halted.

Select one of the following reset conditions:

- **Reset this alert when trigger condition is no longer true (Recommended)**



SolarWinds recommends using this reset condition. If the trigger condition is no longer true when the objects are next polled, this selection automatically resets the alert.

You can use the Condition must exist for more than option in the trigger conditions in conjunction with this reset condition. Trigger conditions that involve volatile components, such as high CPU utilization, can trigger excessively with this reset condition.

- **Reset this alert automatically after**

Select to reset an alert after a set amount of time has passed. If this interval is less than the amount of time you wait for different escalation levels, the escalation levels that occur after this interval do not fire. This reset condition is especially useful to remove event-based alerts from Active Alerts.

For example, if the trigger conditions still exists after 48 hours, you can use this to trigger your alert actions again. The alert is reset and triggers as soon as the trigger condition is detected, which is as soon as the objects are polled for this example.

- **No reset condition - Trigger this alert each time the trigger condition is met**

The alert fires each time the trigger conditions are met.

For example, when the alert for node 192.168.4.32 going down fires, a new alert for 192.168.4.32 fires every time the node is down when it is polled.

- **No reset action**

The alert is active and is never reset. To re-trigger the alert, the alert must be manually cleared from the Active Alerts view.

- **Create a special reset condition for this alert**

Select to build a specific reset condition. For example, you can choose to reset the condition when the node has been up for more than 10 minutes.


The alert wizard evaluates the reset condition for errors. If there are no errors, you can proceed to the next step, or go back to previous steps.

See [Define the conditions that must exist to trigger an alert](#) or [Build complex conditions](#) for more information on creating conditions.

Schedule when an alert monitors your environment

You can configure when an alert monitors your environment. By default, alerts monitor your network for changes all the time. Schedule when you want to monitor your network for the trigger conditions you created for the alert.

You can create multiple schedules that control when an alert is enabled or disabled. For example, you can schedule the alert to monitor your network during off hours, and disable the alert during your maintenance windows.

 Alerts must be enabled to allow schedules to run.

1. Select Specify time of day schedule for this alert.
2. Click Add Schedule.

3. Enter the following information:

- **Schedule Name**

This is not required, but may help you organize or troubleshoot your schedules. If you do not enter a name, a name is automatically generated from the time period.

- **Enable or Disable alert during following time period**

If you choose to disable the alert, it is enabled all other times unless otherwise scheduled.

- **Frequency**

Choose when to monitor on a high level, such as daily, weekly, or monthly.

- **Enable or Disable every**

These options change based on the frequency.

- If you selected Daily:

You can choose to enable or disable the alert every few days, up to every 31 days. You can also select business days. For example, you may want to disable network or disk activity alerts if you run daily, off-site backups of your critical data.

- If you selected Weekly:

Choose which days the alert is enabled or disabled. You may want to disable alerts during a weekly maintenance window.

- If you selected Monthly:

Choose which months the alert is enabled or disabled. This option is useful when you have quarterly or monthly maintenance windows.

Choose either a specific date, such as June 22nd, or a day, such as Thursday.

- **Starting on**

Choose when to begin the schedule.

- Right now - Start the schedule immediately.

- Specific Date - Select a time and day to begin the schedule.

- **Ending on**

Choose an end date for the schedule, if necessary.

4. Click Add Schedule to create the schedule.

When you add a schedule to an alert, the alert only monitors during the time period you have scheduled, or does not monitor during that time. Alert actions can also have schedules, so not all alert actions may occur during the scheduled period.


Define what happens when an alert is triggered

Choose actions that occur whenever the trigger conditions are met. You can also set up escalations levels so that different actions occur if the alert has not been acknowledged quickly enough.

Add actions to alerts

By default, what you enter into the Message displayed when this alert field is displayed in the All Active Alerts resource.

You can create a new action or use an action that you have already created. When you reuse an action, you are also reusing all of its configurations, including its schedule and execution settings.

 If you are alerting others through email, SolarWinds recommends that you notify a small number of users while you fine tune your alerts.

1. Click Add Action.
2. Select an action from the list.
See [Alert Actions](#) for a complete list of available actions.

3. Click Configure Action.

4. Enter the necessary information for the action.

Each action requires different information. Select from the list of [Alert Trigger Actions](#) for more information per action.

Some actions require extra configuration steps, specific information, or special software. See [Alert preconfiguration tasks](#).


Each action has the following sections:

- Name of action - This is not required, but makes it easier to organize and find your actions in the Action Manager.
- Time of Day - You can choose different actions to occur at different times of the day or month. For example, if you want to send a page, you might send it to a different person on weekends or holidays rather than during the week.
- Execution settings - You can select both options, neither option, or a single option.
 - Do not execute this action if the alert has been acknowledged already (Recommended)
 - Repeat this action every X minutes until the alert is acknowledged

5. Click Add Action to save it to the list of actions in the alert.

Add a preexisting action to the alert

You can add actions that have already been configured to an alert. For example, if you configured an action to reboot a VM, you can add that action to a separate alert.

 If you use a preexisting action, any configuration change you make to the action, including schedules, is used in every alert the action is assigned.

1. Click Assign Action(s).
2. Select one or more actions from the list.
3. Click Assign.

Add what happens when an alert is not acknowledged


Escalation levels in Orion Platform products refer to user-defined time intervals between when an alert is activated and when a user acknowledges that alert. You can configure the alert to perform different actions per escalation level.

Escalation Level 1 contains all initial actions that you want to occur when the trigger conditions are met and the alert activates.

Escalation Levels 2 and above include all actions you want to occur if no one acknowledged the alert during the previous escalation levels.

For example, if an alert for a critical server activates and all of the recipient or first-level responders are out for training and do not acknowledge the alert, then the actions fire in the second escalation level. These actions may include emailing managers or other backup staff.

1. In an existing alert, click Trigger Actions.
2. Below the action, click Add Escalation Level.
3. Choose how long you want to wait after the previous escalation level before performing the actions in the new escalation level.
4. Enter new actions in this escalation level.

 You can copy all of the actions as Reset Actions. This lets you quickly craft actions to indicate that the issue has been acknowledged or resolved. Click Copy Actions to Reset Actions Tab.

When an alert is triggered, the actions will be performed in the order that they are displayed on the list. You can [test](#) each action to ensure the action does what you expect it to do.

Define what happens when the alert is reset

Use reset actions to perform specific tasks when an alert is no longer active, such as writing to the log that the issue has been acknowledged. Reset actions are usually used to notify others that the situation has been resolved or to write the resolution to a log file.

1. Click Add Action.
2. Select an action from the list.
See [Alert Actions](#) for a complete list of available actions.
3. Click Configure Action.
4. Enter the necessary information for the action.

Each action requires different information. Select from the list of [Alert Actions](#) for more information per action.

Some actions require extra configuration steps, specific information, or special software. See [Preconfiguration Tasks](#).

Each action has the following sections:

- Name of action - This is not required, but can make it easier to organize and find your actions in the Action Manager.
- Time of Day - You can choose different actions to occur at different times of the day or month. For example, if you want to send a page, you might send it to a different person on weekends or holidays than during the week.


5. Click Add Action to save it to the list of reset actions in the alert.

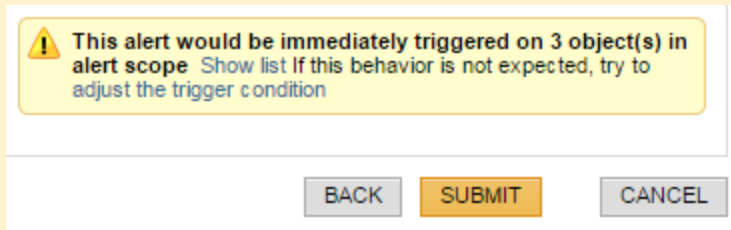
To perform the same actions as when the alert was triggered, click Copy Actions From Trigger Actions Tab. Use the copied trigger actions as a base and modify them to reflect that the alert is no longer active.

When an alert is reset, the actions will be performed in the order that they are listed. You can [test](#) each action to ensure the action does what you expect it to do.

Review the alert's configuration

The Summary tab allows you to check your alert definition before you save any changes.

 Before you click Submit, review the information box above it. This box lists the number of objects that will trigger the alert immediately based on your current trigger condition.



Modify any section by clicking Edit next to that section.

You can [integrate your alerts](#) with other SolarWinds' products, such as AlertCentral or Web Help Desk, by expanding Alert Integration.

Once you have created an alert, it is added to the list of available alerts in the Alert Manager. When the alert is enabled, it immediately monitors your environment for the conditions necessary to trigger it.


Commonly created alerts

The following sections walk you through the easiest method to create common alerts and include tips on how to build more complex alerts.


Alert me when a server goes down


Use the following procedure to create an alert that writes to a log and sends an email when a Windows server goes down.

1. Search for "Email me when a Node goes down" in the Alert Manager.
2. Select the check box next to the alert, and then click Duplicate & Edit.
3. Enter a name for the alert, such as "Notify me when Windows 2008 servers go down".
4. Enable the alert, and then click Trigger Condition or Next.
5. In The scope of alert, select Only following set of objects.
6. Select *Node Machine Type is equal to Windows 2008 Server* as the child condition.


 You can further refine your scope by entering another AND condition. For example, you can enter *Node IP Address starts with 10.10.45* to restrict the scope of the alert to a specific subnet.


7. The actual trigger condition should be *Node Status is equal to Down*.

 Select and enter a value for Condition must exist for more than to prevent being alerted when a node enters the down state frequently within a set amount of time. This prevents you from receiving alerts until the node has been in the down state for longer than the time you have selected.

 You can further suppress alerts by enabling complex conditions in the Advanced options. This allows you to choose to wait until multiple nodes are down before triggering a single alert.

8. Click Reset Condition. The default action should be to reset the alert when the node is up.
9. Click Trigger Actions, and then click Add Action.
10. Select Log the Alert to a file, and then click Configure Action.
 - a. Enter the location of the log. For example, enter `C:\ExampleAlertLog.txt` in the Alert Log Filename Field.
 - b. In the Message text box, type `Node ${N=SwisEntity;M=Caption} is currently down.`
 - c. Click Add Action.
11. Click Add Escalation Level, and enter 5 minutes to wait for 5 minutes before escalating to the next level.
12. Click Add Action in Escalation Level 2, and select Send an Email/Page. Click Configure Action.
 - a. Enter your email as the recipient.
 - b. Add a message.

 You can use variables to customize your message. You can also use a variable that allows you to acknowledge an alert from email (`${N=Alerting;M=AcknowledgeUrl}`).
 - c. Enter your SMTP server information if you have not already done so.

 You can enter a default SMTP server that is used for all your email in the [Configure Default Send Email Action](#) setting.
 - d. Go to Execution settings to click Add Action.
13. Click Copy Actions to Reset Actions Tab, and then click Next.
14. Click Edit next to your logging action, and modify your message to `Node ${N=SwisEntity;M=Caption} is back up.`
15. Click Edit next to your email action, and modify your message. You can also delete the email if you do not want to know if the situation has been resolved.
16. Click Summary to see if any object will trigger the alert, and then click Submit.

Once you have created the alert, it is added to the list of available alerts in the Alert Manager. You can test and view the results of each of your alert actions. See [Testing Alerts](#) for more information.


Discover network device failures

With alerting, Orion Platform products give you the ability to immediately discover whenever any device on your network is experiencing a problem.

Create an alert that uses a custom location property to alert you to a node failure on your monitored network.

Alert on custom properties

The following example creates multiple alerts using the NodeLocation custom property. An alert triggers when a node goes down. Upon triggering, the alert will write to a local log file, send a syslog message, and send an SNMP trap.

 The `${variable}` syntax is required for variables.

1. Click Alerts & Activity > Alerts in the menu bar, and then click Manage Alerts.
2. Select the check box next to Node is down, and then click the Duplicate & Edit button.
3. Click Trigger Condition, and add a child condition. A child condition should already exist for a node being down.
4. Select the node object, and choose NodeLocation in the field drop-down menu. Enter a comparison and value.
5. Click the Trigger Actions, and then click Add Action.
6. Select Log the Alert to a file, and then click Configure Action.
 - a. Enter the log filename in the Alert Log Filename field.
 - b. In the Message text box, type the following:
`Node ${N=SwisEntity;M=Caption} is currently down.`
 - c. Click Add Action.
7. Click Add Action, and select Send a Syslog Message. Click Configure Action.
 - a. Type `127.0.0.1` as the Hostname or IP Address of the Syslog Server, and then type the following in the Message field:
`Node ${N=SwisEntity;M=Caption} is currently down.`
 - b. Click Add Action.
8. Click Add Action, and select Send SNMP Trap. Click Configure Action.
 - a. Type `127.0.0.1` as the SNMP Trap Destination, and then type the following in the Alert Message field:
`Node ${N=SwisEntity;M=Caption} is currently down.`
 - b. Click Next.
 - c. Click Add Action.
9. Click Summary to see if any objects will trigger the alert, and click Submit.

After you have created the alert, it is added to the list of available alerts in the Alert Manager. You can [test](#) and view the results of each of your alert actions.

- You can view results of your Syslog message action in the Web Console or through the Syslog Viewer on your SolarWinds Orion server.
- To view the results of your SNMP Trap action, click Start > All Programs > SolarWinds Orion > Syslog and SNMP Traps > Trap Viewer.

View triggered alerts in the Orion Web Console


View active triggered alerts through Alerts & Activity > Alerts in the menu bar. Click each alert to view the details, which includes a historic count of how frequently the object triggers the alert and other objects that are experiencing the same set of conditions that triggered the alert you are viewing.

You can also add the All Active Alerts resource to any view.

Remove alerts from the Active Alerts list

When an alert has triggered and becomes active, you can then acknowledge it. After an alert is acknowledged, alert actions in higher escalation levels are halted and the time it was acknowledged and the account that acknowledged it is recorded. You can also add notes that other users can read.

Depending on your organization, acknowledging an alert can have different purposes outside of halting further notifications. The most common purposes are to provide an audit trail or to prevent multiple people from working on the same issue.

 You must enable the Allow Account to Clear Events privilege to acknowledge alerts. For more information about access privileges for Orion Web Console users, see [Define what users can access and do](#).

1. Click Alerts & Activity > Alerts in the menu bar.
2. Click Acknowledge next to the alerts you want to acknowledge.

Tip: Depending on how you configure the email, you can acknowledge an alert directly from an email notification.

You can hide acknowledged alerts by clicking More, and then selecting Hide Acknowledged Alerts.

Test alert triggers and actions


You do not have to actually experience a device failure to confirm that your alerts are working. The trigger condition is automatically evaluated and trigger and reset actions can be tested individually.

Test trigger conditions

Alert conditions are automatically evaluated on the Summary tab. Scroll to the bottom of the page and view the information box above the Submit button.

Test alert actions while creating or editing an alert

When you simulate actions, the action will be performed regardless of whether the trigger condition is true. If the action sends a message to a recipient, you should reduce the recipient list to yourself and a small number of team members until you are confident the alert is ready to be enabled in your production environment.

 The Send Email/Page, Play a Sound, and Text to Speech Output actions do not have to fire. You can view what the message will look like when the trigger or reset action fires without performing the action.

1. Click Trigger Actions or Reset Actions.
2. Click Simulate next to the alert action you want to test.
3. Select an object to resolve any variables you have used in your alert action.
4. Click Execute. Test email, play a sound, and text to speech actions without sending an email by clicking Simulate.

Test alert actions in the Action Manager

You can also test actions independent of the trigger or reset conditions by using the Action Manager.


1. Select the action you want to test.
2. Click Test.
3. Select an object to resolve any variables you have used in your alert action.
4. Click Execute. Test email actions without sending an email by clicking Simulate.

After the alert test completes, you can view the results of your alert actions.

- To view the results of your email alert action, open `EvaluationAlertLog` in your Orion folder, typically `<Volume:>\ProgramData\Solarwinds \Logs\Orion\ActionsExecution.log`.
- To view results of your Syslog message action, click Start > All Programs > SolarWinds Orion > Syslog and SNMP Traps > Syslog Viewer.
- To view the results of your Syslog message action, click Start > All Programs > SolarWinds Orion > Syslog and SNMP Traps > Trap Viewer.

Modify multiple alerts or share alerts

Use the Alert Manager to bulk edit multiple alerts. You can enable or disable multiple alerts or add pre-configured actions.


 Alerts must be enabled to be executed. For example, if an alert is scheduled to run for a short period of time each year, it must be enabled so the schedule runs. A disabled alert will **not** be executed, even if it is scheduled to run.

Add actions to alerts without opening the Alert Wizard


Assign actions that you have already configured to alerts. You can assign multiple actions to multiple alerts. Actions are categorized into trigger and reset actions based on how the action was created in the Alert Wizard.

SolarWinds does not provide generic actions due to the differences in intent behind trigger and reset actions. For example, a trigger action to send an email is usually a notification that an event happened, while the associated reset action is usually a notification that the event has been resolved.

Share alerts with others


 SolarWinds customers share their customized alerts in the SolarWinds thwack community. Visit thwack.solarwinds.com to download and import alerts created by others.

Export an alert to save the alert definition as an XML file on your local computer. Alerts are exported to XML and can only be imported from XML. You can send this file to other coworkers or share it in the SolarWinds thwack community.

 Before you share an alert, check the exported file for confidential information, such as SMTP server credentials, and delete before making it public. Also review your company policy on sharing this type of file.

Build complex conditions

Complex conditions are generally enabled by users who are comfortable with building normal trigger conditions, or who have trialed alerts using the normal trigger conditions and require more control over the trigger conditions to better refine the environmental conditions that trigger an alert.

 Do not use complex conditions until you have tested the trigger conditions individually. Creating an alert with complex conditions without testing it may prevent you from receiving important alerts.

1. Navigate to the Trigger Condition page.
2. Expand Advanced options.
3. Select Enable complex conditions.

You can use complex conditions to do the following:

- [Wait for multiple objects to meet the trigger condition before alerting](#)
- [Evaluate multiple condition blocks](#)
- [Evaluate multiple object types](#)

Wait for multiple objects to meet the trigger condition


With complex conditions enabled, you can choose to trigger alerts only when multiple objects meet the trigger condition.

After you have enabled complex conditions, the following option is available in your trigger condition:

☐ Condition must exist for more than minutes ▼

☐ Alert can be triggered if more or equal ▼ objects (at the same time) have met the specified condition

This setting combines all alerts that would be sent for each object into a single alert.

 Do not use this setting until you are confident that the trigger condition is correct. This setting can prevent important alerts from triggering.

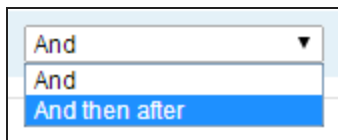
For example, if you were monitoring computers used in a high availability cluster, you may only want to be alerted if more than half the cluster is down at the same time.

1. Enable complex conditions.
2. In the trigger condition, select Alert can be triggered if.
3. Enter how many objects must meet the trigger condition before sending an alert.

Evaluate multiple condition blocks

You can use complex conditions to evaluate multiple condition blocks, or sections, independently. For example, you may want to create an alert when an application is down and when your fail-over server is active for more than an hour.

1. Enable complex conditions.
2. Click Add Section.
3. Select And then after from the drop-down menu between the two condition sections.



4. Choose how long to wait before evaluating the next section.
5. Create the next condition block.

How condition blocks are evaluated

The condition blocks are evaluated at the same time. If they are all true based on the conditions, the alert triggers. For example, condition A, B, and C must be true in order for the alert to trigger.

`(Condition A) & (Condition B) & (Condition C)`

Condition blocks are evaluated using variations of AND, so the trigger condition in each section must be met.

A condition block can be evaluated at a different time than other condition blocks. For example, if you want to be alerted if the backup system is active for more than an hour, you can choose to wait an hour after the primary condition block, where the application going down is the trigger condition, before evaluating whether the backup system is still active.

Evaluate multiple object types

To evaluate multiple object types, you should use complex conditions. Complex conditions can be used to alert on different object types within the same alert. For example, you can create an alert to notify you when IIS is down and the free space on the volume is less than 30 GB.

1. Enable complex conditions.
2. Click Add Section.
3. Choose a different value in I want to alert on.

Manage alert actions

You can edit, test, enable, disable, and delete alert actions from the Action Manager.

Mostly for bulk actions and assigning previously created actions to alerts. View meta data about the action to help troubleshoot alert actions from a single area instead of trying to find the action in an alert.

Assign an action to an alert

You can use actions that you have already configured in multiple alerts. For example, if you have configured an action to email emergency response teams, you can assign this action to multiple alerts. When you assign an alert, it is added to the highest escalation level.

Enable and Disable Alerts

Use the On/Off toggle or select an alert and click Enable/Disable to enable or disable alerts.

Alerts must be enabled to be evaluated. For example, if an alert is scheduled to run for a short period of time each year, it must be enabled so the schedule runs. A disabled alert will not be evaluated, even if it is scheduled to run.

Available alert actions

Orion Platform products provide a variety of actions to signal an alert condition on your network.

Change a custom property

Custom properties are additional fields, such as country, building, asset tag, or serial number, that you can define and store in your SolarWinds Orion database. After properties are added, you can view or filter using them.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select the Change Custom Property option, and then click Configure Action.
3. Under Custom Property Settings, select the custom property and enter the value you want to change it to.
4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.



This is often used to prevent an action from occurring during specific windows.

5. Select how frequently this action occurs for each triggered alert in Execution Settings.
6. Click Add Action.

The action is added to the [trigger](#) or [reset](#) action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the value of the custom property you selected changes.

Dial a paging or SMS service


This action forwards alerts to a paging or SMS service. You must download and install NotePager Pro from Notepage.net to your SolarWinds Orion server to use this action.

For instructions on configuring this action, see the NotePage Technical Support page at <http://www.notepage.net/solar-winds/technicalsupport.htm> and [SolarWinds Network Performance Monitor Integration](#) at www.notepage.net.


Email a web page to users

Send a web page, including content of resources available in the Orion Web Console, to others.


1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select the Email a Web Page option, then click Configure Action.
3. Enter the Recipients.

 Multiple addresses must be separated with commas.

4. Enter the Subject and Message of your alert trigger email/page.
 - For the Optional Web Server Authentication section, select User currently logged in, Another user, or No user defined.

 Use variables to make the message dynamic.

- You can create a dynamic URL to send information about the object that triggered the alert.
5. Enter your SMTP server information.
 6. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.

 This is often used to prevent an action from occurring during specific windows.

7. Select how frequently this action occurs for each triggered alert in Execution Settings.
8. Click Add Action.

The action is added to the [trigger](#) or [reset](#) action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, an email is sent to the recipients.

Create a dynamic URL


Use variables to create a URL that changes based on the object that triggers the alert. Click Insert Variable and search for URL to find all of the variables you can use to create the dynamic URL.

For example, enter `${N=SwisEntity;M=DetailsUrl}` in the URL field to email a link to the Details view of the object that triggered the alert. When the email is sent, the variable resolves to a valid URL such as `http://myserver/Orion/View.aspx?NetObject=N:3` and the email contains the content of the Details view in the body.


Execute an external batch file

There are several circumstances where you may want to execute a program when a specific network event occurs. For example, you may want to run a custom script to reboot your SQL servers.

External programs selected for this action must be executable using a batch file called from the command line. Programs executed this way run in the background. However, you can set the SolarWinds Alerting Engine Service to Interact with Desktop.

 SolarWinds recommends that scripts and batch files be placed on the root of c:\ to simplify the path for the batch file.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select the Execute an External Program option, then click Configure Action.
3. Under Execute an External Program settings:
 - a. Enter the Network path to external program in the field provided.
For example: Use `c:\test.bat`, where `c:\` is the disk on your main poller and `test.bat` is your external program to be executed.
 - b. Select either Define User or No User Defined for Optional Windows Authentication
4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.


 This is often used to prevent an action from occurring during specific windows.

5. Select how frequently this action occurs for each triggered alert in Execution Settings.
6. Click Add Action.

The action is added to the [trigger](#) or [reset](#) action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the external program runs.


Execute an external Visual Basic script

In some situations, you may want to execute a Visual Basic (VB) script when a network event occurs to perform a specific action.

 SolarWinds recommends that scripts and batch files be placed on the root of c:\ to simplify the path for the batch file.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select the Execute an External VB Script option, then click Configure Action.

3. Under Execute an External VB Script settings:
 - a. Select a VB Script Interpreter from the drop down list.
 - b. Enter the Network path to the external VB Script in the field provided.
For example: Use `c:\test.vbs`, where `c:\` is the disk on your main Orion poller and `test.vbs` is your external VB Script to be executed.
 - c. Select either Define User or No User Defined for Optional Windows Authentication
4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.


 This is often used to prevent an action from occurring during specific windows.
5. Select how frequently this action occurs for each triggered alert in Execution Settings.
6. Click Add Action.

The action is added to the [trigger](#) or [reset](#) action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the VB script runs.

Log the alert message to a file

SolarWinds can be configured to log alerts to a designated file which can be viewed at a later time.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select the Log the Alert to a File option, then click Configure Action.
3. Under Log to File Settings:
 - a. Enter the log filename in the Alert Log Filename field.
 - b. Enter a maximum log file size in MB (0 = unlimited).
 - c. Enter the Message of your alert trigger in the field provided.
4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.

 This is often used to prevent an action from occurring during specific windows.
5. Select how frequently this action occurs for each triggered alert in Execution Settings.
6. Click Add Action.


The action is added to the [trigger](#) or [reset](#) action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the alert is logged to the file with the message you created.

Log the alert to the NPM event log

Record when an alert is triggered to the NetPerfMon (NPM) event log on your SolarWinds Orion server or on a remote server for later investigation.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select Log the Alert to the NetPerfMon Event Log from the options, and then click Configure Action

3. Under Log the Alert to the NetPerfMon Event Log settings, enter the text you want written to the file.

 Use variables to make the message dynamic.

4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.
This is often used to prevent an action from occurring during specific windows.
5. Expand Execution Settings to select when the action occurs.
6. Click Add Action.

The action is added to the [trigger](#) or [reset](#) action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the alert is logged to the NPM event log with the message you created.

Change the resource allocation of a virtual machine

If a virtual machine is experiencing performance issues, you can have an alert trigger a specified allocation of resources. This alert management action is available if the integration with Virtualization Manager is enabled.


1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select Manage VM - Change CPU/Memory Resources, and click Configure Action.
3. Enter a name for the action.
4. Under Select Virtual Machine, specify the virtual machine on which you want to adjust the number of CPUs, the memory capacity, or both.
 - a. To change the resource allocation of the virtual machine that triggered the alert, click Execute this action.

 This option is only available if the alert is built to trigger for virtual machines.

- b. To change the resource allocation of a different virtual machine, click Select specific VM, and search for a virtual machine.
5. To power off the virtual machine before changing the resource allocation, and then power it on again after the resource allocation has been changed, select the relevant option.

 If the option is not selected, the action will be performed live on the virtual machine.

6. Under Specify New Resources, specify whether you want to add more resources to the virtual machine, or replace the existing resources with new resources, and then specify the parameters of the new resource or resources.
 - a. Select Number of processors, and specify the number of processors to allocate.
 - b. Select Memory, and specify the memory capacity to allocate.
7. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.

 This is often used to prevent an action from occurring during specific windows.

8. Select how frequently this action occurs for each triggered alert in Execution Settings.
9. Click Add Action.

The action is added to the [trigger](#) or [reset](#) action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the specified CPU and memory resources will be allocated to the virtual machine.


Delete a snapshot of a virtual machine

If a virtual machine is experiencing resource issues, you can have an alert trigger a virtual machine snapshot to be deleted. This alert management action is only available if the integration with Virtualization Manager is enabled.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select Manage VM - Delete Snapshot, and click Configure Action.
3. Under Select Virtual Machine, specify the virtual machine from which you want to delete a snapshot.
 - a. To delete a snapshot of the virtual machine that triggered the alert, click Execute this action.

 This option is only available if the alert is built to trigger for virtual machines.

- b. To delete a snapshot of a different virtual machine, click Select specific VM, and search for a virtual machine.
4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.

 This is often used to prevent an action from occurring during specific windows.

5. Select how frequently this action occurs for each triggered alert in Execution Settings.
6. Click Add Action.

The action is added to the [trigger](#) or [reset](#) action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the snapshot of the specified virtual machine will be deleted.

Move a virtual machine to a different host


If a virtual machine is experiencing issues, you can have an alert trigger the virtual machine to be moved to a different host. This alert management action is only available if the integration with Virtualization Manager is enabled.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select Manage VM - Move to a Different Host, and click Configure Action.
3. Under Select Virtual Machine, specify the virtual machine that you want to move.
 - a. To move the virtual machine that triggered the alert, click Execute this action.

 This option is only available if the alert is built to trigger for virtual machines.

- To apply the action only to virtual machines of a specific vendor, select the relevant option, and specify whether you want to perform to action on Hyper-V or VMware virtual machines.
- b. To move a different virtual machine, click Select specific VM, and search for a virtual machine.

4. To power off the virtual machine before moving it to a different host, and then power it on again after the action has been completed, select the relevant option.

 If the option is not selected, the action will be performed live on the virtual machine.

5. Under Select Target Host, search for the host where you want to move the selected virtual machine.
6. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.
This is often used to prevent an action from occurring during specific windows.
7. Select how frequently this action occurs for each triggered alert in Execution Settings.
8. Click Add Action.

The action is added to the [trigger](#) or [reset](#) action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the specified virtual machine will be moved to a different host.


Move a virtual machine to a different storage

If a virtual machine is experiencing storage issues, you can have an alert trigger the moving of the virtual machine to a different storage location. This alert management action is only available if the integration with Virtualization Manager is enabled.


1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select Manage VM - Move to a Different Storage, and click Configure Action.
3. Under Select Virtual Machine, specify the virtual machine that you want to move.
 - a. To move the virtual machine that triggered the alert, click Execute this action.

 This option is only available if the alert is built to trigger for virtual machines.

- To apply the action only to virtual machines of a specific vendor, select the relevant option, and specify whether you want to perform to action on Hyper-V or VMware virtual machines.
 - b. To move a different virtual machine, click Select specific VM, and search for a virtual machine.
4. To power off the virtual machine before moving it to a different storage, and then power it on again after the action has been completed, select the relevant option.

 If the option is not selected, the action will be performed live on the virtual machine.

5. Under Select Target Datastore, search for the datastore where you want to move the selected virtual machine.
 - a. In a VMware environment, select one of the available datastores.
 - b. In a Hyper-V environment, select one of the available datastores, and click either Use the default location to move the virtual machine to the default location of the datastore, or click Specify custom path, and enter a custom location.
6. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.

 This is often used to prevent an action from occurring during specific windows.

7. Select how frequently this action occurs for each triggered alert in Execution Settings.
8. Click Add Action.

The action is added to the [trigger](#) or [reset](#) action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the specified virtual machine will be moved to a different datastore.

Pause a virtual machine


If a virtual machine is experiencing issues, you can have an alert trigger a pause for the virtual machine. This alert management action is only available if the integration with Virtualization Manager is enabled.

This action can only be configured for Hyper-V virtual machines.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select Manage VM - Pause, and click Configure Action.
3. Under Select Virtual Machine, specify the virtual machine that you want to pause.
 - a. To pause the virtual machine that triggered the alert, click Execute this action.

 This option is only available if the alert is built to trigger for virtual machines.

- b. To pause a different virtual machine, click Select specific VM, and search for a virtual machine.
4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.

 This is often used to prevent an action from occurring during specific windows.

5. Select how frequently this action occurs for each triggered alert in Execution Settings.
6. Click Add Action.


The action is added to the [trigger](#) or [reset](#) action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the specified virtual machine will be paused.


Power off a virtual machine

If a virtual machine is experiencing issues, you can have an alert trigger the virtual machine to be powered off. This alert management action is only available if the integration with Virtualization Manager is enabled.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select Manage VM - Power Off, and click Configure Action.

3. Under Select Virtual Machine, specify the virtual machine that you want to power off.
 - a. To power off the virtual machine that triggered the alert, click Execute this action.

 This option is only available if the alert is built to trigger for virtual machines.
 - b. To power off a different virtual machine, click Select specific VM, and search for a virtual machine.
4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.


 This is often used to prevent an action from occurring during specific windows.
5. Select how frequently this action occurs for each triggered alert in Execution Settings.
6. Click Add Action.


The action is added to the [trigger](#) or [reset](#) action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the specified virtual machine will be powered off.

Power on a virtual machine

If a virtual machine is powered off, you can have an alert trigger the virtual machine to be powered on. This alert management action is only available if the integration with Virtualization Manager is enabled.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select Manage VM - Power On, and click Configure Action.
3. Under Select Virtual Machine, specify the virtual machine that you want to power on.
 - a. To power on the virtual machine that triggered the alert, click Execute this action.

 This option is only available if the alert is built to trigger for virtual machines.
 - b. To power on a different virtual machine, click Select specific VM, and search for a virtual machine.
4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.

 This is often used to prevent an action from occurring during specific windows.
5. Select how frequently this action occurs for each triggered alert in Execution Settings.
6. Click Add Action.

The action is added to the [trigger](#) or [reset](#) action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the specified virtual machine will be powered on.


Restart a virtual machine

If a virtual machine is experiencing issues, you can have an alert trigger the virtual machine to be restarted. This alert management action is only available if the integration with Virtualization Manager is enabled.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select Manage VM - Reboot, and click Configure Action.
3. Under Select Virtual Machine, specify the virtual machine that you want to reboot.
 - a. To reboot the virtual machine that triggered the alert, click Execute this action.

 This option is only available if the alert is built to trigger for virtual machines.

- b. To reboot a different virtual machine, click Select specific VM, and search for a virtual machine.
4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.

 This is often used to prevent an action from occurring during specific windows.

5. Select how frequently this action occurs for each triggered alert in Execution Settings.
6. Click Add Action.

The action is added to the [trigger](#) or [reset](#) action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the specified virtual machine restarts.


Suspend a virtual machine

If a virtual machine is experiencing performance issues, you can have an alert trigger the virtual machine to be suspended. This alert management action is only available if the integration with Virtualization Manager is enabled.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select Manage VM - Suspend, and click Configure Action.
3. Under Select Virtual Machine, specify the virtual machine that you want to suspend.
 - a. To suspend the virtual machine that triggered the alert, click Execute this action.

 This option is only available if the alert is built to trigger for virtual machines.

- b. To suspend a different virtual machine, click Select specific VM, and search for a virtual machine.
4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.

 This is often used to prevent an action from occurring during specific windows.

5. Select how frequently this action occurs for each triggered alert in Execution Settings.
6. Click Add Action.

The action is added to the [trigger](#) or [reset](#) action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the specified virtual machine is suspended.


Take a snapshot of a virtual machine

If a virtual machine is experiencing issues, you can have an alert trigger a snapshot of the virtual machine to be taken. This alert management action is only available if the integration with Virtualization Manager is enabled.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select Manage VM - Take Snapshot, and click Configure Action.
3. Under Select Virtual Machine, specify the virtual machine of which you want to take a snapshot.
 - a. To take a snapshot of the virtual machine that triggered the alert, click Execute this action.

 This option is only available if the alert is built to trigger for virtual machines.

- b. To take a snapshot a different virtual machine, click Select specific VM, and search for a virtual machine.
4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.

 This is often used to prevent an action from occurring during specific windows.

5. Select how frequently this action occurs for each triggered alert in Execution Settings.
6. Click Add Action.

The action is added to the [trigger](#) or [reset](#) action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, a snapshot is taken of the specified virtual machine.

Play a sound when an alert is triggered

The Play a Sound action uses the SolarWinds desktop notification client to play the sound on your computer when an alert arrives.

You must download and install the client on every computer that you want to play a sound when an alert arrives. After installing the desktop notification client, configure which sound you want to play when an alert is received.

Computers that do not have the desktop notification client installed on them do not play a sound when an alert arrives. If you want an alert notification sound to play on your desktop or laptop, you must install and configure the desktop notification client on that computer.

Download the desktop notification client from *<Your SolarWinds Orion server>/DesktopNotificationTool/SolarWinds.DesktopNotificationTool.msi*. Run the installer and follow the on-screen instructions to install the client.

The desktop notification client requires the following information to connect to your SolarWinds Orion server and receive alerts:

- Orion Server Name or IP Address
- Orion User Name
- Password

You can use the server name and credentials that you use to logon to your SolarWinds product.

SolarWinds can be configured to play a sound upon alert trigger or reset. This alert action is frequently used in NOC environments. The SolarWinds Desktop Notification client must be installed on each computer that you want to play a sound. The following procedure configures a sound to play for an alert.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select the Play a Sound option, and then click Configure Action.
3. Under Play a sound settings:
 - If not installed, click Download our desktop notification client to download and install the notification client. From the notification client, select an alert sound.
4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.



This is often used to prevent an action from occurring during specific windows.

5. Select how frequently this action occurs for each triggered alert in Execution Settings.
6. Click Add Action.

The action is added to the [trigger](#) or [reset](#) action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, a sound plays through the client.

Send a Windows Net message

If a computer is experiencing issues, you can have an alert trigger a Windows Net Message to be sent to a specific computer or to all computers.


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.




The only operating systems supporting Windows Net Messaging are Windows Server 2003 and Windows XP or earlier.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select the Send Net Message option, then click Configure Action.
3. Under Send a Net Message settings:

- a. Enter Computer Name or IP address in the field provided.

 You can enter multiple computers or IP addresses by separating them with commas.

- b. Enter the Message of your alert trigger in the field provided.
4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.


 This is often used to prevent an action from occurring during specific windows.

5. Select how frequently this action occurs for each triggered alert in Execution Settings.
6. Click Add Action.


The action is added to the [trigger](#) or [reset](#) action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the message is sent to the selected computers.

Restart IIS sites or application pools

If IIS or application pools are experiencing performance or resource issues, you can use an alert to restart them.

 You must know the IIS Server name and the Site or Application Pool to restart a remote instance of IIS.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select Restart IIS Site/Application Pool from the options, and then click Configure Action.
3. Expand Restart IIS Site/Application Pool Settings.
 - a. Select the IIS Action to Perform from the drop down list.
 - b. Choose the Site or Application Pool.
4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.

 This is often used to prevent an action from occurring during specific windows.

5. Select how frequently this action occurs for each triggered alert in Execution Settings.
6. Click Add Action.


The action is added to the [trigger](#) or [reset](#) action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the selected site or pool restarts.

Send an SNMP trap


SNMP traps signal the occurrence of significant events by sending SNMP messages to a monitoring device. You can have an alert trigger this action to inform you of these events.

This action requires the following information:

- UDP port number
 - SNMP version number
 - SNMP credentials
1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
 2. Select the Send SNMP Trap option, then click Configure Action.
 3. Under Send SNMP Trap Message:
 - a. Enter SNMP Trap Destinations in the field provided.

 Multiple IP Addresses should be separated by commas or semicolons.

- b. Select a [Trap Template](#) from the drop down lists.
4. Enter the Message of your alert trigger in the field provided.
 - a. Optionally click Insert Variable to add variables using the following procedure:
5. Expand SNMP Properties.
 - a. Enter a UDP Port number in the field provided.
 - b. Select an SNMP Version from the drop down list.
 - c. Enter the SNMP Community String in the field provided.
6. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.

 This is often used to prevent an action from occurring during specific windows.

7. Select how frequently this action occurs for each triggered alert in Execution Settings.
8. Click Add Action.

The action is added to the [trigger](#) or [reset](#) action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the SNMP trap message is sent.

Send a GET or POST request

SolarWinds 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.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select the Send a GET or POST Request to a Web Server option, then click Configure Action.
3. Under HTTP request settings:
 - a. Enter a URL in the field provided.
 - b. Select either Use HTTP GET or Use HTTP POST.
4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.

This is often used to prevent an action from occurring during specific windows.

5. Select how frequently this action occurs for each triggered alert in Execution Settings.
6. Click Add Action.

The action is added to the [trigger](#) or [reset](#) action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the GET or POST request is sent to the server. You can view the server logs to confirm that the action occurred.


Send a syslog message

SolarWinds can log received alerts to the syslog of a designated machine for later investigation. The following procedure configures an alert to send a message to a designated syslog server.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select the Send a SysLog Message option, then click Configure Action.
3. Under Send a SysLog message settings:
 - a. Enter the Hostname or IP Address of the syslog server in the field provided.

 Multiple syslog servers should be separated by commas.

- b. Select a Severity and a Facility from the drop down lists.
4. Enter the Message of your alert trigger in the field provided.
 5. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.


 This is often used to prevent an action from occurring during specific windows.

6. Select how frequently this action occurs for each triggered alert in Execution Settings.
7. Click Add Action.

The action is added to the [trigger](#) or [reset](#) action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the syslog message is sent.

Send an email or page

This action sends an email from the product to selected recipients for investigation into the cause of the alert.

 Before configuring this alert you must first configure the default SMTP server the product uses to send email. You can change the default SMTP server later or use different SMTP servers for specific alerts.

You need the following information:

- The SMTP host name or IP address
- The SMTP port number
- Whether the SMTP server uses SSL

- The SMTP credentials, if necessary
- Default sender email address

Configure the SMTP server in the alert action or from the Settings page.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select the Send an Email/Page option, then click Configure Action.
3. Enter recipients and the message.



- You must provide at least one email address in the To field, and multiple addresses must be separated with commas. Some pager systems require a valid reply address to complete the page.
- Messaging is disabled if both the Subject and Message fields are empty.

4. Enter the SNMP information.
5. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.



This is often used to prevent an action from occurring during specific windows.

6. Select how frequently this action occurs for each triggered alert in Execution Settings.
7. Click Add Action.

The action is added to the [trigger](#) or [reset](#) action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the email or page is sent.

Manually set a custom status

Setting a custom status can be useful if you want to change the status of a familiar node, but does not affect actual, polled values. For example, if the custom status is set to Up, but the server is down or unresponsive, packet loss continues to be 100%. Alerts based on the status do not trigger in this instance, but alerts based on a polled value, such as packet loss, do trigger.



When the status is set with an alert, the status does not update to the actual, polled status. The status must be switched manually to a different status or configured to use the polled status. Change the status to use the polled status from the node details page or create a reset action to set the status to use the polled status.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select the Set Custom Status option, then click Configure Action.
3. Under Change Object Status Manually:
 - a. Select Change to a specific status if you are creating a trigger action, and choose a status.
 - b. Select Use polled status if you are creating a reset action.
4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.



This is often used to prevent an action from occurring during specific windows.

5. Select how frequently this action occurs for each triggered alert in Execution Settings.
6. Click Add Action.


The action is added to the [trigger](#) or [reset](#) action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the status for the object changes.

Use the speech synthesizer to read alerts


The Text to Speech Output action uses the SolarWinds desktop notification client and your computer's speech synthesizer to convert text messages-to-speech messages. The action notifies users of new alerts by reading the alert out loud. This capability is especially helpful for users who are visually impaired or who are not always at their desks to read alerts onscreen.

Download and install the client on each computer that you want to play a sound. Then configure which synthesizer you want to play.

SolarWinds uses Microsoft® Speech Synthesis Engine version 5.0. If you are under active SolarWinds maintenance, you may also install and use other text-to-speech engines by visiting the SolarWinds website. The following procedure configures text-to-speech output for an alert trigger or reset.

 Due to restrictions on Windows service applications, the Text to Speech action is not available to SolarWinds installations on Windows 7 or Windows Server 2008 and higher.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select the Text to Speech Output option, then click Configure Action.
3. Under Text to Speech Output settings click Download our desktop notification client to download, install, and configure the notification client.
4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.

 This is often used to prevent an action from occurring during specific windows.

5. Select how frequently this action occurs for each triggered alert in Execution Settings.
6. Click Add Action.

The action is added to the [trigger](#) or [reset](#) action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the message is read.

Log an alert to the Windows Event Log on a specific server

You may specify that an alert be logged to the Windows Event Log either on the SolarWinds server or on a remote server for later investigation.

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select the Windows Event Log option, then click Configure Action.

3. Under Event Log Settings:
 - a. Select either Use Event Log Message on Network Performance Monitor Server or Use Event Log Message on a Remote Server.
 - b. Enter the Message of your alert trigger.
4. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.



This is often used to prevent an action from occurring during specific windows.

5. Select how frequently this action occurs for each triggered alert in Execution Settings.
6. Click Add Action.

The action is added to the [trigger](#) or [reset](#) action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, the alert message is added to the Windows Event log.

Create a ServiceNow incident

This alert management action is only available if the integration with ServiceNow® is enabled.

For information about configuring ServiceNow integration, see [Configure an Orion Platform product with ServiceNow](#).

1. When editing or adding an alert, click Add Action in the Trigger or Reset Action section of the Alert Wizard.
2. Select Create ServiceNow Incident, and click Configure Action.
3. Under Select ServiceNow Instance, specify the ServiceNow instance where you want to create the incident.
4. Under Incident Detail, define the properties of an incident template that will be used for new incidents. For example, here you can define the urgency, impact, and other properties of incidents. Text areas can hold macro variables to add information about alerts and alert objects.



If the property you want is not displayed in the Incident Detail section, click Select Properties at the bottom of the section, and select the property from the list.


5. Under State Management, define the status of the incident when the incident is reset, reopened, acknowledged, and closed. You can also specify notes to be added to the incident.
6. Schedule the action by selecting Time of Day > Use special Time of Day schedule for this action. This schedule only applies to the alert action you are editing.




This is often used to prevent an action from occurring during specific windows.

7. Select how frequently this action occurs for each triggered alert in Execution Settings.
8. Click Add Action.

The action is added to the [trigger](#) or [reset](#) action list, and you can test the action using the Simulate button. When the trigger or reset conditions of the alert are met, an incident will be created or updated in the specified ServiceNow instance.

 When you use this alert action, we recommend that you only use it on the trigger tab. It is also recommended that you only use one ServiceNow action per alert.

To deactivate the integrated behavior, remove the alert action from the alert definition.

 You can specify one alert action for one ServiceNow instance. To create an incident in another ServiceNow instance, specify another alert action and use a different ServiceNow instance.

Changes in the alerting engine

As of Orion Platform version 2015.1, alerts are no longer created with the desktop-based, Advanced Alerts Manager or Basic Alerts Manager. Alerts are instead created and managed in the SolarWinds Orion Web Console.

Alerts that you created in the desktop-based Alert Manager are migrated to the web-based alerting engine when upgrading to Core version 2015.1 or later. Some alerts may not be successfully migrated and include information about why they were not migrated in the migration log. You can view the alert migration logs in the informational banners displayed after you update your installation.

Changed or removed functionality

The suppression section has not been carried over to web-based alerting. Use options, such as Condition must exist for more than, in the trigger conditions to accomplish similar tasks.

Database changes

The following are a list of tables that have been changed that you may be using in custom SQL queries:

- Engines has been renamed to AllEngines.
- Nodes has been split into NodesCustomProperties, NodesData, and NodesStatistics.
- History has been split into table-specific history tables, such as the AlertHistory table.

The new alerting engine also includes the following new alerting tables:

- Actions
- ActionsAssignments
- ActionsProperties
- AlertActive
- AlertActiveObjects
- AlertConditionState
- AlertConfigurations
- AlertHistory
- AlertHistoryView (introduced in 2015.1.3)
- AlertMigrationLog

- AlertObjects
- AlertSchedules

For a list of database changes from Orion Platform version 2014.2 to version 2016.1, including new tables, column changes, or data constraint or data type changes, see the online [Database Changes](#) spreadsheet.

Macro or variable changes

The following variables are no longer valid:

- `${Property}` - The property the alert is monitoring. You can select a new variable with the specific property you want to view.
- `${TriggeredValue}` - The value that triggered the alert. You can select a new variable with the specific property you want to view.
- `${AlertStartTime}` - When the alert active. You can use the Time of Day scheduler to control when the alert is active.
- `${AlertEndTime}` - When the alert is no longer active. You can use the Time of Day scheduler to control when the alert is not active.
- `${ObjectSubType}` - Determines if the node supports SNMP or is ICMP only. You can use `Node.ObjectSubType` as the macro name.

Alert migration to the web

The Advanced Alert Manager and the Basic Alert Manager are deprecated in SolarWinds Orion Core 2015.1 and later. A web-based alerting engine replaces the previous alerting engine and includes new alerting variables.

To facilitate using the web-based alerting engine, part of the upgrade process migrates alerts created with the desktop-based alerting engine to the web-based alerting engine. All alerts are migrated, including alerts that are disabled.

Migration issues

Some alerts may not be successfully migrated. The migration log records all alerts that are migrated and includes error messages for alerts that either cannot be migrated or that are not migrated successfully.

Common reasons that migration may not be successful include:

- [Invalid alert variables or macros](#) - Some variables are no longer supported.
- Invalid conditions - Some conditions are no longer supported.
- Large alert scope - The number of objects that are relevant to an alert may be too large to migrate.


Limitations to migrated alerts

After an alert has been migrated, you can only view the alert definition through the web-based Alert Manager. You can no longer click the alert in the views.

Share alerts with other SolarWinds products

Alerts may be shared with selected other SolarWinds products that are not part of the SolarWinds Orion Platform, such as AlertCentral and Web Help Desk.

1. On the Alert Summary page, expand Alert Integration.
2. Select the Integrate alert with other SolarWinds check box.
3. Provide an appropriate Alert Subject. You can choose to use this name as the subject field for the alert.
4. Choose the alert Severity.

 This information may be used to determine how a shared alert is handled by the other product.

5. Include additional alert properties in the alert by clicking Insert Variable and choosing the ones you want to include. This ensures that the variables you used in the alert message are translated correctly to the other product.


Configure ServiceNow

Integrate an Orion Platform product with ServiceNow

Integrate your Orion Platform product with ServiceNow® to automatically open new ServiceNow tickets based on critical events defined in your Orion Platform product.

The integration with ServiceNow allows for two-way communication between your Orion Platform product and ServiceNow. By integrating the two systems, you can:

- Automatically create incidents in ServiceNow and assign them to the correct tech or group
- Synchronize the acknowledgment of alerts and tickets in SolarWinds Orion and ServiceNow
- Update, close, and reopen tickets
- Suppress ticket storms

 You can integrate one Orion Platform product with multiple ServiceNow instances.

The integration requires NPM 12.0, SAM 6.3, or any other Orion Platform product running Core version 2016.1 or later.

Before you begin

Before you can configure the integration details in your SolarWinds Orion product, check the prerequisites and configure your ServiceNow instance.

- The communication between the SolarWinds server and the ServiceNow instance uses HTTPS port 443. Open this port for outbound communication.
- For minimum hardware and software requirements, see the administrator guide of your product.

- Download the ServiceNow integration application from the [ServiceNow app store](#).
- [Install the integration app and configure your ServiceNow instance for the integration.](#)

Install and configure the SolarWinds Alert Integration application in ServiceNow

The SolarWinds Alert Integration application enables the communication between your SolarWinds server and the ServiceNow instance.

After downloading the SolarWinds Alert Integration application from the ServiceNow store, deploy the application in ServiceNow.

1. Navigate to your downloaded system applications.
2. Locate the SolarWinds Alert Integration application, and click Install.

When the installation is complete, the caption of the Install button will change to Installed.

After the installation is complete, SolarWinds recommends that you create a ServiceNow integration user with Web service access only.

Create a ServiceNow integration user with Web service access only

1. Navigate to the user administration section in ServiceNow, and create a new user.
2. Provide a user ID, a password, and other required information.
3. Specify that the new user should have Web service access only.
4. Edit the newly created user, and add the `x_sow_intapp.integration_user` role to the role list.

After installing the integration application and creating an integration user, you can now [configure the integration with ServiceNow in your SolarWinds Orion server](#).

Configure an Orion Platform product with ServiceNow

After completing the [configuration of the integration in ServiceNow](#), you can configure the integration to be able to automatically create, update, and resolve alerts that were raised in your Orion Platform product in your ServiceNow® instance.

1. In the Orion Web Console, click Settings > All Settings.
2. In the Alerts & Reports group, click ServiceNow Instances.
3. Click Add Instance.
4. Enter a name and the URL for the ServiceNow instance.
5. Enter the ServiceNow credentials:
 - Username
The user name of the account that is configured for the SolarWinds integration role.
 - Password
6. Test the connection to your ServiceNow instance. If the connection is not working, you receive descriptive messages to help you solve the issue.

7. If you are accessing your ServiceNow instance through a HTTP proxy, select Use a HTTP proxy server, and click the Configure your HTTP proxy settings link to edit the details. For more information, see [Configure web proxy settings](#).
8. Click Save.

Configure web proxy settings

If your SolarWinds Orion server does not have Internet access, you can use a proxy server to allow the Orion server to connect to certain pages and websites. Use a proxy server to:

- Access the [thwack community](#)
- Access the product blog
- Check for maintenance updates
- Access the ServiceNow® instance you integrated with your SolarWinds Orion server. For information about integrating SolarWinds Orion with ServiceNow, see [Integrate an Orion Platform product with ServiceNow](#).

To configure web proxy settings:

1. In the Orion Web Console, click Settings > All Settings > Product specific settings > Proxy Settings.
2. Select Use the following settings, and specify the IP address and port number of the proxy server.
3. If the proxy server requires authentication, select the check box, and specify the user name and password.
4. Enter a URL, and click Test connection to verify that you can reach the destination address through the proxy.
5. Click Save.

How conditions are evaluated

Conditions are a set of user-defined rules governing alert triggers and resets.

All child conditions must be satisfied (AND)

Every child condition in the group must be true before the alert is triggered.

In the following example, there are three child conditions.

- 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%.

You can also think of the condition as:

```
Alert when: (Node Status = Up) AND (Percent Loss >= 75) AND (CPU Load >= 85)
```

At least one child condition must be satisfied (OR)

At least one child condition must be true before the alert is triggered.

In this example the alert trigger reads:

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.

All child conditions must NOT be satisfied

Every child condition must be false before the alert is triggered.

In this example the alert trigger reads:

Do not alert when: (Node Status = Down) AND (Percent Loss <= 75) AND (CPU Load <= 85)

Alternatively, you can think of the trigger as:

Alert when: (Node Status != Down) AND (Percent Loss > 75) AND (CPU Load > 85)

The conditions have been inverted (Node Status = Down instead of Node Status = Up).

At least one child condition must NOT be satisfied

Any child condition must be false before the alert is triggered.

In this example the alert trigger reads:

Do not alert when: (Node Status = Down) OR (Percent Loss <= 75) OR (CPU Load <= 85)

Alternatively, you can think of the trigger as:

Alert when: (Node Status != Down) OR (Percent Loss > 75) OR (CPU Load > 85)

The conditions have been inverted (Node Status = Down instead of Node Status = Up).


General alert variables

The following are valid, general alert variables.

GENERAL VARIABLE	DESCRIPTION
<code>\${N=Alerting;M=AlertID}</code>	The ID of the alert
<code>\${N=Alerting;M=AlertName}</code>	The name of the alert from the alert field Name of alert definition in Alert Properties
<code>\${N=Alerting;M=AlertDescription}</code>	The description of the alert from the alert field Description of alert definition in Alert Properties
<code>\${N=Alerting;M=AlertDetailsURL}</code>	The URL used to get more information about the triggered alert
<code>\${N=Alerting;M=AlertMessage}</code>	The alert message from the alert field Message displayed when

GENERAL VARIABLE	DESCRIPTION
	this alert is triggered in Trigger Actions
<code>\${N=Alerting;M=DownTime}</code>	The amount of time the alert has been active
<code>\${N=Alerting;M=ObjectType}</code>	The object type that the alert is monitoring
<code>\${N=Alerting;M=Severity}</code>	The severity of the alert from the alert field Severity of Alert in Alert Properties
<code>\${N=Alerting;M=LastEdit}</code>	The last time the alert definition has been edited
<code>\${N=Alerting;M=Acknowledged}</code>	Acknowledged status
<code>\${N=Alerting;M=AcknowledgedBy}</code>	Who the alert was acknowledged by
<code>\${N=Alerting;M=AcknowledgedTime}</code>	Time the alert was acknowledged
<code>\${N=Alerting;M=Notes}</code>	Information from the Notes field when you acknowledge alerts through the Web Console
<code>\${N=Alerting;M=AlertTriggerCount}</code>	Count of triggers
<code>\${N=Alerting;M=AlertTriggerTime}</code>	Date and time of the last event for this alert. (Windows control panel defined "Short Date" and "Short Time")
<code>\${N=Generic;M=Application}</code>	SolarWinds application information
<code>\${N=Generic;M=Copyright}</code>	Copyright information
<code>\${N=Generic;M=Release}</code>	Release information
<code>\${N=Generic;M=Version}</code>	Version of the SolarWinds software package

It is possible to use previous generation variables, for example `${NodeName}`. However, when using the variable picker, the new format is displayed by default. Previous generation variables can only be entered manually.

 Some variables are no longer valid.

Defunct alert variables


The following variables are no longer valid:

- `${Property}` - The property the alert is monitoring. You can select a new variable with the specific property you want to view.
- `${TriggeredValue}` - The value that triggered the alert. You can select a new variable with the specific property you want to view.

- `${AlertStartTime}` - When the alert active. You can use the Time of Day scheduler to control when the alert is active.
- `${AlertEndTime}` - When the alert is no longer active. You can use the Time of Day scheduler to control when the alert is not active.
- `${ObjectSubType}` - Determines if the node supports SNMP or is ICMP only. You can use `Node.ObjectSubType` as the macro name.

Manage the Orion Web Console

The Orion Web Console is an integral part of the Orion Platform products and can be accessed from virtually any computer connected to the Internet.

 To customize the Orion Web Console, you need administrator rights.

You can customize the Orion Web Console for multiple users, update polling settings and thresholds, and store individually customized views as user profiles.

Log in to the Orion Web Console

1. Launch the Orion Web Console using either of the following methods:
 - Start Orion Web Console in your SolarWinds Orion program folder.
 - Launch a browser and enter `http://ip_address` or `http://hostname`, where *ip_address* is the IP address of your SolarWinds Orion server, or where *hostname* is the domain name of your SolarWinds Orion server.
2. Enter the user name and password, and click Login.

Manage Orion Polling Engines

To optimize your polling engines for best performance, SolarWinds recommends tuning them regularly. If you use more than one polling engine, you must balance the load so each engine performs best.

View information about the performance of all polling engines in your Orion Platform product installation in the Polling Engine view by clicking Settings > All Settings, and then Polling Engines in the Details group.

Modify polling engine settings by clicking Settings > All Settings, and then Polling Settings in the Thresholds & Polling group.

Use Additional Polling Engines

Because larger networks can quickly become too extensive, use Additional Polling Engines to increase the monitoring capacity of your SolarWinds NPM installation.


Required Settings

If you have an additional polling engine, you need to add its IP address to Windows Servers on the Security tab.

Make sure that the following options are set:

- Ensure that a case-sensitive community name has been specified.
- Ensure that Accept SNMP packets from any host is selected OR ensure that the ipMonitor system is listed within the Accept SNMP packets from these hosts list.

- Ensure that your network devices allow SNMP access from the new polling engine. On Cisco devices, you can for example modify the Access Control List.

 In SolarWinds NPM versions 10.2 and later, Additional Polling Engines no longer require that the primary polling engine in your environment is running to support data collection for Universal Device Pollers, and EnergyWise, ESX Server, and wireless devices.


View a polling engine status

View information about the performance of all polling engines in your Orion Platform product installation in the Polling Engine view by clicking Settings > All Settings, and then Polling Engines in the Details group.


Modify polling engine settings by clicking Settings > All Settings, and then Polling Settings in the Thresholds & Polling group.

Update polling settings

Click Settings > All Settings, and in the Thresholds & Polling group, click Polling Settings to configure your poller.

 Depending on the Orion Platform products you have installed, additional polling settings may be available. See your SolarWinds Orion Administrator Guide for more information about the settings.

Configure polling interval settings

 You can improve your SolarWinds Orion server performance by entering longer polling intervals.

Configure how frequently the polling engine requests information from devices.

Default Node Poll Interval

The interval for polling the status and response time of monitored devices. By default, this interval is 120 seconds.

Default Interface Poll Interval (SolarWinds NPM)

The interval for polling the status and response time of monitored interfaces. By default, this interval is 120 seconds. Available only if SolarWinds NPM is installed.


Default Volume Poll Interval

The interval for polling the status and response time of volumes. By default, this interval is 120 seconds.

Default Rediscovery Interval

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

Rediscovery scans your network for changes to your monitored nodes. If you want to discover changes to your environment, schedule a [network discovery](#) to occur on a periodic basis and check the [scheduled discovery results](#).


 The minimum rediscovery interval is five minutes (in earlier versions, the interval was one minute). You cannot submit polling interval settings if the default rediscovery interval is not set to at least five minutes.

Lock Custom Values

Select this option to store the configured custom ICMP polling interval settings.

Re-Apply Polling Intervals

Apply the settings specified in this section to all objects in the database by clicking Re-Apply Polling Intervals. Click Submit to use the current settings for new objects.

 If you leave the page without submitting the changes, your settings will be applied to objects in the database, but will not be saved. For objects added to the database in the future, the saved settings will be used. Not submitting the changes can result in different settings for objects that are already in the database, and different settings for newly added objects.

Configure polling statistics intervals

Configure the default polling intervals for device statistics. To apply poller settings, click Re-Apply Polling Statistic Intervals.

Default Node Topology Poll Interval

Configure the interval for polling topology data of monitored devices. By default, this interval is 30 minutes. To reduce network load, increase this polling interval.

Default Node Statistics Poll Interval

Configure the interval for polling performance statistics of monitored devices. By default, this interval is 10 minutes.

Default Interface Statistics Poll Interval


Configure the interval for polling performance statistics of monitored interfaces. By default, this interval is 9 minutes.

Default Volume Statistics Poll Interval

Configure the interval for polling the performance statistics of volumes. By default, this interval is 15 minutes.

Configure the dynamic IP address and hostname resolution

Select the default IP address version (IPv4 or IPv6) to use when resolving the address of monitored dual stack devices.


 A dual stack device is capable of providing IP addresses in both IPv4 and IPv6 formats.


To monitor IPv6 devices, enable IPv6 on the SolarWinds Orion server.


Immediately change the settings by clicking Re-Apply Resolution Preference.

Configure Database Settings

Configure the time of day when the database maintenance runs, and how long data are retained in the SolarWinds Orion database.

 Shortening retention periods can improve the database performance.

 Changing default settings can require additional space in the SolarWinds Orion database. Consider your SQL environment resources, such as disk space and hardware configuration before you change the retention periods.

 It can take more than 10 minutes to propagate some changes to SolarWinds Orion database settings.

Archive Time

Configure the time of day when the maintenance of the SolarWinds Orion database runs.

Auditing Trails Retention

Specify the number of days until the audit trails statistics are deleted from the database.

Detailed Statistics Retention

Specify the time period in which all statistics collected in the SolarWinds Orion database are summarized into hourly statistics. By default, this period is seven days.

Hourly Statistics Retention

Specify the time period in which all statistics collected in the SolarWinds Orion database are summarized into daily statistics. By default, this period is 30 days.

Daily Statistics Retention

Specify how long daily statistics are kept in the SolarWinds Orion database. After the specified time, the daily statistics are deleted. By default, this period is 365 days.

Container Detailed Statistics Retention

Specify when group statistics are summarized into hourly statistics. The default is seven days.

Container Hourly Statistics Retention

Specify when hourly group statistics are summarized into daily statistics. The default is 30 days.

Container Daily Statistics Retention

Specify how long group statistics are kept in the SolarWinds Orion database. The default is 365 days.

Baseline Data Collection Duration

Specify the number of days that are included into the [baseline](#).

Interface Baseline Calculation Frequency

Specify how often the interface baseline calculation runs.

Detailed Interface Availability Statistics Retention

Specify the number of days until the detailed interface availability statistics in the SolarWinds Orion database are summarized into hourly statistics. By default, this period is seven days.

Hourly Interface Availability Statistics Retention

Specify the number of days until the hourly interface availability statistics are summarized into daily statistics. By default, this period is 30 days.

Daily Interface Availability Statistics Retention

Specify the number of days until the daily interface availability statistics are deleted from the database. By default, this period is 365 days.

Detailed Wireless Statistics Retention

Specify the number of days until the detailed wireless statistics in the SolarWinds Orion database are summarized into hourly statistics. By default, this period is seven days.

Hourly Wireless Statistics Retention

Specify the number of days until the hourly wireless statistics are summarized into daily statistics. By default, this period is 30 days.

Daily Wireless Statistics Retention

Specify the number of days until the daily wireless statistics are deleted from the database. By default, this period is 365 days.

Detailed UnDP Statistics Retention

Specify the number of days until the detailed UnDP statistics are summarized into hourly statistics.

Hourly UnDP Statistics Retention

Specify the number of days until the hourly UnDP statistics are summarized into daily statistics.

Daily UnDP Statistics Retention

Specify the number of days until the daily UnDP statistics are deleted from the database.

Events Retention

Specify the number of days until the all network events data are deleted from the SolarWinds Orion database. By default, this period is 30 days.

Syslog Messages Retention

Specify the number of days until all data related to received Syslog messages are deleted from the SolarWinds Orion database. By default, this period is seven days.

Trap Messages Retention

Specify the number of days until all data related to received trap messages are deleted from the SolarWinds Orion database. By default, this period is 30 days.

Max Alert Execution Time

Specify the time period until the alerts are disabled if they are not executed successfully. If the defined alert condition persists, Orion continues trying to execute the alert.

Alert Acknowledge URL Text

Provide text that is displayed when alerts are available for acknowledgment over the web. When viewing an alert, click the text to acknowledge the alert.

Allow alert actions for unmanaged objects

Select this option if you want the SolarWinds Alerting Engine to execute configured alert actions for unmanaged objects.



Enabling this option increases the processing load on both the SolarWinds server and the database server.

Discovery Retention

Specify the number of days until all network discovery profiles are deleted from the SolarWinds Orion database. The retention starts when a discovery is first defined. By default, this period is 60 days.

Downtime History Retention

Specify the number of days until the downtime history is deleted from the database. By default, this period is seven days.

Configure network settings

Configure the settings related to ICMP and SNMP requests.

ICMP Timeout

Configure the period after which all ICMP (ping) requests made by the poller time out if a response is not received. By default, this period is 2500 ms.

ICMP Data

Specify the text that is included in all ICMP packets sent by the poller.

SNMP Timeout

Configure the period after which all SNMP requests made by the poller time out if a response is not received. By default, this period is 2500 ms.

SNMP Retries

Configure the number of times the poller retries the request if there is no response to an SNMP poll request within the SNMP timeout period. By default, this value is 2.

UCS API Timeout

Configure the period after which all UCS API requests made by the poller time out if a response is not received. By default, this period is 240 seconds.

Perform reverse DNS lookup

Select this option if you want the SolarWinds Orion server to perform reverse DNS lookups on monitored DHCP nodes. By default, reverse DNS lookup for DHCP nodes is enabled.

Configure calculations and threshold settings

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

Availability Calculation (advanced)

Configure the type of calculation that is performed to [determine device availability](#).

Baseline Calculation (advanced)


Enable this option to ensure that baselines for the transmission rates of the elements of your network are calculated upon startup. This [baseline](#) is used as a starting point for any comparison statistics.

Enable Auto Dependencies

Enable this option to ensure that the SolarWinds Orion server collates topology information from networked devices and creates dependency links between devices.

Allow Secure Data on Web (advanced)

Select this option if your network is secure and you want to allow users to view community strings and other potentially sensitive information in the Orion Web Console. Sensitive information about your network is not available in the Orion Web Console.

 This setting does not affect the display of custom reports that you export to the web.

Node Warning Level

Configure the period after which devices that do not respond to polling are displayed as Down in the Orion Web Console. By default, this period is 120 seconds.

Counter Rollover

Specify a method that decides [what happens if a polled value is less than the previous polled value](#).

Default Assigned IP Address

Specify the node IP address that is recorded if DNS resolution fails for a monitored node. If you leave this field blank, no IP address will be stored.

Disable HTML Encoding for Polled Data

Specify if you want to HTML-encode polled data. HTML encoding provides added security for polled data in the Orion Web Console.

Calculate node availability

Determine the availability under Orion Polling Settings > Calculations & Thresholds > Availability Calculation by using one of the following methods.

Node Status

The default method is based on 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.


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 view. 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 view.

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. This provides an average availability over the selected time period.

Percent Packet Loss

This method is a more complicated calculation that bases the availability of a selected node on its packet loss percentage. 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.

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. This provides an average availability over time.

 The Percent Packet Loss method introduces a historical dependency into each availability node record. It is best practice to leave calculations based on Node Status unless you specifically need node availability based on packet loss.

Define baselines for nodes


Using the baseline feature, you can display baselines on different charts in the Orion Web Console.

Define a baseline for an individual node

1. Click Edit thresholds on the resource, and select the thresholds you want to edit.
2. Select Override Global Orion Threshold or Set Dynamic Threshold, and set either a static threshold, or click Use Dynamic Baseline Thresholds to define a formula for calculating a baseline. For information about threshold types, see [Thresholds](#).
3. Click Submit.


Define a baseline for multiple nodes

1. Click Settings > All Settings > Node & Group Management > Manage Virtual Devices in the Orion Web Console.
2. Click the Thresholds tab.
3. Select the entity type for which you want to configure a baseline threshold from the Show list.
4. Select the nodes for which you want to configure a baseline.
5. Click Edit Thresholds, and select the thresholds you want to edit.
6. Select Override Global Orion Threshold or Set Dynamic Threshold, and set either a static threshold, or click Use Dynamic Baseline Thresholds to define a formula for calculating a baseline.
7. Click Submit.

 For example, to configure thresholds for all virtual machines under a given host, first select all vNodes, and deselect the vNodes for which you do not want to define thresholds.

Assign credentials to virtual servers

If you did not provide the credentials within the Network Sonar Discovery, or when adding the node to the database, assign credentials based on the server vendor.

 VMware ESX or vCenter accounts used as credentials must have read-only permissions as a minimum.

Assign credentials to Hyper-V servers

1. Click Settings > All Settings > Manage Virtual Devices.
2. On the Virtualization Polling Settings page, select Hyper-V.
3. Select a Hyper-V server from the list, and click Edit Properties.
4. Under Polling Method > Windows Servers, choose a credential, or select New Credential, and specify a new credential set.
5. Click Test to verify the credential set, and click Submit.

Assign credentials to VMware servers

1. Click Settings > All Settings > Manage Virtual Devices.
2. On the Virtualization Polling Settings page, select VMware.
3. Select a VMware server from the list, and click Assign ESX Credential.
4. Choose an existing credential, or specify a new credential set.
5. Click Test to verify the credential set, and click Assign Credential to assign it to the VMware server.

Set general thresholds

Orion general thresholds are used for nodes and volumes in all Orion Platform products.


 Thresholds set on specific objects are not affected by changes made to general thresholds.

1. Click Settings > All Settings in the menu bar.
2. In the Thresholds and Polling grouping, click Orion Thresholds.
3. Enter values for Critical Level or Warning Level for selected thresholds.

PERCENT PACKET LOSS	
Critical Level	<input type="text" value="50"/>
Warning Level	<input type="text" value="30"/>


4. Click Submit.

Monitored thresholds are changed on a global level.

 To access thresholds for virtual objects, go to Settings, and click Virtualization Thresholds in the Thresholds & Polling grouping.

Set how many retries are necessary before packet loss is reported


Configure the Response Time Retry Count for your polling engine to manage the amount of network-wide packet loss reported by Orion Platform products. This setting specifies the number of times Orion retries ICMP pings on a monitored device before packet loss is reported.

 This configuration change requires an insertion into your SolarWinds Orion database. SolarWinds recommends installing and using the SQL Server Management Studio to perform this insertion.

To configure the Response Time Retry Count for your polling engine:

1. Create a full backup of the SolarWinds Orion database.
2. To start the Orion Service Manager, click SolarWinds Orion > Advanced Features program folder.
3. Click Shutdown Everything.

4. On your SolarWinds Orion database server, execute the following query on the SolarWinds Orion database.


 Specify your own custom values for Maximum, CurrentValue, and DefaultValue.


```
INSERT INTO [OrionDatabaseName].[dbo].[Settings] (SettingID, Name,
Description, Units, Minimum, Maximum, CurrentValue, DefaultValue) VALUES
('SWNetPerfMon-Settings-Response Time Retry Count', 'Response Time Retry
Count', 'Number of times Orion retries ICMP pings on a monitored device
before reporting packet loss', '', 1, Maximum, CurrentValue, DefaultValue)
```

5. To start the Orion Service Manager, click SolarWinds Orion > Advanced Features program folder.
6. Click Start Everything.


Set the node warning level

A device may drop packets or fail to respond to a poll for many reasons. When the device fails to respond, the device status is changed from Up to Warning. You can specify how long a node can remain in the Warning status before it is marked as Down. During the interval specified, the service continually checks the node status.

 Some of the events or alerts for down nodes you are receiving can inform you about nodes that are not actually down. Their status can be caused by intermittent packet loss on the network.

 Set the Node Warning Interval to a higher value to avoid false notifications.


1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. In the Thresholds & Polling grouping, select Polling Settings.
4. Scroll down to Calculations & Thresholds, and enter a higher value for Node Warning Level.

 The default Node Warning Level interval is 120 seconds.

5. Click Submit.

Delete polling engines

If there are polling engines in your SolarWinds environment that have no assigned monitored objects, you can delete them from the Polling Engine details view.


-  ■ This method for deleting polling engines from your SolarWinds environment is only available for polling engines that no longer have objects assigned for monitoring.
- If you want to delete an existing polling engine to which monitored objects are currently assigned, use Node Management to reassign monitored objects to other polling engines, and delete the polling engine as indicated in this procedure.

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. Click Polling Engines in the Details group.

4. Verify that the Elements listing for the polling engine you want to delete reports "0 elements assigned," and click Delete unused polling engine.
5. Click Yes, delete to confirm the deletion.

Thresholds

Many Orion Web Console resources can display error and warning states when a monitored value on a device exceeds a threshold. Orion Platform products come with predefined static thresholds for monitored statistics, but you can override these and customize them for each object.

 You can use thresholds to define trigger conditions for alerts.

Orion Platform products provide two threshold levels: critical and warning. A value that crosses a warning threshold appears yellow, and a critical threshold appears red.

If you want to change the predefined value for a threshold, use a static threshold or a dynamic baseline threshold.

- A **Static threshold** is a constant value that you set for a threshold. For example, the warning threshold for response time might be 500 ms, and the critical value might be 1000 ms. You should be familiar with the performance of that object to know what a reasonable value for a static threshold is.
- A **Dynamic baseline threshold** uses deviations. Data for a statistic are collected for a week, and then used to calculate the mean and standard deviation. The warning and critical threshold values are defined as 2 and 3 standard deviations above the mean, respectively. For example, if the mean value for packet loss for a specific node is 0%, the warning threshold for packet loss would be 3% (+2 standard deviations) and the critical threshold would be 4% (+3 standard deviations). Dynamic baseline thresholds are the most accurate way to define thresholds for a specific device.

Baselines are calculated once, after data has been collected for a week. You can recalculate baselines on demand.

Set general thresholds

Orion general thresholds are used for nodes and volumes in all Orion Platform products.


 Thresholds set on specific objects are not affected by changes made to general thresholds.

1. Click Settings > All Settings in the menu bar.
2. In the Thresholds and Polling grouping, click Orion Thresholds.
3. Enter values for Critical Level or Warning Level for selected thresholds.

PERCENT PACKET LOSS	
Critical Level	<input type="text" value="50"/>
Warning Level	<input type="text" value="30"/>

4. Click Submit.

Monitored thresholds are changed on a global level.

 To access thresholds for virtual objects, go to Settings, and click Virtualization Thresholds in the Thresholds & Polling grouping.

Customize thresholds for single objects


Get notified when polled values on critical devices reach different values than on other objects. For example, set warning and critical thresholds for CPU load on critical devices to a lower percentage than the default settings.

1. Click Settings > All Settings in the menu bar.
2. In the Node & Group Management grouping, click Manage Nodes.
3. Find the node or interface for which you want to set custom thresholds.
4. Select the object, and click Edit Properties.
5. Scroll down to Alerting Thresholds, select the Override Orion General Thresholds check box by the metric, and provide values for Warning and Critical thresholds.



If you want to use [dynamic thresholds](#), click Use Dynamic Baseline Thresholds. The integer values will be replaced with macros for dynamic thresholds (`${USE_BASELINE_WARNING}`, `${USE_BASELINE_CRITICAL}`).

When the polled values for the selected metric cross the thresholds on the object, the object will be highlighted, and appropriate alerts triggered.

 To customize thresholds for virtual objects, go to Settings, and click Manage Virtual Devices in the Node & Group Management grouping. Select a VMware object, click Edit Thresholds, and change the thresholds.

General threshold types

Avg CPU Load

Monitored network devices experiencing CPU loads higher than the value set for the Critical 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 Critical Level, display as red in High CPU Load reports and resources. Gauges for these devices also display as red.

You can choose to calculate exhaustion using average daily values or peak daily values.

Disk Usage

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

You can choose to calculate exhaustion using average daily values or peak daily values.

Percent Memory Used

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

You can choose to calculate exhaustion using average daily values or peak daily values.

Percent Packet Loss

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

Orion Platform products calculate percent packet loss using ICMP ping requests made on the [Default Poll Interval](#). The poller sends a ping to 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 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 Critical 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 Critical Level, also display in High Response Time reports and resources. Gauges for these devices also display as red.

Orion Platform products calculate response time using ICMP ping requests made on the Default Node Poll Interval. The poller sends a ping to 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 the poller does not receive a ping response within the [Default Poll Interval](#), it will attempt to ping the non-responsive device once every 10 seconds for the period designated as the Warning Interval.

Baselines and baseline calculations

With baselines, you can define what is normal for individual monitored objects based on polled data. By default, the baseline calculator uses the last seven days of collected statistic values to determine what is normal for individual monitored objects. The baseline is calculated using mean and standard deviation.


You can use baselines to detect deviations from the average polled values and be alerted on the deviations. Baselines can be displayed on some charts in the Orion Web Console.

What data is subject to statistical baseline calculation?

NODES	INTERFACES	VOLUMES
CPU Load	Received (Incoming) Errors & Discards	Percent Disk Usage
Percent Memory Used	Transmitted (Outgoing) Errors & Discards	
Response Time	Received (Incoming) Percent Utilization	
Percent Loss	Transmitted (Outgoing) Percent Utilization	

Use mean and standard deviations as thresholds

To get notified when polled values for a node or interface are outside the range specified by mean and standard deviations, set dynamic baseline thresholds.

 If you have a contextual understanding of the metric you are monitoring, consider defining the thresholds manually. Baselines are calculated values and do not know what is crucial for your environment.

1. Click Settings > Manage Nodes.
2. Locate and select the node or interface, and click Edit Properties.
3. Scroll down to Alerting Thresholds, select Override Orion General Thresholds, click Use Dynamic Baseline Thresholds.



Before you use calculated deviations as thresholds, click Latest Baseline Details to review the latest baseline statistics.

Mean and standard deviations will now be used as alerting thresholds for the node or interface.


Customize how the baseline is calculated

A baseline is a period when things are operating normally in your environment. Any anomalies that occur during the baseline period will be calculated into the results and skew the recommended values. If you are aware of an anomaly, re-baseline to ensure that the recommended values are accurate.


Consider customizing baselines if significant changes happen that influence what is normal in your environment, such as merging a new company, onboarding a large number of users, or making substantive improvements to the infrastructure.

By default, baseline calculations are based on data collected during seven days. Node baseline calculations are performed daily, and interface baseline calculations are performed weekly on Sunday.

1. Log in to the Orion Web Console using an account with administrative privileges.
2. Click Settings > All Settings in the menu bar.
3. In Thresholds & Polling, click Polling Settings.
4. Scroll down to Database Settings, and adjust the number of days in the Baseline Data Collection Duration field so that the time does not include a known deviation from the normal status.

 The Baseline Data Collection Duration cannot exceed the Detailed Statistics Retention configured in the same section.

5. To change the frequency of calculating interface baselines, choose the Interface Baseline Calculation Frequency.


 You can customize the calculation frequency only for interface baselines. The number of monitored interfaces is usually much larger than the number of nodes. Calculating baselines for nodes usually does not affect performance as much as performing the same calculations for all monitored interfaces.

6. Click Submit.

Your settings will now be used for calculating baselines.

Set SolarWinds NPM thresholds

SolarWinds NPM thresholds are relevant for nodes and interfaces. They include Cisco Buffer Misses, Interface Errors and Discards, Interface Percent Utilization, and Flapping Routes.

- 
- When a metric reaches the specified Critical Level threshold on a node or interface, the node or interface will be displayed as bold red in resources and reports.
 - When a metric reaches the specified Warning Level thresholds on a node, the node or interface will be highlighted in red in appropriate resources and reports.
 - Flapping Routes use different colors when the thresholds are exceeded: red for the error threshold and yellow for the warning threshold.

1. Log in to the Orion Web Console using an account with Administrator Rights.
2. Click Settings > All Settings in the menu bar.
3. In the Thresholds & Polling grouping, click NPM Thresholds.


4. Provide the values for Critical Level and Warning Level for the selected metrics.
5. For the Interface Percent Utilization metric, specify if you want to use average or peak daily values in calculations for capacity forecasting.
6. Click Submit.

Monitored thresholds are changed on a global level for NPM

See also [Define UnDP Warning and Critical thresholds](#).


Define UnDP Warning and Critical thresholds

If values polled by UnDPs on a device reach a certain level (critical or warning threshold), the UnDP on the device is highlighted in the Orion Web Console.

 To get notified about exceeding a threshold in an email, configure an alert. See [Alerting on printer toner running low based on a custom UnDP poller](#) for an example of using custom pollers in alerting.

To see pollers with exceeded thresholds in a map, see [View UnDP status on maps](#).

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. In the Thresholds & Polling grouping, click Custom Poller Thresholds.
4. Select a poller.
5. Select whether the expected polled value is a Text or a Number.

 The Poller Value Type determines how the polled value will be interpreted. It also influences the set of possible comparison functions.

- For the Number type, available values include `is greater than` or `less than`.
- For the Text type, available values include for example `contains`.

6. Build conditions to define both Warning and Critical Thresholds:
 - a. Select whether All Child Conditions Must Be Satisfied (AND) or if only At Least One Child Condition Must Be Satisfied (OR).
 - b. Select a comparison relation, and provide a threshold value on which the comparison is based.

- c. Click + to add additional conditions, as required, to define the poller threshold.

7. After configuring all thresholds, click Submit.

If a value reported by the device belongs to the range defined by the Warning Threshold, pollers in maps will be yellow.

If a value reported by the device belongs to the range defined by the Critical Threshold, pollers in maps will be red.

Manage Orion Web Console user accounts

Users need an Orion Web Console account to perform actions in your SolarWinds product, such as acknowledging alerts. Default account views and privileges are assigned in the account manager.

You may not need to grant all users accounts if they only need to review reports or access views. See [Share views with non-Orion Web Console users](#) for more information.

Add users individually, add group accounts, or use Active Directory accounts. If a user is in multiple group accounts, the permissions of the group highest on the Groups tab of the Account Manager are applied to the user. By default SolarWinds uses MSAPI to authenticate Active Directory users, but you can [authenticate users with LDAP](#).

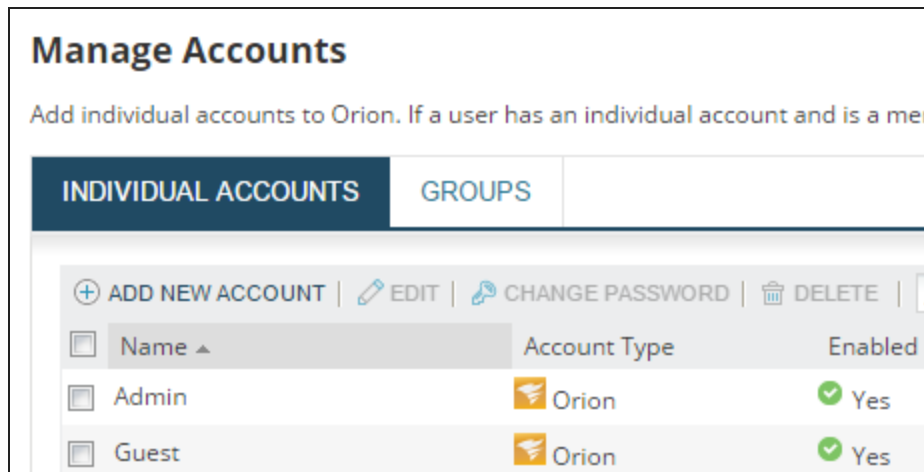
i To prevent issues with accounts, make sure that your SQL Server does not have the `no count` connection option enabled.

Create users

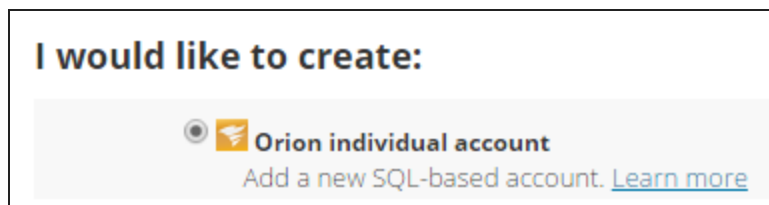
Before you begin, consider what tasks the user must perform, and what views and menu bars are most suitable.

Users created using default settings can log in to the Orion Web Console and see information available in views, resources, and reports. For administration and customization tasks, users need extra rights.

1. Log in to the Orion Web Console, and click Settings > All Settings.
2. Click Manage Accounts in the User Accounts grouping, and click Add New Account on the Individual Accounts tab.



3. Select Orion individual account, and click Next.



4. Provide the account credentials, and click Next.
5. On Define Settings, provide rights so that the user can perform assigned tasks, select default views and menu bars, and then click Submit.

The user account is listed in the Individual Accounts tab.

Create users based on existing Active Directory or local domain accounts

Users can use their existing Active Directory credentials to log in to the Orion Web Console, so you do not need to manage an extra user account.

- You must enable Windows Account Login in the Orion Web Console.
 1. Click Settings > All Settings, and in Product Specific Settings, click Web Console Settings.
 2. In Windows Account Login, select Enable automatic login, and click Submit.
- To maintain administrative privileges, individual and group Windows user accounts must be defined in the same domain as the SolarWinds server they can access.
- Only Security AD groups are supported. Distribution Groups are not supported.

1. Log in to Orion Web Console, and click Settings > All Settings.
2. Click Manage Accounts in the User Accounts grouping, and click Add New Account.

3. Select Windows individual account or Windows group account, and click Next.

Add New Account

SELECT TYPE > ENTER ACCOUNT INFO > DEFINE SETTINGS >

I would like to create:

- ☐ **Orion individual account**
Add a new SQL-based account. [Learn more](#)
- ☐ **Windows individual account**
Add existing Active Directory or local accounts to Orion. [Learn more](#)
- ☒ **Windows group account**
Add existing Active Directory or local group accounts to Orion. [Learn more](#)

4. Provide the credentials for an account with administrative access to the Active Directory or local domain, and click Next.
5. If a system account is available, you can use it. Select Use [Account Name] account to access Active Directory or Local Domain, and click Test Active Directory.

You may need to specify the credentials manually.

ACTIVE DIRECTORY OR LOCAL DOMAIN AUTHENTICATION

☒ Use "NETWORK SERVICE" account to access Active Directory or Local Domain [Help](#)

Machine "..." is not joined to an Active Directory Domain.

"NETWORK SERVICE" account successfully executed Local Domain search.

☐ Specify credentials to access Active Directory or Local Domain

User Name:

Password:

This user has administrative access to Active Directory or local domain accounts

Password for the user account granted administrative access to Active Directory or local domain accounts

6. To specify the credentials manually, select Specify credentials to access the Active Directory or Local Domain, and provide the credentials.
7. Search for the Active Directory or local domain account.

To search for all users or groups in the domain, enter `domain name*` and click Search.

SEARCH FOR ACCOUNT

Group name:

Use Domain\Groupname format

8. Select the appropriate users in the Add Users area, and click Next.
9. On Define Settings, provide rights so that the user can perform assigned tasks, select default views and menu bars, and then click Submit.

Users can now log in to the Orion Web Console using their local domain or Active Directory credentials.

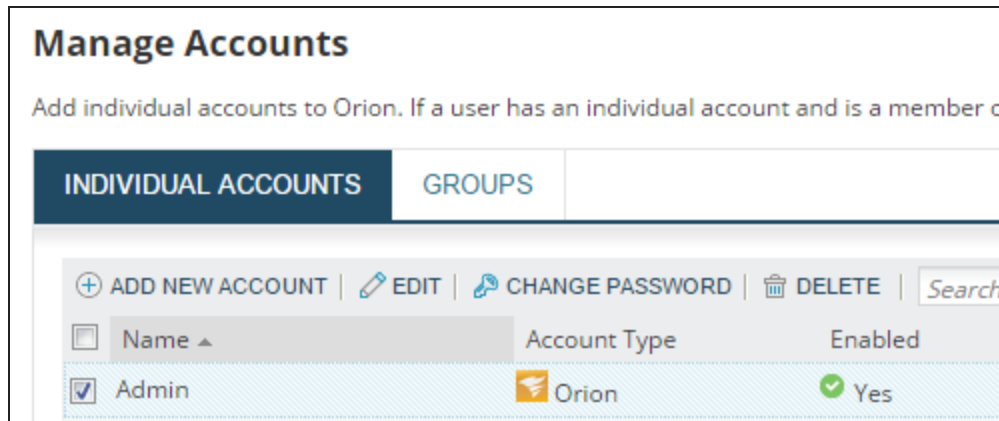
If you use Active Directory, users can also [automatically login](#) with their Windows credentials.

Change account passwords

When you log in to the Orion Web Console for the first time, SolarWinds recommends that you change the password for the Admin account.

Only users with administrator rights can change the password.


1. Log in to the Orion Web Console, and click Settings > All Settings.
2. Click Manage Accounts in the User Accounts grouping.
3. Select a user, and click Change Password.




4. Enter and confirm the new password, and click Change Password.

Enable users to authenticate through LDAP

You can choose to have all of your AD users authenticate through LDAP. The SolarWinds Orion server does not need to be added to the Windows domain with this authentication method.

 We do not support Anonymous authentication through LDAP.

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. Click Advanced AD Settings in the User Accounts grouping.
4. Toggle Authenticate Active Directory Users via LDAP.
5. Enter your LDAP server information and select the authentication method that matches what is used in LDAP.

 Click Discover DN to fill in the distinguished name (DN) of the AD domain automatically. If the DN field does not populate, verify that the Directory Server Address is correct.

Windows individual accounts now use LDAP. If you created Orion Web Console accounts that use Active Directory or local accounts and those accounts cannot authenticate through LDAP, those accounts cannot login.

If you disable this selection, Windows users or group members created while it was enabled cannot login.


Define what users can access and do

Each user or group account can have different privileges applied to it, such as the ability to modify alert definitions or delete nodes.


1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. Click Manage Accounts in the User Accounts grouping.
4. Select an account, and click Edit.
5. Specify the login options.

LOGIN OPTION	SETTING
Should the user be able to log in immediately?	Set Account Enabled to Yes. Disabling an account does not delete it. Account definitions and details are stored in the SolarWinds Orion database and can be enabled later.
Should the user be able to log in only temporarily?	Specify the expiration date.
Should the user be logged in indefinitely even if the browser is closed?	Select Yes for the Disable Session Timeout option. Session timeouts are global and set in Web Console Settings . By default, new user accounts are configured to timeout automatically.


6. Specify what tasks the user should be able to do.

TASK	ACCESS (SELECT YES FOR THIS OPTION OR DO AS INSTRUCTED)
Add and edit user accounts and reset passwords. <div>  SolarWinds recommends that you do not allow users to change their own Orion Web Console account passwords. </div>	Allow Administrator Rights Granting administrator rights does not assign the Admin menu bar to a user.
Add, edit, and delete nodes.	Allow Node Management Rights
Create, edit, and delete maps in the Network Atlas.	Allow Map Management Rights
Add, edit, schedule, and delete reports.	Allow Report Management Rights To only allow access to some reports, select the report category the user can access.
Add, edit, and delete alerts.	Allow Alert Management Rights To only allow some actions, keep No in Allow Alert Management rights and Allow items in the Alerts section as appropriate. To only access some alerts, select the category the user can access, or No Limitation.
Customize views.	Allow Account to Customize Views 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.
Enable/disable monitoring elements.	Allow Account to Unmanage Objects
Acknowledge and clear events, advanced alerts, and Syslogs.	Allow Account to Clear Events, Acknowledge Alerts and Syslogs.

7. If you want the user to use additional browser functions, such as right-click menu options, set Allow Browser Integration to Yes.

 Right-click menu options also depend on installing the SolarWinds Desktop Toolset and running the Toolset Integration Tray application on each client computer.

8. Provide the maximum Number of Items in the Breadcrumb List.

 To show all available items in breadcrumb drop-downs, set this option to 0.


9. Click Submit.

New account settings are applied when a user next logs in.

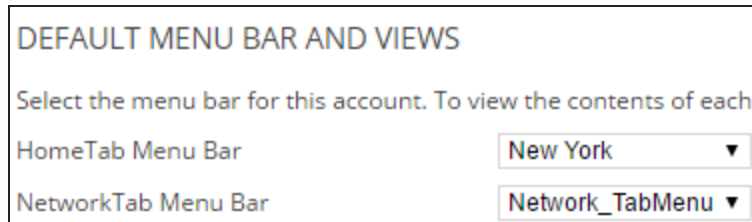
The user account also controls the [default menu bars and views](#), and [how much of your network they can access](#) through the Orion Web Console.

Set default menu bars and views for users

The items users see in My Dashboards and in Alerts & Activity are specified in their user accounts.

 Improve performance by setting the Home Page View to a view with a limited number of resources on it.

1. Click Settings > All Settings in the menu bar.
2. In the User Accounts grouping, click Manage Accounts.
3. Select a user, and click Edit.
4. Scroll down to Default Menu Bars and Views, and select top menu bars from the lists.



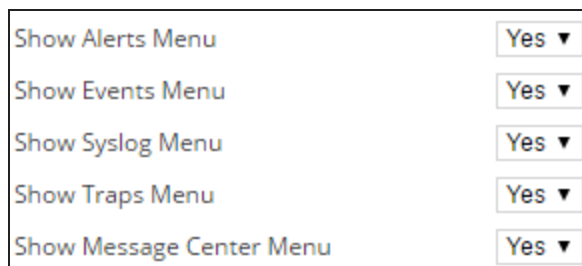
DEFAULT MENU BAR AND VIEWS

Select the menu bar for this account. To view the contents of each

HomeTab Menu Bar New York ▼

NetworkTab Menu Bar Network_TabMenu ▼

5. Select Yes for the items the user will see in the Alerts & Activity menu bar.



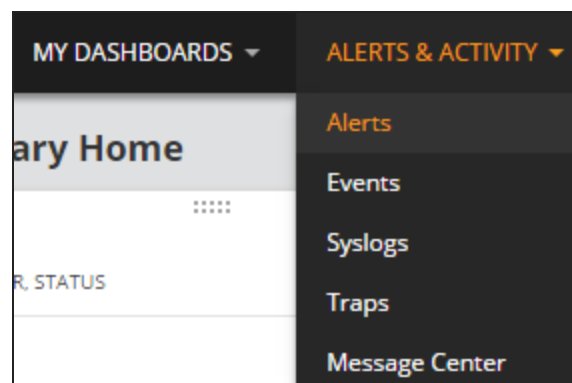
Show Alerts Menu Yes ▼

Show Events Menu Yes ▼

Show Syslog Menu Yes ▼

Show Traps Menu Yes ▼

Show Message Center Menu Yes ▼



6. Select an item and use the arrows to change the order of menu bars. Select an item from the list to specify the default Home page view.



Tabs ordering

Home
Network
Applications
Storage

Home Page View New York IT Summary

7. Click Submit.

The user can now use the specified links in My Dashboards and Alerts & Activity menu bars.

New account settings are applied when a user next logs in.

You can set default view for feature-specific views, such as hardware health or F5, or for product-specific view, such as VSAN or Application Details.

Limit users to specific network areas

Account limitations ensure that Orion Web Console users only view the network objects that are relevant to their job duties.

You can use account limitations in the following ways:

- 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

Predefined account limitations use built-in SolarWinds Orion properties to [limit user access](#). For greater flexibility, you can create your own account limitations in the [Account Limitation Builder](#), based on [custom properties](#).

Restrict user access to network areas by applying limitations

Account limitations restrict user access to specific network areas or withhold certain types of information from designated users.

To limit user access, apply a limitation on the user account, and specify the network area the user can access. Depending on the limitation, you can use [logical operators and wildcards](#).



Pattern limitations can have a negative impact on performance and are error prone.

If the default limitations are not enough, you can [create limitations based on custom properties](#), and apply them on user accounts.



- Group limitations are not applied until after the group availability is calculated.
- Because SolarWinds NetFlow Traffic Analyzer (NTA) initially caches account limitations, it may take up to a minute for account limitations to take effect in SolarWinds NTA.


1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. In the User Accounts grouping, click Manage Accounts.
4. Edit an individual or group account.
 - a. Click Add Limitation in the Account Limitations section.
 - b. Select the type of limitation to apply, and click Continue.
 - c. Define the limitation, and click Submit.

The limitation will be added to the Edit Account page.
5. Click Submit.

When the user logs back in, the account respects the limitations applied to it.

Patterns for limitations

When restricting user access to network areas, you can specify the limitation with patterns using OR, AND, EXCEPT, and NOT operators with _ and * as wildcards if the limitation allows pattern matching.


 Patterns are not case sensitive.

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.


Create limitations based on custom properties

You can define the part of a monitored network that users can access based on custom properties, and create custom limitations. Custom limitations are added to the list of available limitation types that you can apply on individual user accounts. After you create the limitation, you must edit accounts to use the limitation, and then select how the account is restricted.

-  ■ Before you start, plan how you want to limit the user access, and create [custom properties](#).
■ This procedure requires access to the computer that hosts the SolarWinds Orion server.

1. Click Start > All Programs > SolarWinds Orion > Grouping and Access Control > Account Limitation Builder.
2. Click Start on the splash screen.
3. Click Add Limitation.
4. Select a Custom Property. The fields are populated automatically based on your selection.
5. Choose a Selection Method.

 This is the selection format that will appear when you are choosing values for the [account limitation](#) in the Orion Web Console.

 [Pattern matching](#) is the most powerful selection, but it is also the selection most prone to errors when restricting access and impacts performance.

6. Click OK.

Your account limitation is added to the top of the table view. You may now [apply the limitation on user accounts to restrict user access to monitored objects](#) in the Orion Web Console.


Delete account limitations

Deleting a limitation makes it unavailable for future use in the Orion Web Console. If the limitation is applied to user accounts, the accounts will remain limited.

 This procedure requires access to the computer that hosts the SolarWinds Orion server.

1. Start the Account Limitation Builder in the SolarWinds Orion > Grouping and Access Control program folder.

2. Click Start on the splash screen.
3. Click the row of the limitation that you want to delete.

 Use <Shift+Click> to highlight multiple consecutive rows or <Ctrl+Click> to highlight multiple non-consecutive rows.

4. Click Edit > Delete Selected Limitations.


The limitation is now unavailable for limiting user accounts in the Orion Web Console.

Configure automatic login

You can log in automatically to the Orion Web Console using any of the following methods.

Use a Windows Active Directory Account

Create users based on active directory or local domain accounts, and enable automatic login for users logged in to the server. See [Create users based on existing Active Directory or local domain accounts](#).

 Windows authentication must be enabled in the Configuration Wizard and the Web Console Settings. See [Enable Windows Authentication with Active Directory](#).

Automatically log in with Windows Pass-through Security

Users can be authenticated through Windows Security, with no need to log in with separate credentials. For more information, see [Log in with Windows pass-through security](#).

Share content to non-SolarWinds users with the DirectLink account

If the DirectLink account is active, any URL referring directly to an Orion Web Console page will bypass the login page by logging the user into the DirectLink account. See [Share views with non-Orion Web Console users](#).

Pass-through user credentials in a URL

See [Automatically login by passing your credentials through the URL](#).


Users are authenticated in the following priority:

1. Windows Active Directory Authentication when enabled
2. The Account or User ID and Password passed on the URL
3. The Account or User ID and Password entered on the login.aspx page
4. The Windows User if Pass-through Security is enabled
5. The Windows Domain to which the User belongs, for example, Development\Everyone
6. A DirectLink Account

Enable Windows Authentication with Active Directory

The Orion Web Console can authenticate Active Directory users and users who are members of Active Directory security groups by using MSAPI or LDAP. By default, Windows individual or group accounts use MSAPI to authenticate accounts.

You can only use one authentication protocol at a time. All Windows accounts are authenticated through MSAPI or LDAP, depending on which one is enabled.

 SolarWinds offers a free analyzer tool for Active Directory that provides instantaneous visibility into effective permissions and access rights. The tool provides a complete hierarchical view of the effective permissions access rights for a specific file folder (NTSF) or share drive. Download it for free from here: http://www.solarwinds.com/products/freetools/permissions_analyzer_for_active_directory/.

Authenticate users through MSAPI


1. Enable the Orion Web Console to use automatic Windows Authentication.
 - a. Start the Configuration Wizard in the SolarWinds Orion > Configuration and Auto-Discovery program folder.
 - b. Select Website, and click Next.
 - c. Provide the appropriate IP Address, Port, and Website Root Directory, and select Yes - Enable Automatic Login Using Windows Authentication.
 - d. Click Next, and complete the Configuration Wizard.
2. Log in to the Orion Web Console using the appropriate domain and user, providing `Domain\Username` or `Username@Domain` as the User Name.
3. Run the Configuration Wizard and enable Windows authentication.
4. Login to the Orion Web Console, and navigate to Settings > All Settings. In Web Console Settings, select Enable automatic login in the Windows Account Login drop-down.

Supported Active Directory scenarios

The following Active Directory login scenarios are supported for SolarWinds products using the latest version of the Orion Platform.

SCENARIO	WEB CONSOLE LOGIN SUPPORTED?	LOCAL LOGIN REQUIRED?	NETWORK ATLAS AND UNMANAGE UTILITY LOGIN SUPPORTED?
Login with "Orion Server" domain AD account	Yes	No	Yes
Login with "Orion Server" domain Group AD account		LogonFallback must be enabled.	

SCENARIO	WEB CONSOLE LOGIN SUPPORTED?	LOCAL LOGIN REQUIRED?	NETWORK ATLAS AND UNMANAGE UTILITY LOGIN SUPPORTED?
Login with trusted domain AD user			No
Login with trusted domain AD Group User			
Login with "Orion Server" domain Group AD account (group user belongs to trusted domain) ¹			
Login with trusted domain Group AD account (group user belongs to "Orion Server" domain) ²	No	N/A	
Login with AD user or Group user from a foreign AD forest	Yes, when LDAP is enabled No, without an Additional Website ³		

-  1. Use a group account from the domain where the Orion Platform product server is located. This group contains a user from the trusted domain. Log in with this user.
2. Use a group account from the domain where the Orion Platform product server is located. This domain is trusted by the domain in which the Orion server is located. This group contains a user from the domain of the Orion server. Log in with this user.
3. Active Directory authentication is performed by the web service. If you need to authenticate users from an AD forest other the one to which your primary SolarWinds server belongs, you must have an Additional Web Server in the AD forest wherein the users to be authenticated exist.

Enable LogonFallback

LogonFallback must be enabled when the Active Directory user of the Orion Web Console does not have local login rights to the web server.


1. Locate the file `web.config` on the server hosting your Orion Web Console.
The default location is `c:\inetpub\SolarWinds\`.
2. Create a backup of `web.config`.
3. Locate row `<add key="LogonFallback" value="false" />`.
4. Set `value="true"`.
5. Save `web.config`.
6. Restart your SolarWinds website in Internet Information Services Manager.

Log in with Windows pass-through security

To authenticate users through Windows pass-through security, IIS NT Security must be enabled on your server.

Pass-through security can be configured to employ Domain security, Local computer security, or both Domain and Local computer security at the same time.

The Orion Platform account credentials must match the credentials used for the Domain or Local computer security.


-  ■ This procedure requires access to the computer that hosts the SolarWinds Orion server.
- When authenticating users with Windows Security, ensure your Orion server uses the NetBIOS domain name, instead of the fully qualified domain name.

1. If you are using NT Domain Authentication Format for pass-through accounts, [create these pass-through accounts](#) in the Orion Web Console Account Manager using Domain\UserID as the User Name. For example:
 - Washington\Edward
 - StLouis\Bill
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. For example:
 - SolarWindsS2\Edward
 - Server3\JonesR
3. Start the Internet Information Services Manager, enable Windows Authentication for the SolarWinds NetPerfMon website, and restart Internet Services.

Log in to the Orion Web Console using the Windows account credentials you have already established.

Share views with non-Orion Web Console users

Any URL referring directly to a Orion Web Console page bypasses the login screen, logging the user into the DirectLink account. If the DirectLink account does not exist, users are directed to the login page.

-  ■ The DirectLink account is created like any other account, and it can include custom views and account limitations.
- If you embed a view in another website, you may need to either disable cross-frame (X-Frame) protection in your IIS configuration, or add the website to the X-Frame-Options header in IIS. SolarWinds enables cross-frame protection by default to decrease security risks. Consult microsoft.com for more information.


1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. In the User Accounts grouping, click Manage Accounts.

4. Click Add New Account.
5. Type DirectLink as the User Name.
6. Type a Password, confirm it, and click Next.
7. Edit DirectLink account options. See [Define what users can access and do](#).
8. Click Submit.

Users can now look at views without an account on the Orion Web Console.

Automatically login by passing your credentials through the URL

Create a favorite or bookmark that includes your Orion individual account user name and password as parameters within the URL.

 HTTP requests are not encrypted, so account information sent in HTTP requests are not secure. For more information about enabling HTTPS on your Orion Platform product server, consult www.microsoft.com.

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 SolarWinds Orion server as the `DOMAIN`. Provide your Orion user name as the `USER`, and then provide your Orion user account password as the `PASSWORD`.

Administrative functions

View secure data

Sensitive network information, such as community strings, logins, and passwords, is not viewable in the Orion Web Console by default.

If you have secured your network, you can display secure data in the Orion Web Console.

1. Click Settings > All Settings in the menu bar.
2. In the Thresholds & Polling grouping, click Polling Settings.
3. Scroll down to the Calculations & Thresholds area, and select Allow Secure Data On Web (Advanced).


 This setting does not affect the display of [custom reports](#) that you export to the web.


Handle counter rollovers

Specify a method that decides what happens if a polled value is less than the previous polled value.

Orion Platform products are capable of handling either 32-bit or 64-bit counters.

By default, counters are assumed to be 32-bit.

 32-bit counters have a maximum value of 2^{32} , or 4,294,967,296.

 64-bit counters have a maximum value of 2^{64} , or 18,446,744,073,709,551,616.

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. In the Thresholds & Polling grouping, click Polling Settings.
4. Scroll down to the Calculations & Thresholds area, and select the Counter Rollover method.

- If you use 32-bit counters, select Method 1.

This method detects a rollover, and calculates based on it.


First, the method checks whether the device rebooted and reset its counters to 0. In this case, the last value is 0.

When it is a real rollover, we take the maximum value of the 32 or 64 bit number, take the difference between the maximum and the last polled value, and add it to the current polled value: $(MaxValue - LastPolledValue) + CurrentPolledValue$

- If you use 64-bit counters, select Method 2.

When a rollover is detected, Orion drops the poll and takes a new sample within 20 seconds. The new data point is stored, throwing the first data point away.

In memory, we have the value from the previous poll (A) and the LastPolledValue (B). Because $B < A$, we detect counter rollover. Orion drops the last poll and does a fast poll within 20 seconds. The value stored in the database is calculated as $C - B$.

 Orion fully supports the use of 64-bit counters, but these counters can exhibit erratic behavior in some implementations. If you notice peculiar results, disable the use of 64-bit counters for the problem device, and contact the device manufacturer.

Configure web proxy settings

If your SolarWinds Orion server does not have Internet access, you can use a proxy server to allow the Orion server to connect to certain pages and websites. Use a proxy server to:

- Access the [thwack community](#)
- Access the product blog
- Check for maintenance updates
- Access the ServiceNow® instance you integrated with your SolarWinds Orion server. For information about integrating SolarWinds Orion with ServiceNow, see [Integrate an Orion Platform product with ServiceNow](#).

To configure web proxy settings:

1. In the Orion Web Console, click Settings > All Settings > Product specific settings > Proxy Settings.
2. Select Use the following settings, and specify the IP address and port number of the proxy server.
3. If the proxy server requires authentication, select the check box, and specify the user name and password.
4. Enter a URL, and click Test connection to verify that you can reach the destination address through the proxy.
5. Click Save.

Orion Web Console and chart settings

The Web Console Settings page allows an Orion Web Console administrator to customize the Orion Web Console user environment.

1. Click Settings > All Settings in the menu bar.
2. In the Product Specific Settings grouping, click Web Console Settings.
3. When you finish configuring the settings, click Submit.

Web Console settings

Session Timeout

Provide the amount of time, in minutes, that Orion Web Console waits through user inactivity before the user is logged out.

Windows Account Login

Select whether you want to enable or disable automatic login with Windows Active Directory Credentials. With this feature enabled, the user can log in automatically.

Page Refresh

Specify the amount of time that passes before an Orion Web Console view reloads automatically

Site Logo

Select the box, and provide a path to a [banner graphic](#) that appears at the top of every Orion Web Console page.

NOC View Logo

Select the box, and provide a path to a banner graphic that appears at the top of every NOC view.

Site Login Text

Provide a text all Orion Web Console users will see before they log in. Enter up to 3500 characters. HTML tags are allowed.

Help Server

Provide the URL of the server where online help for Orion Platform products 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 online help for your products, including the Orion Platform offline help, copy it to a web server, and change the Help Server URL to that of the web server. You can download the online help from the documentation page for your product at https://support.solarwinds.com/Success_Center.

Status Rollup Mode

Specify how the availability status of nodes in node trees or on maps is displayed in the Orion Web Console.

- **Mixed Status** shows Warning ensures that 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.

Examples:

`Critical + Down = Critical,`
`Critical + Warning = Critical,`
`Up + Down = Mixed Availability.`

- **Show Worst Status** ensures the worst state in a node group is displayed for the whole group.

Examples:

`Up + Down = Down`
`Unreachable + Shutdown = Shutdown.`

Child Status Rollup Mode

Specify how the status of any single node on the node tree or on a map is displayed.

- Select **Show Worst Status** to ensure that the worst status of the node group is displayed for the whole group (e.g. red if any of the nodes are down).
- Select **Show Worst Status (Interfaces only)** to ensure that the worst status of any of the interfaces on a selected node is displayed. Only if you have SolarWinds NPM installed.
- Select **Show Worst Status (Applications only)** to ensure that the worst status of any of the applications on a selected node is displayed.
- Select **Show only ICMP Status** to only display up/down status for monitored interfaces.

Child Status Display Mode

Select whether you want to use a static or blinking icon to display the status of the children of any single node on the node tree or on a map. By default, a static icon displays the status of child objects.

Integration Tips

Specify whether you want to show or hide the list of products in the How SolarWinds Products Work Together section of the Settings page.

Drag and Drop Views

Turn on or off the ability to drag resources around on views.

Auditing settings

Select **Enable Audit Trails** to keep a record of all actions taken by Orion Web Console users. Depending on the number of technicians or the activity level of your installation, this may increase the storage needs of your database.

Chart settings

Chart Aspect Ratio

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

Thumbnail Aspect Ratio is the height/width ratio for chart thumbnails.

95th Percentile Calculations

[95th Percentile Calculations](#) adds annotation lines to charts at the entered percentile. This value is normally set to 95.

Maximum Number of Data Series Displayed on Chart

The Maximum Number of Data Series Displayed on Chart setting determines the maximum number of data series that will display on a chart at the same time. The default value for this setting is 10.

Show Data Points on Lines

The actual data points that are used to create a chart may be shown by checking Show Data Points on Lines.

Font Size

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, Worldwide Map, and Active Alerts settings

Notify About New Removable Volumes

Select the box if you want to be notified when removable volumes are added to your network and [discovered during network discovery](#).

You should configure the default send email action to receive notifications.

Automatic Geolocation

Select the box to [place nodes automatically](#) on worldwide maps.

Active Alerts Refresh

Specify how often the active alerts grid page is refreshed.

Active Alerts settings

Select how frequently you want the active alerts resource to refresh. Any alerts that trigger within the refresh interval appear when the grid refreshes.

Custom properties

Every object you monitor includes a list of default properties used to describe the devices, such as IP address, host name, or MAC address. You can also create custom properties and use them to create special alerts, reports, views, and groups.

Custom properties are user-defined fields, such as country, building, asset tag, or serial number, that you can associate with monitored network objects.

 Custom properties must use the Latin1 character set.

Custom property uses include:


- Add information to nodes, such as contact, owner, or support contract.
- Add a custom property that is used as an [account limitation](#) on nodes.
- Add a custom property to nodes for grouping on the web or in a report.
- Add a custom property and display it as an annotation on a chart.

A collection of the most commonly used properties is available out-of-the-box, but you can [create custom properties](#) to meet your precise requirements.

When a custom property is defined, you can [import values](#) for the property from a text- or comma-delimited file.


To apply a property to only a few objects, go to the [Edit](#) view in the Orion Web Console.

You may also create external records by [exporting custom properties](#) from selected objects as a spreadsheet.


 When you create, edit or remove a custom property, an event is logged. These events are audited, and you can display them in Audit Events resources.

Create a custom property


Custom properties help you add custom labels to monitored objects, group objects based on the property or alert on objects with a certain value for the property.

 Depending on the selected object type, some options are not available.


1. Click Settings > All Settings in the menu bar.
2. In the Node & Group Management grouping, click Manage Custom Properties.
3. Click Add Custom Property.
4. Select the object type for the property, and click Next.

 The available object types depend on the Orion Platform products installed. All installations allow you to create Node and Volume custom properties.


5. Define the custom property, and click Next.

 Frequently used custom properties are available as templates. Select a template, and adjust the settings if necessary. Templates ensure that naming conventions are met when necessary for certain workflows.

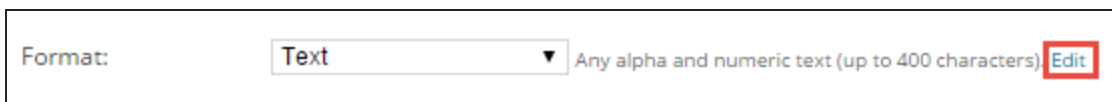
a. Edit the Property Name and Description fields.

 Property names are not case-sensitive, and must be unique for each object type. For example, you can have separate Comment properties for Nodes, Volumes, and other object types.

b. Select the Format for the property.


 We recommend that you limit the string length for text properties. The string length can affect SQL performance, especially when custom properties are used in limitations. The shorter the string length, the faster the queries.

To limit the string length, click Edit, and provide the maximum number of characters.



The screenshot shows a 'Format:' label followed by a dropdown menu currently set to 'Text'. To the right of the dropdown, there is a text description: 'Any alpha and numeric text (up to 400 characters)'. An 'Edit' button is highlighted with a red box.

c. Create a drop-down menu with specific values for the property by selecting Restrict values, and adding the values.


 Restricting values helps to maintain the consistency of values for individual custom properties.

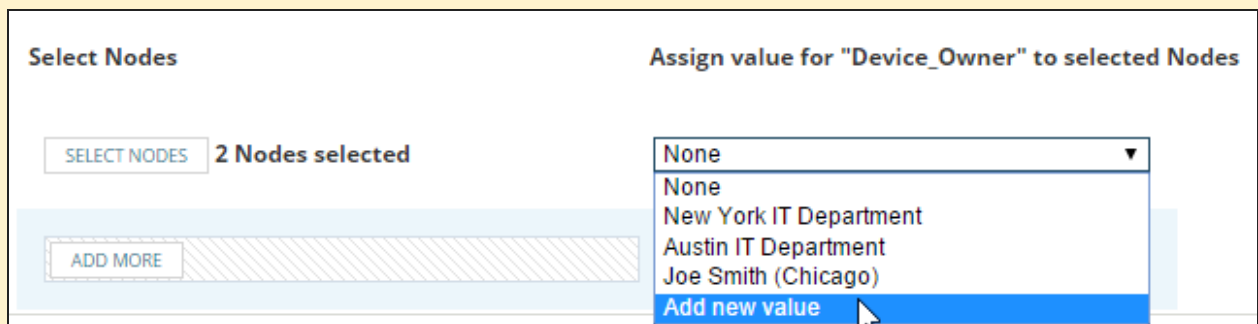
d. If you want to limit how the custom property for nodes should be used, clear boxes in the Usage section.

6. Select objects for which you want to define the custom property.

- Click Select <Objects>, and locate, and select the objects in the Available <Objects> pane.
- Click Add, and then click Select <Objects>.

7. Enter or select a default value for the property.

 To add a value for properties with restricted values, select Add New Value from the drop-down menu, and enter the new value.

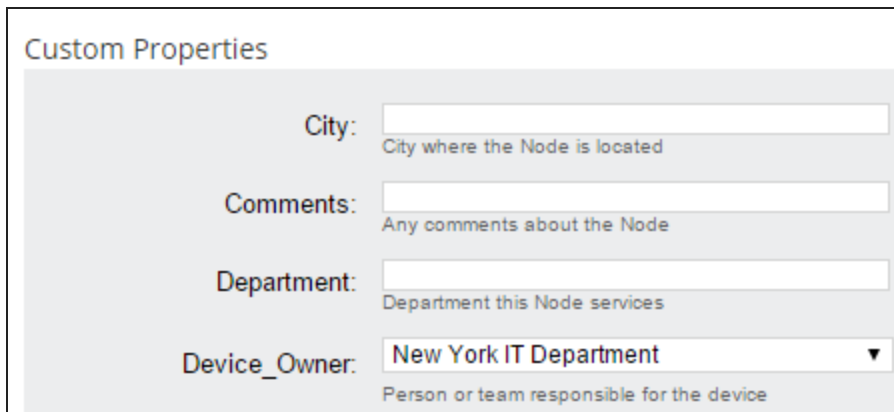


The screenshot shows two side-by-side panels. The left panel, titled 'Select Nodes', contains a 'SELECT NODES' button, the text '2 Nodes selected', and an 'ADD MORE' button. The right panel, titled 'Assign value for "Device_Owner" to selected Nodes', features a dropdown menu. The dropdown is open, showing a list of values: 'None', 'None', 'New York IT Department', 'Austin IT Department', 'Joe Smith (Chicago)', and 'Add new value'. The 'Add new value' option is highlighted in blue.

8. To apply the selected property to a different group of objects, click Add More, select the objects, and click Submit.

You have created a custom property and provided its value for the selected objects.

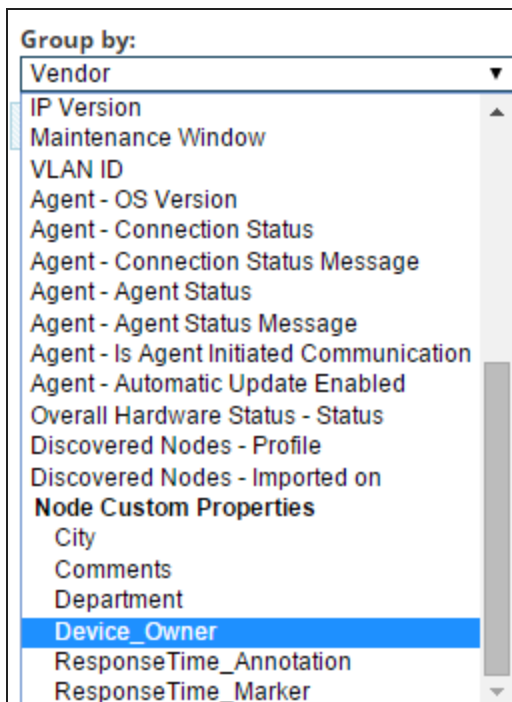
Now, you can [specify the property value](#) in the object properties. For example, for node properties, click Settings > Manage Nodes, select the object, and click [Edit Properties](#).



The screenshot shows a form titled "Custom Properties" with four fields:

- City:** A text input field with the placeholder text "City where the Node is located".
- Comments:** A text input field with the placeholder text "Any comments about the Node".
- Department:** A text input field with the placeholder text "Department this Node services".
- Device_Owner:** A dropdown menu with "New York IT Department" selected and the placeholder text "Person or team responsible for the device".

You can now use the custom property for sorting objects of the type in Group By lists.



The screenshot shows a "Group by:" dropdown menu. The list of options includes:

- Vendor
- IP Version
- Maintenance Window
- VLAN ID
- Agent - OS Version
- Agent - Connection Status
- Agent - Connection Status Message
- Agent - Agent Status
- Agent - Agent Status Message
- Agent - Is Agent Initiated Communication
- Agent - Automatic Update Enabled
- Overall Hardware Status - Status
- Discovered Nodes - Profile
- Discovered Nodes - Imported on
- Node Custom Properties**
- City
- Comments
- Department
- Device_Owner** (highlighted)
- ResponseTime_Annotation
- ResponseTime_Marker

Remove a custom property


! If the custom property is used in reports or alerts, remove it from the definition of all alerts and reports before you remove it from the Orion Web Console. Reports defined using removed custom properties do not work, and alerts stop triggering.

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. In the Node & Group Management grouping, click Manage Custom Properties.

4. Select properties you want to remove, and click Delete.
5. Confirm your action when prompted.

Import custom property values

If you have a spreadsheet listing custom property values, such as asset tags of all your network nodes, you can make this information available for reporting and publication in the Orion Web Console.

 Your data must be formatted as a table, and at least one column title should match an existing object property such as IP Address.

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. In the Node & Group Management grouping, click Manage Custom Properties.
4. Click Import Values.
5. Browse to the custom property data file, and click Open.
6. Select the object type you want in the Import Values For drop-down, and click Next.
7. For each detected Spreadsheet Column in your data, select the corresponding Orion Database Column, and select the Relationship between the columns.
 - Select Matches to indicate columns in the spreadsheet that correspond to existing columns in the SolarWinds Orion database, such as IP Address or MAC address.

SPREADSHEET COLUMN	RELATIONSHIP	ORION DATABASE COLUMN
Caption	matches ▼	Caption
IP_Address	matches ▼	IP_Address

- Select Imports To to import the data in the spreadsheet column to the selected SolarWinds Orion database column.

 This option overwrites any existing data in the corresponding custom properties.

- Select Imports To, and select <No Match Found, Ignore> for any spreadsheet column you do not want to import.

[» Create this custom property now](#)

- Click Create This Custom Property Now to open the Add Custom Property in a new browser tab if you need to create a custom property for this spreadsheet column.

8. Click Import.

When you view the values of the object type, the values of the custom property you selected are populated.

Export custom property data

If you want to keep records of custom properties for selected monitored nodes, you can export them as a spreadsheet. For example, you can create a single spreadsheet that lists the asset tags of all your network nodes.

 You can only select custom properties for a single object type.

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. In the Node & Group Management grouping, click Manage Custom Properties.
4. Select the custom properties you want to export, and click Export Values. You can [Filter objects](#) to find the custom properties more easily.
5. To export custom property data for specific objects, click Select <Objects>, and select the objects.
6. Select the database columns you want to export. You can also change which custom properties you want to export.
7. Select the file type for the exported data. This can be .csv, .txt, .html or xls.
8. Click Export.

The exported file is downloaded to your browser's default download location.

Change custom properties values

You can change the value of a custom property from the Manage Custom Properties page or bulk edit the values of a custom property assigned to objects.

 You can only edit properties of one object type at a time.

Edit values for custom properties

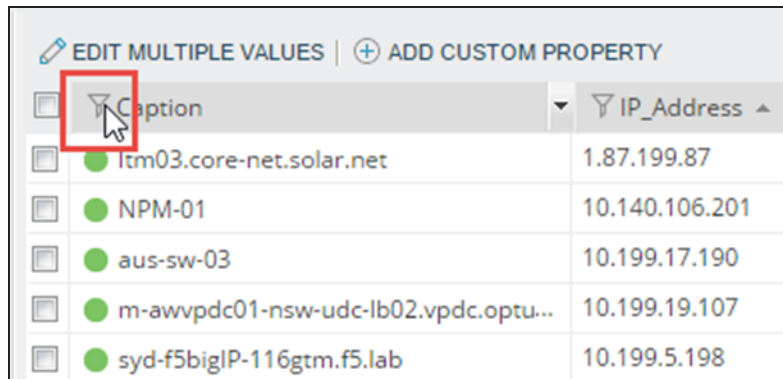
When you are entering a large amount of data, it can be easier to [import the values from a spreadsheet](#).

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. In the Node & Group Management grouping, click Manage Custom Properties.
4. Select the custom properties, and click View / Edit Values. You can [filter objects](#) to find the custom properties more easily.
5. To add or change a value for a property, enter the value into the field.
6. To add the same custom property value for multiple objects, select the objects, and click Edit Multiple Values. Select the property, enter the value, and click Save Changes.
7. When you have added or edited the values, click Save Changes.

Filter objects when assigning custom properties

You can limit objects displayed in the Custom Property Editor to find the objects you want to edit.

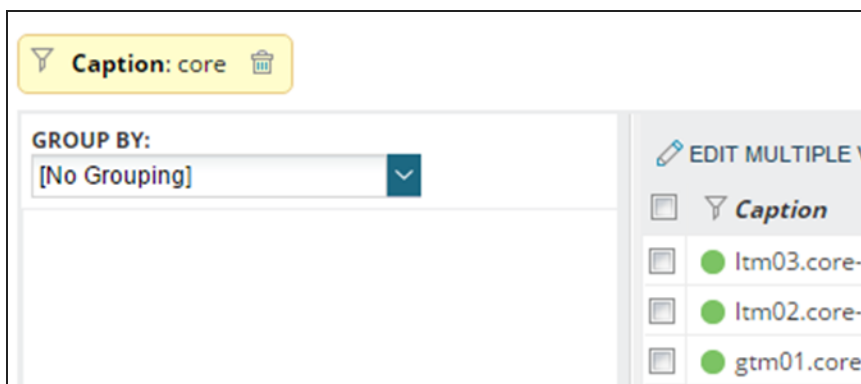
1. Click Settings > All Settings in the menu bar.
2. In the Node & Group Management grouping, click Manage Custom Properties.
3. Select the custom properties for which you want to assign values, and click View / Edit Values.
4. In the column captions, click the Filter icon, and enter filter text.



Caption	IP_Address
itm03.core-net.solar.net	1.87.199.87
NPM-01	10.140.106.201
aus-sw-03	10.199.17.190
m-awvpdc01-nsw-udc-lb02.vpdc.optu...	10.199.19.107
syd-f5bigIP-116gtm.f5.lab	10.199.5.198

The table will only display objects matching the filter options. The condition is added above the Group by section of the Custom Property Editor.

To remove the filter, click the trash icon next to the filter.




Caption: core
🗑️

GROUP BY:
 [No Grouping]

Caption
itm03.core-
itm02.core-
gtm01.core-

Manage the Orion Web Console

The Orion Web Console is an integral part of the Orion Platform products and can be accessed from virtually any computer connected to the Internet.

 To customize the Orion Web Console, you need administrator rights.

You can customize the Orion Web Console for multiple users, update polling settings and thresholds, and store individually customized views as user profiles.

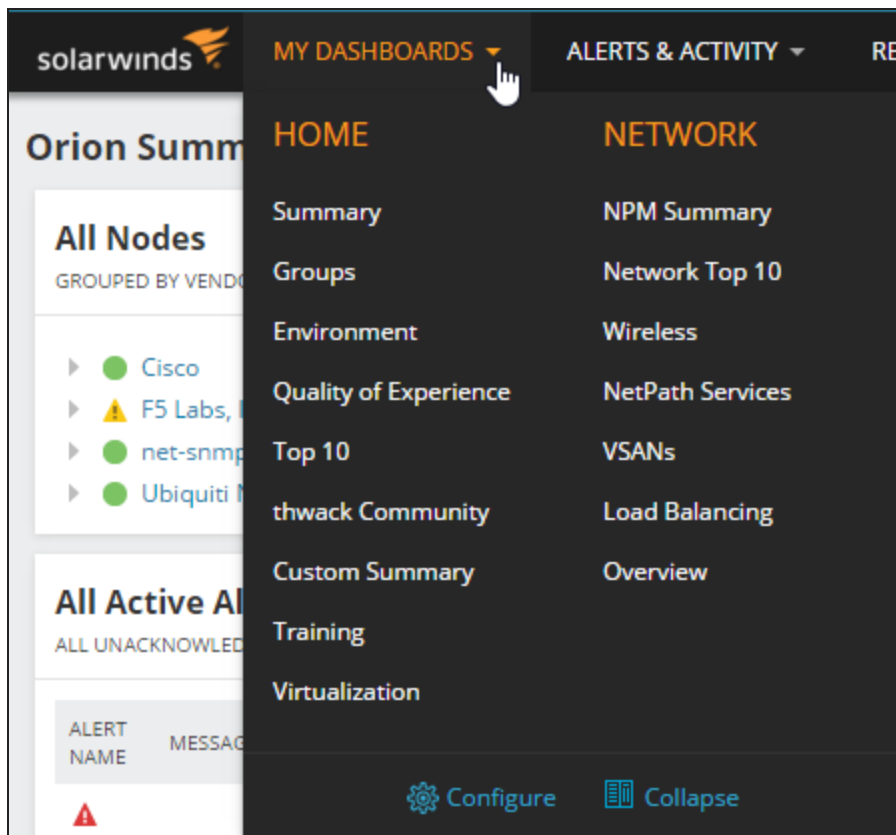
Customize the Orion Web Console look, views, settings, charts, and maps

 You need the Allow Administrator Rights privilege.

My Dashboards

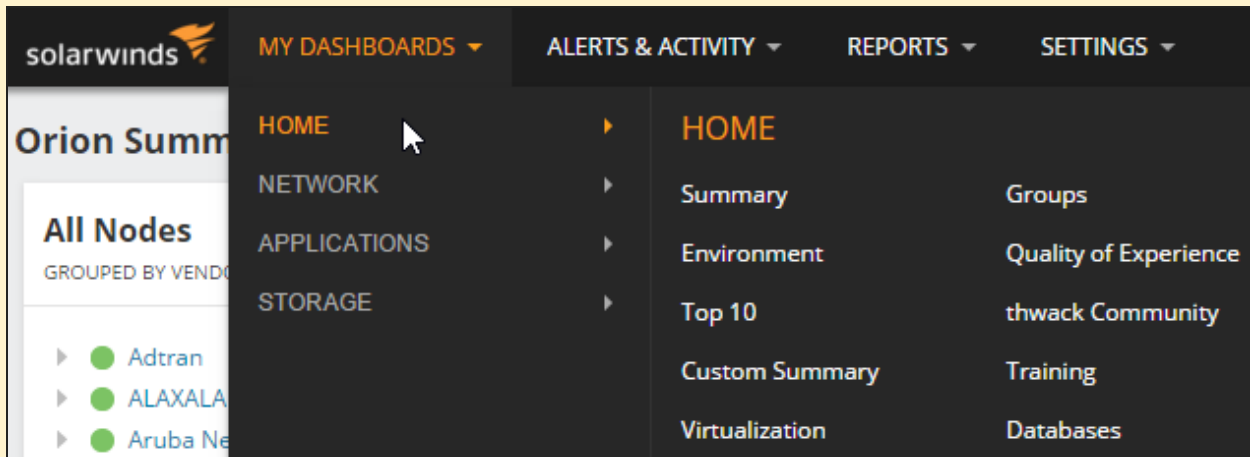
My Dashboards provide menu bars with shortcuts to Orion Web Console views. The default menu bars include Home, and a menu bar for each installed Orion Platform product.

Click My Dashboards to show the default menus.



You can customize views and labels offered in default menus for individual users.

- 💡 If you do not need to see all items in menu bars, and prefer navigating to display items in a menu bar, click My Dashboards > Collapse.



Customize My Dashboards

Menu bars available in My Dashboards depend on both the settings in your user account and the products you have installed.

1. [Find out](#) which menu bar is assigned to Home, Network, or other product-specific tab for your user.
2. [Add an Orion Web Console view or an external web page to the menu bar](#). The change will concern all users who access the menu bar from My Dashboards.

💡 To add a link to a details view for an important device, go to the view, copy the URL, and add it as an extra item to the view.

3. To provide access to a specific set of links for specific users, create a menu bar, add the links and assign the menu bar as the Home tab for the users.

Specify My Dashboards and Alerts & Activity items for users

The items users see in My Dashboards and in Alerts & Activity are specified in their user accounts.

- 💡 Improve performance by setting the Home Page View to a view with a limited number of resources on it.

1. Click Settings > All Settings in the menu bar.
2. In the User Accounts grouping, click Manage Accounts.
3. Select a user, and click Edit.
4. Scroll down to Default Menu Bars and Views, and select top menu bars from the lists.

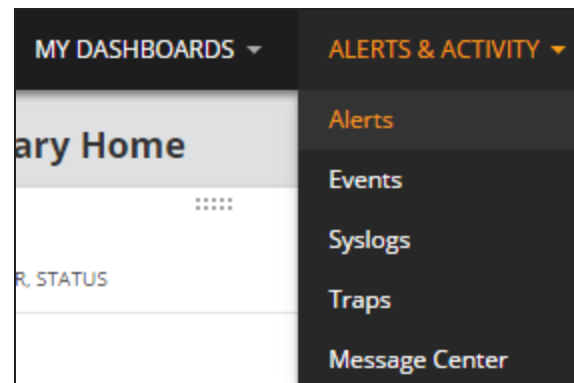
DEFAULT MENU BAR AND VIEWS

Select the menu bar for this account. To view the contents of each

HomeTab Menu Bar	New York ▼
NetworkTab Menu Bar	Network_TabMenu ▼

5. Select Yes for the items the user will see in the Alerts & Activity menu bar.

Show Alerts Menu	Yes ▾
Show Events Menu	Yes ▾
Show Syslog Menu	Yes ▾
Show Traps Menu	Yes ▾
Show Message Center Menu	Yes ▾



6. Select an item and use the arrows to change the order of menu bars. Select an item from the list to specify the default Home page view.

Tabs ordering	Home Network Applications Storage	⬆ ⬆ ⬆ ⬆
Home Page View	New York IT Summary	

7. Click Submit.

The user can now use the specified links in My Dashboards and Alerts & Activity menu bars.

Add items to My Dashboards


What users see in My Dashboards depends on menu bars assigned to them in their user account. To add an item to My Dashboards for all users who can see a menu bar, add the item to the menu bar.

1. Click My Dashboards > Configure.
2. Click Edit.


Menu Bar: New York				
✎ Edit 🗑 Delete				
NEW YORK IT SUMMARY	ENVIRONMENT	QUALITY OF EXPERIENCE	VIRTUALIZATION	TOP 10

3. Drag available items from the left-hand column to Selected Items on the right.

Available items	Selected items
% Loss & Traffic	New York IT Summary EDIT
Accounts	Quality of Experience
Active Directory EDIT 	All Interfaces
Admin	Environment
All Maps EDIT 	Virtualization
All Nodes	Top 10 EDIT
All Volumes	
Capacity Dashboard	
	SUBMIT CANCEL

 Hover over any view title to read the description.
To change the order of menu items, drag and drop items in the Selected column.

4. Click Submit to save your changes.

-  You can also add links to node details views for specific nodes, or to external Internet pages as a menu item.
- a. Click Add below the Available items list, provide a name, URL and description for the menu item, and click add.
 - b. Drag the new item to the Selected items column.

Users who can see the menu bar in My Dashboards will see the added items.

Add menu bars

When you have a list of items you want users to access from My Dashboards, create a menu bar.

1. Click My Dashboards > Configure.
2. Scroll to the bottom of the page, and click New Menu Bar.
3. Name the menu bar.

4. Drag views from the Available items column into Selected items.

Add Menu Bar

Name for New Menu Bar

Drag items from the Available Items column to the Selected Items column. Rearrange items by dragging them. Select the 'Submit' button to save.

Available items	Selected items
% Loss & Traffic	New York IT Summary <input type="button" value="EDIT"/> <input type="button" value="trash"/>
Accounts	
Active Directory <input type="button" value="EDIT"/> <input type="button" value="trash"/>	

5. Click Submit.

The new menu bar is created. You can now assign it to users who will see the items in My Dashboards.

Change the Orion Web Console color scheme

1. Click Settings > All Settings in the menu bar.
2. In the Customize Navigation & Look grouping, click Color Scheme.
3. Select a color scheme, and click Submit.

Change the Orion Web Console logo

1. Create a graphic to replace the SolarWinds logo.

The recommended logo size is 250 x 50 pixels. The maximum allowed size is 900 x 500 pixels.

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

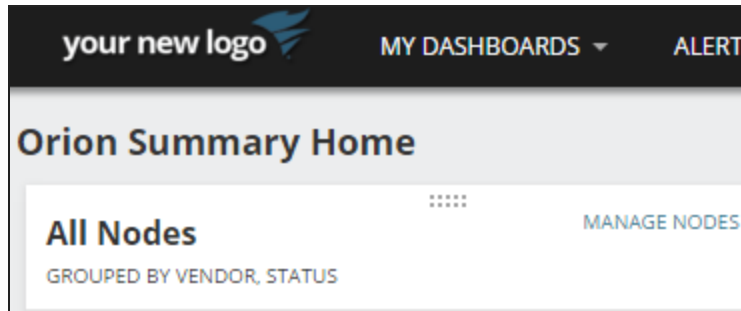
The default location of the directory is `C:\Inetpub\SolarWinds\NetPerfMon\`.

3. Click Settings > All Settings in the menu bar.
4. In the Product Specific Settings grouping, click Web Console Settings.
5. Ensure the Site Logo box is selected, and click Browse to navigate to your logo.

☒ SITE LOGO



☐ Upload logo from external path

6. Click Submit.



Use Orion Web Console breadcrumbs


As you navigate Orion Web Console views, you can use breadcrumbs to pick other views that are on the same or higher navigational level as your current view.

-  You cannot view breadcrumbs in wizards, dashboards, or full-page resources such as All Active Alerts.
-  Only the first 50 monitored nodes, listed in alphanumeric order by IP address, are displayed.

1. Click a breadcrumb to open the view.
2. Click > next to a breadcrumb to open a clickable list of all views at the same navigation level. For example, if you are on a Node Details view, clicking > displays a list of other monitored nodes.

Customize breadcrumbs


1. Click > at an appropriate level in the breadcrumbs to open the drop-down.
2. Click Customize This List.
3. Select an option from the menu, and click Submit.

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

Create, delete, modify, or restrict 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 be assigned to menu bars. With NOC View Mode enabled, views may be optimized for display in Network Operations Centers.

 To make views and graphs larger for larger screens, resize the columns dynamically (drag the division bars) and use your browser zoom controls, such as <Ctrl>+<+> in Chrome.

Create new views

You can customize the Orion Web Console for individual users by creating views.

-  You need Administrator Rights for creating views.

Plan what should be on a view before you create it.

OPTION	ACTION
Identify objects to see on the view.	Select the appropriate object type, such as nodes, interfaces, groups, applications, and so on.
View information for all objects of the selected object type.	Select a Summary view.
View details for a selected object.	Select a Details view.
Select information about the objects you want to see.	Select resources.
Divide the information into several tabs.	Enable Left Navigation.
Optimize the view for large screens or mobile devices.	Create a Network Operations Center (NOC) view.
Limit what devices should be displayed on the view.	Add a limitation.
Access the view from the Menu Bar.	Add the view into the menu bar.

Create views



[Check out this video on creating a new view.](#)

1. Log in to the Orion Web Console, and click Settings > All Settings.
2. Click Add New View in the Views grouping.
3. Name the view, and select the view type.

Add New View


Name of New View

Type of View

SUBMIT

4. Click Submit.

You have now created an empty view. The Customize view page opens automatically. Add resources that contain the information you want to see.

 The Type of View affects how the view is made accessible to users, and your choice may not be changed later. For more information, see [Specify views for device types](#).

After you have created a new view, the [Customize page](#) opens.

Add resources and columns to views, and define subviews

Administrators can edit views on the Customize page for the view. Click Customize Page on the view, or access the page through Manage Views.

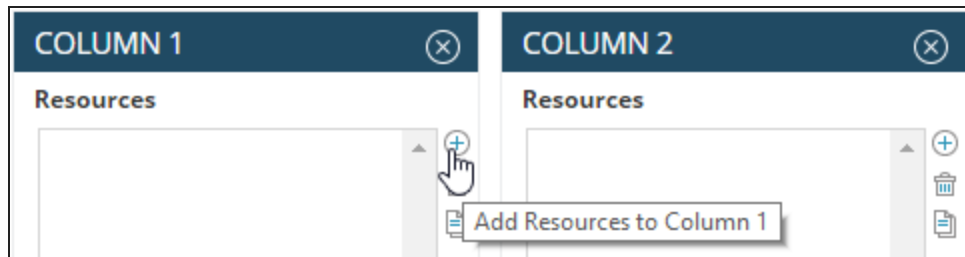
1. Click Settings > All Settings in the menu bar.
2. In the Views grouping, click Manage Views.
3. Select the view, and click Edit.

Add resources to the view



[Check out this video on adding and customizing resources.](#)

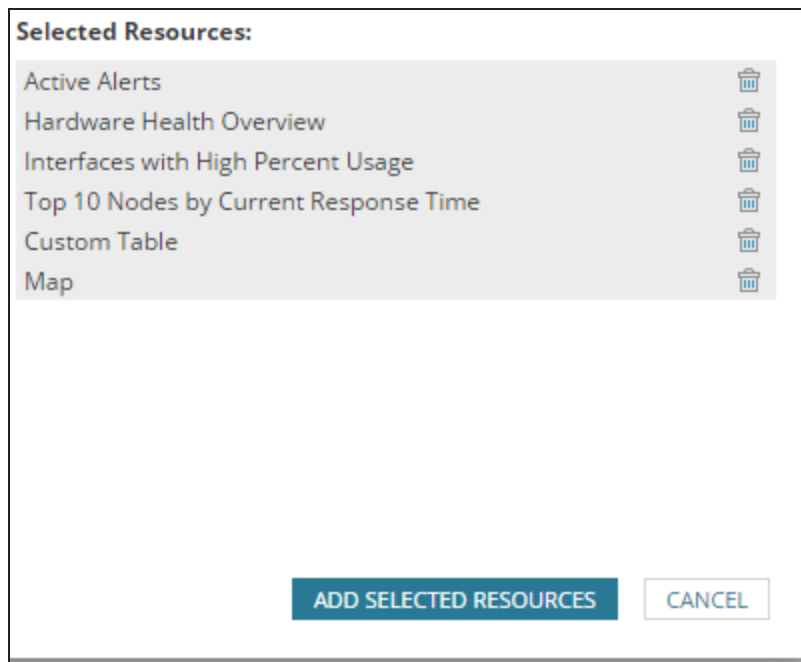
1. On the Customize page, click + next to the column that you want to add the resources.



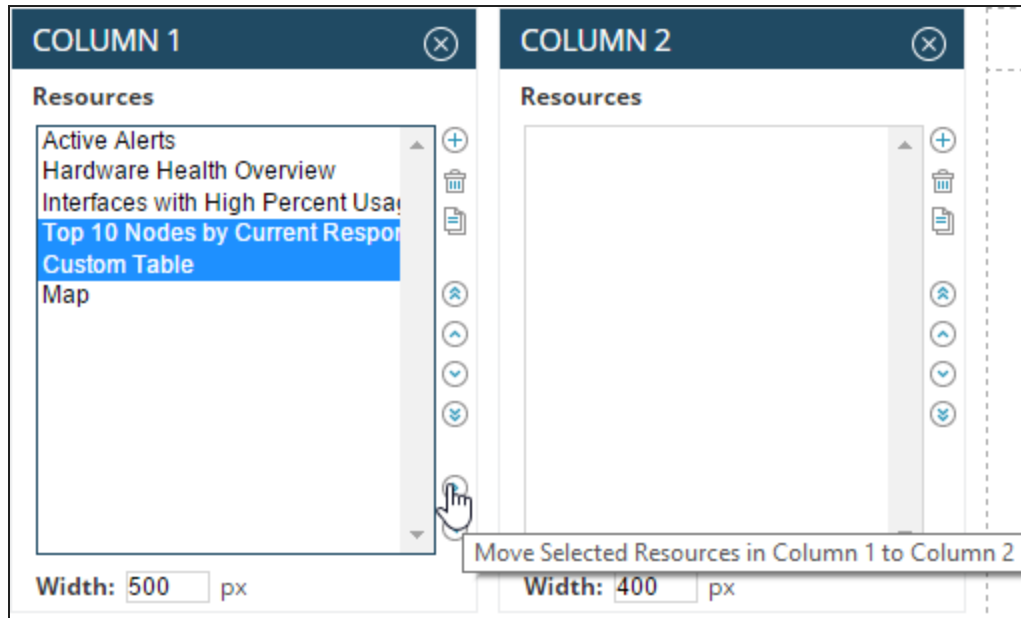
i To open the Customize view page, click Settings > All Settings > Manage Views. Select the view, and click Edit.

2. Select resources in the middle pane, and click Add Selected Resources.

i You can limit offered resources by criteria in the Group by list, or search for a resource in the Search box.



3. Use the arrow icons next to the columns to move resources between columns.



4. Click Done.

The view should now be populated with the resources you selected.

- Resources already in your view are not marked in the list. You can add a resource on a view more than once.
- Some resources may require additional configuration.
- 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.

Add columns

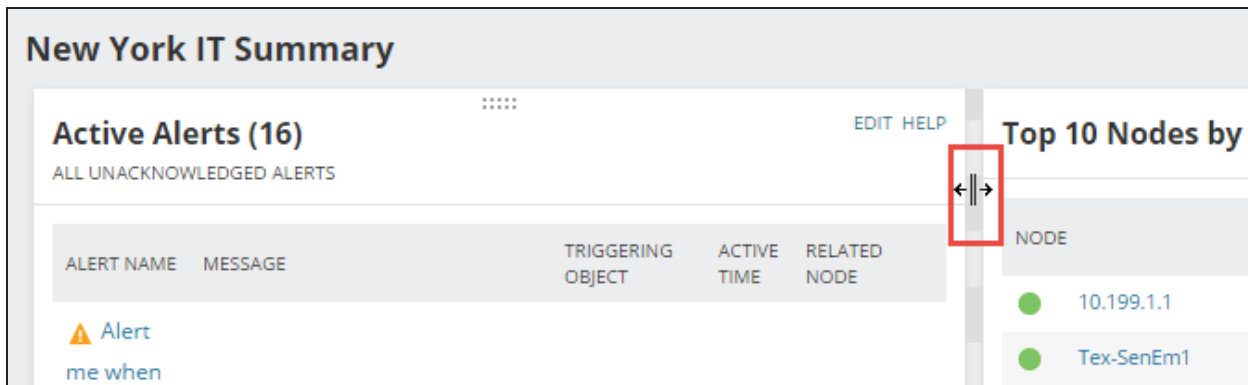
Resources on views are divided into columns.

On the Customize Page, click Add New Column.

- You do not have to add resources here. You can click Done, and drag resources between the columns on the view.

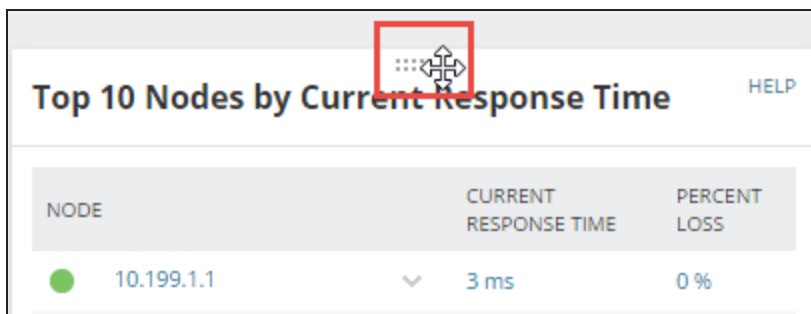
Change column width

To change a column width, position the cursor between the columns and drag the column border to achieve the appropriate width.



Move resources on views

To move resources within a column or between columns on a subview, drag the handle at the top of the resource to the new location.

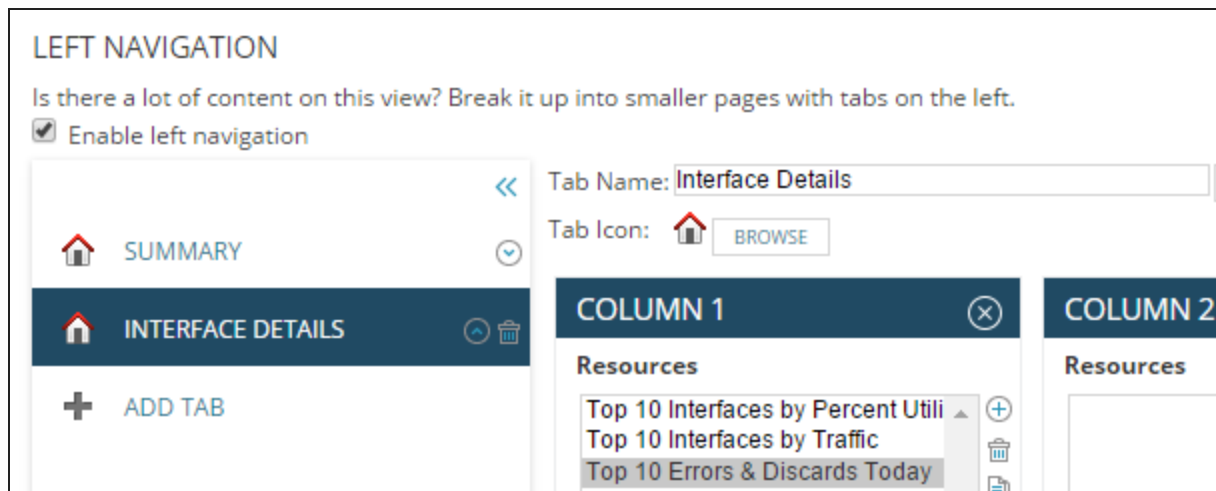


Divide content into subviews

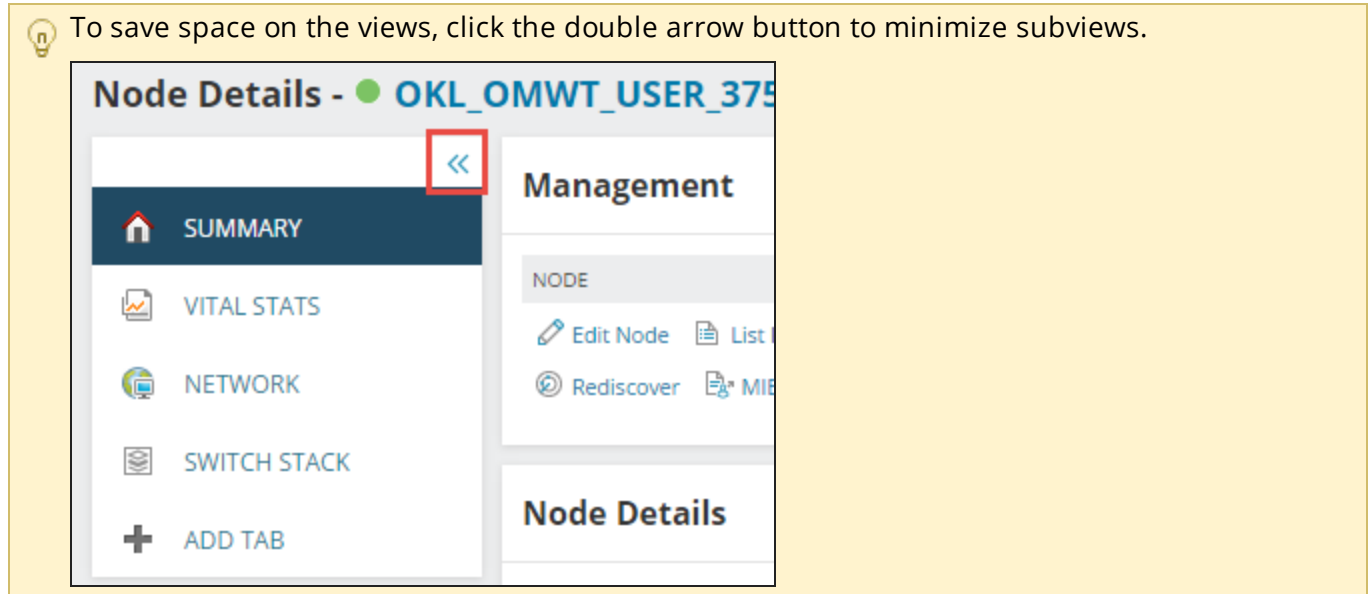
If there is too much information on the view, group and divide resources into subviews.

1. On the Customize view, select Enable Left Navigation.

i To open the Customize view page, click Settings > All Settings > Manage Views. Select the view, and click Edit.



2. Click Add Tab.
3. Type a name for the new tab, and click Update.
4. Select an icon, and add resources.
5. Click Done.



When you are done with your changes, click Preview, and then click Submit.

Create custom summary views

The Custom Summary view enables you to create a fully customized object-based view.

i You need the Allow Account to Customize Views right enabled.

1. Click My Dashboards > Home > Custom Summary.
2. Click Edit in any Custom Object Resource.
3. Provide a Title and Subtitle for the resource.

4. Select an object type from the Choose Object Type drop-down.

Title:

Subtitle:

Choose Object Type:

Select object:

5. Click Select Object.
6. On the Select Objects window, use the Group by selection field to filter the list of monitored objects.
7. Select one or more objects on which to base the selected resource, click the green arrow to move objects into the Selected Objects pane and click Submit to add the objects.
8. Specify what information about the selected object(s) you want to see in the resource, and click Submit.

Select a Chart:

Select object: ☐ Automatically display nodes related to the current view.
If resource is added to a Node Details Page, show objects on that node.

Limit Series: ☐ Number of top series displayed:

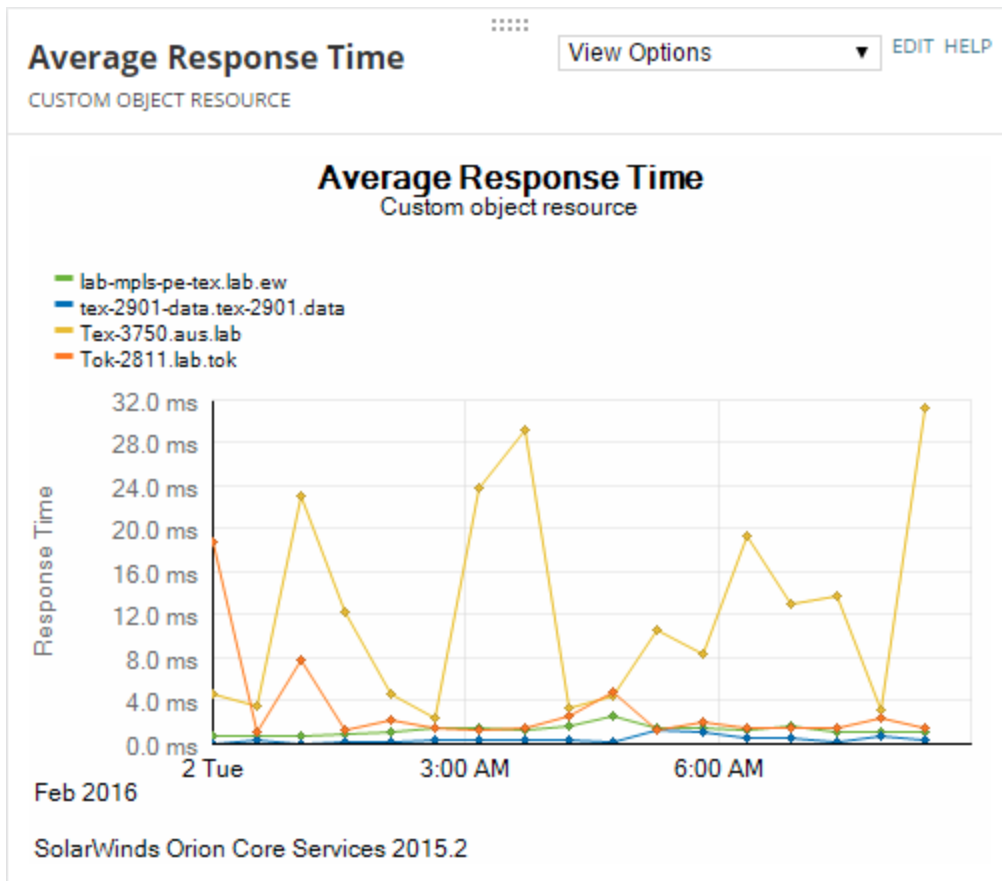
Show Sum in Data Series:

Time Period:

Sample Interval:

Auto-Hide Resource: ☐ Yes ☒ No

The fields displayed and information required depend upon the object type selected.



Add external website views

You can select any external website and add it to the Orion Web Console as a view.

You need Administrator Rights.

1. Log in to the Orion Web Console and click Settings > All Settings in the menu bar.
2. In the Customize Navigation & Look grouping, click External Websites.
3. Click Add.
4. Provide a Menu Title. This will be used for the website in the My Dashboards menu bar.
5. If you want to include a heading for the view, provide an optional Page Title.
6. Provide the URL of the external website, in the following format:

```
http://domain_name
```

7. Select the Menu Bar to which you want to add the website link.

See [My Dashboards](#).

If you select Admin as the menu bar, the website will be available from My Dashboards > Home for administrators.

8. Click OK.
9. Click Preview to see the external website in the Orion Web Console.

Optimize views for TV screens or mobile devices


A Network Operations Center (NOC) view provides a single page view of critical statistics that can fit on a TV screen or a mobile device. If you define multiple subviews, they rotate automatically on the screen, each subview available as a separate slide.

Headers and footers are compressed in NOC views, increasing the available space to display resources.

Enable NOC Views

You can configure any Orion Web Console view to appear in the NOC view form.

1. Log in to the Orion Web Console as an administrator.
2. Open a view, and click Customize Page in the top right corner of the view.
3. Select Enable NOC view mode.
4. If the view contains several subviews, select the rotation interval for the subview.

 To get a direct link to a NOC view, use the Link to NOC View link.

5. Click Done & Go to NOC View.

You have created a NOC version of your view with a compressed header and footer, and without the left navigation area.

Customize NOC Views

To add resources, remove resources, or add subviews on a NOC view, click the top-right icon, and select Customize Page.

Exit NOC Views


Click the NOC Settings icon, and select Exit NOC Mode.

You will return to the default view with the full header, footer and left navigation.

Manage NOC Views

You can display a list of all NOC views defined in your Orion to get a better understanding of your NOC views. From the NOC views list, you can easily add, edit or manage your NOC views.

1. Click Settings > All Settings.
2. In the Views grouping, click Created NOC views.

 You can view NOC views from any view. Click Customize Page, and click List of created NOC views in the NOC view section.

3. Manage the NOC views:
 - To add a new view, click Add New View.
 - To edit a NOC view, select the view, and click Edit.
 - To disable a NOC view and maintain the default view, select the view and click Disable NOC.

Display subviews

If more subviews are defined for the view, you can see white circles in the top right corner. The currently

active tab is displayed in orange.

To display a subview, click the circle.

Move resources in NOC Views

If you want to move resources within a NOC view, you turn on the drag&drop mode.

1. Click the Settings icon in the top right corner of the NOC view, and select Enable Drag&Drop / Pause.
2. Drag and drop resources within the selected pane.
3. When you have finished repositioning the resources, click the Settings icon again, and select Disable Drag&Drop / Resume.

Change the NOC view logo

You can hide the default SolarWinds logo on the NOC view, or use a customized image in the top left corner of your NOC views.

Logo requirements:

- Supported image formats: .png, .jpg
- Maximum resolution: 900x200 px

To use a customized logo on your NOC views:

1. If you already are in a NOC view, click the NOC Settings icon and select Customize NOC View Logo.
2. To hide the logo, clear the NOC View Logo option.
3. To change the logo:
 - a. Make sure that NOC View Logo is selected.
 - b. Click the Browse button for NOC View Logo and navigate to the appropriate logo image.

By default, the SolarWinds logo is used on NOC views. It is available as `SW_NOClogo.png` in `/NetPerfMon/images` on your Orion server.
4. Click Submit to apply your changes in the view.


Limit objects on a view

As a security feature, administrators can limit which devices are displayed on a view.

1. Click Settings > All Settings in the menu bar, and click Manage Views in the Views grouping.
2. Select a view, and click Edit.

 You can also open the Customize View page from the view, by clicking Customize Page.

3. On the Customize View page, click Edit in the View Limitation area.
4. Select the type of view limitation you want to apply, and click Continue.
5. Provide or select strings or options to define the device types that you want to include or exclude from the selected view, and click Submit.

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

Use a view as a template

When you want to create multiple views based on the same device type, create one view, and use it as a template to create other new views.

1. Click Settings > All Settings in the menu bar.
2. In the Views group, click Manage Views.
3. Select the view you want to copy, and click Copy.
4. [Edit](#) the copied view.

Delete views

1. Click Settings > All Settings in the menu bar.
2. In the Views group, click Manage Views.
3. Select the view you want to delete, and click Delete.

Specify views for device types


In the Orion Web Console, you can specify views displayed for each type of device you have on your network, such as routers, firewalls, or servers.

1. Click Settings > All Settings in the menu bar.
2. In the Views grouping, click Views by Device Type.
3. Select a Web View for the individual types of devices currently monitored on your network.
4. Click Submit.

When you click a device now, the view specified for the device type will be displayed.

Export views to PDF

Many views in the Orion Web Console can be exported to portable document format (PDF).

 The Export to PDF feature requires IIS Anonymous Access. Confirm that the IUSR_SERVERNAME user is in the local Users group on your Orion server.

1. Open a view, and click Export to PDF in the top right corner of the view.
2. If you are prompted to save the PDF file, click Save.
3. Navigate to a location, provide a file name, and click Save.

Customize resources in the Orion Web Console

Click Edit in the resource to view customization options. Available options depend on the resource type, and include for example the following items:

- Title and subtitle
- Time relevant for displayed data
- Maximum number of items shown in the resource

Submitting your changes gets you back to the view, where you can review the changes in the resource.


Resource configuration examples

Several resources that may be selected from the Add Resources page require additional configuration.

Display a Network Atlas map in the Orion Web Console

Network maps created with Network Atlas can give a quick overview of your network. Add a Network Atlas map on a view.

1. Open a view where you want to add the map, and click Customize Page.
2. Click the plus sign in the column to open the Add Resource dialog.
3. Enter `map` in the Search box, and click Search.
4. Select Map, and click Add Selected Resources.
5. Click Preview to preview the map, and click Edit to customize the resource.
6. Select a map.
7. Specify the Zoom percentage at which you want to display the map.

 If you leave the Zoom field blank, the map displays at full scale, based on the size of the column in which the map displays.

8. Click Submit.

The map is added to the view.

Display a list of objects on a network map

1. Open the view where you want to add the list of objects on a map, and click Customize Page.
2. Click the plus sign in the column to open the Add Resource dialog.
3. Enter `map` in the Search box, and click Search.
4. Select List of Objects on Network Map, and click Add Selected Resources.
5. Click Preview to preview the map, and click Edit to customize the resource.
6. Select a network map from the list of maps, and click Submit.

The view will now include a resource listing objects on the selected map.

Display a custom list of available maps

Clicking a map in the list opens the map in a new window.

1. Open the view where you want to add the list of maps, and click Customize Page.
2. Click the plus sign in the column to open the Add Resource dialog.
3. Enter `map` in the Search box, and click Search.
4. Select Custom List of All Maps, and click Add Selected Resources.
5. Click Preview to preview the resource, and click Edit to customize the resource.
6. Select maps you want to include in your maps list.
7. Click Submit.


Display the Worldwide Map

The worldwide map provides a quick geographical overview of your network at any level from global down to street.

1. Open the view where you want to add the Worldwide Map, and click Customize Page.
2. Click the plus sign in the column to open the Add Resource dialog.
3. Enter `map` in the Search box, and click Search.
4. Select Worldwide Map, and click Add Selected Resources.
5. Click Preview, and if the map looks correct, click Done.

You have now added the Worldwide map to the view. Customize the world map now.

1. Click Edit in the Worldwide Map resource title bar.
2. Provide a Title and Subtitle for the map.

 Titles and subtitles can be entered as either text or HTML.

3. Enter a value for Height. The default is 400 px.
4. Click Set Location and Zoom Level if you want to change the default location (the center of the map) and zoom of the map.
To set the default zoom and location manually, click Advanced, and enter the latitude and longitude of the default location and the zoom level.
5. To filter the groups and nodes to be displayed, click Group and/or Nodes, and enter a SWQL filter.
Click Examples to see a few SWQL filter samples.
6. Click Submit.

Display events received during a given time period


1. Open the view where you want to add the events summary, and click Customize Page.
2. Click the plus sign in the column to open the Add Resource dialog.
3. Enter `event` in the Search box, and click Search.
4. Select Event Summary, and click Add Selected Resources.
5. Click Preview to preview the resource, and click Edit to customize the resource.
6. Select the time period for displaying events in Time Period.
7. Click Submit.

Specify user-defined links

You can copy URLs of external websites or customized views from preview pages, and copy them to the User Links resource.

1. Open the view where you want to add the links resource, and click Customize Page.
2. Click the plus sign in the column to open the Add Resource dialog.
3. Enter `links` in the Search box, and click Search.
4. Select User Links, and click Add Selected Resources.
5. Click Preview to preview the resource, and click Edit to customize the resource.

6. 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, select Open in New Window.

 Https URLs are not supported.

7. Click Submit.

Specify Custom HTML


When you have static information that you want to provide in the Orion Web Console, add the Custom HTML resource on a view. This resource can also provide quick access to customized views.

1. Open the view where you want to add the custom resource, and click Customize Page.
2. Click the plus sign in a column to open the Add Resource dialog.
3. Enter `html` in the Search box, and click Search.
4. Select Custom HTML, and click Add Selected Resources.
5. Click Preview to preview the resource, and click Edit in the resource.
6. Enter HTML formatted content as required.
7. Click Submit.

Filter nodes

The Orion Web Console can maintain a customizable node list for your network. Node lists can be configured for specific views using SQL query filters.

1. Open the view where you want to add the node list, and click Customize Page.
2. Click the plus sign in a column to open the Add Resource dialog.
3. Enter `nodes` in the Search box, and click Search.
4. Select All Nodes - Table, and click Add Selected Resources.
5. Click Preview to preview the resource, and click Edit in the resource.
6. 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:
 - 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.
7. Select the property for the filter text provided above:
 - 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.
8. To apply a SQL filter to the node list, enter an appropriate query in the Filter Nodes (SQL) field.


 By default, node list resources are designed to sort nodes alphabetically by node caption. This configuration cannot 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.

9. Click Submit.

Group nodes within a view

The Orion Web Console can maintain a customizable node list for your network. Node lists can be configured for specific views with node grouping.


1. Open the view where you want to add the node list, and click Customize Page.
2. Click the plus sign in a column to open the Add Resource dialog.
3. Enter `nodes` in the Search box, and click Search.
4. Select All Nodes - Tree, and click Add Selected Resources.
5. Click Preview to preview the resource, and click Edit in the resource.
6. Select up to three criteria, in specified levels, for Grouping Nodes within your web console view.
7. Select whether you want to put nodes with null values In the [Unknown] Group or ungrouped At the Bottom of the List.
8. To apply a SQL filter to the node list, enter an appropriate query in the Filter Nodes (SQL) field.

 By default, node list resources are designed to sort nodes alphabetically by node caption. This configuration cannot 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.

9. Click Submit.

Add a Service Level Agreement Line to charts (SolarWinds NPM)

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 displays the appropriate line on your charts.

-  ■ Interface data is only available in SolarWinds NPM.
- The SLA line may not appear immediately. It may take several minutes for the change to be detected by the Orion Web Console.


1. Click Settings > All Settings in the menu bar.
2. In Node & Group Management, select Manage Custom Properties.
3. Click Add Custom Property.
4. Select Interfaces as the custom property object type, and click Next .
5. Click SLA in the list of predefined Property Templates, make any required changes to the fields displayed, and click Next.
6. Click Select Interfaces.
7. Select and add all interfaces to which you want to apply the same service level, and then click Select Interfaces.
8. 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.

9. To enter a different SLA value for a different set of interfaces, click Add More.
10. Click Submit.

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.


Filter nodes in resources using SQL queries

When you are managing or monitoring large numbers of network devices, 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](#).

 If you have upgraded to Orion Platform version 2015.1.x or later, your custom SQL or SWQL query or filter may no longer work correctly. For a list of database changes from Orion Platform version 2014.2 to version 2016.1, including new tables, column changes, or data constraint or data type changes, see the [Database Changes](#) spreadsheet.

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

SQL Query Examples

 By default, node list resources are designed to sort nodes alphabetically by node caption. This configuration cannot 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.

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)


Specify what a Custom Object resource displays

Custom Object resources can display performance data for any monitored objects.

You can graph data for multiple objects on the same chart, such as memory usage on all storage devices. The resource can include a sum of all the series.

1. Click Edit in the resource.
2. Edit the resource Title and Subtitle.
3. Select an object type in Choose Object Type.

4. Select objects to be displayed in the resource:
 - a. Click Select Object.
 - b. In the Group By: field, select a grouping criterion.

 Defined custom properties are listed for all grouping types.

- c. Select objects (either a group, or expand a group and select individual child objects), and click the arrow to move the objects into the pane on the right.
 - d. Click Submit.

The selected objects will appear on the Edit Custom Object Resource page, together with appropriate options.

5. Select a Chart to include in your custom object resource.
6. If you want to automatically display nodes related to the current view, select the option in Select Object.
7. To limit the number of data series in the resource, select Limit Series, and select the number of series to allow.
8. Select whether or not you want to Show Sum in Data Series.
9. Select the Time Period and Sample Interval.
10. To automatically hide the resource when there is no data for it to report, select Yes for the Auto-Hide Resource option.
11. Click Submit.

Customize charts in the Orion Web Console

Use the customization options available in the chart to customize the data, layout and time frame shown by the chart.

Available customization options depend on the chart.

Drop-down customization options

Some charts have drop-down menus that include the following options:

- View chart data over the Last 7 Days or over the Last 30 Days
- Select Edit Chart or click on the chart to open the chart resort in a new tab.
- View Chart Data as an HTML format document
- View Chart Data in Excel to see chart data in an Excel™-compatible format


Edit Resource page

If a chart has an Edit button, click it to get to the Edit Resource page. Edit titles, time periods, or other details, and click Submit to go back to the view and see the changes applied in the chart.

Titles and subtitles

You can customize the title and subtitle for the resource and for the chart.


To change the chart labels, click Advanced, and enter a text or variable that displays as the chart title or subtitle.

 The default for the chart subtitle is `${ZoomRange}`, which shows the selected zoom range.

Other options depend on the chart type.

Calculated series: Show a trend line

Select the box to display a trend line on the graph. This shows potential future results as extrapolated from collected historical data.

 The trend lines are intended only as approximate predictions of future data.

Calculated series: Show the sum of all data series

Select the box if you want to display the sum of all data series in the form of stacked bars or lines.

Calculated Series: Show the 95th percentile line

Select the box to show the 95th percentile line. This is a well-known statistical standard used to discard maximum spikes, based on 5 minute data samples. The calculation gathers these values every 5 minutes for however long you select, throwing away the top 5% so as to yield the 95th percentile value.

Maximum Number of Items to Display:

Enter the highest number of items you want to display in this chart.

Time periods: Default zoom range

Select the default range of data to be displayed from the drop-down list.

Time periods: Amount of historical data to load


Select the amount of historical data to load from the drop-down list.

Time periods: Sample interval

Select the sample interval to be used from the drop-down list. Each sample interval is represented on a chart by a single point or bar. Data within a selected sample interval is summarized automatically.

Custom Chart page

Click Export or click the chart to open the Custom Chart page in a new tab. You can change the chart settings and click Refresh to see the changes applied in the same tab.

 If the chart has a drop-down menu, you can also access the custom chart page by selecting the Edit chart option.

Title, Subtitle, Subtitle #2

Enter a title and optional subtitles to be displayed above the chart.

Time Period: Select a Time Period

Select the time period that you want the chart to cover.

Alternatively, you can enter a specific time period for the chart.

Time Period: Beginning Date/Time

Enter the start date and time for the chart in one of the formats shown. If you do not enter a time, this will default to 12:00:00 AM.

Time Period: Ending Date/Time

Enter the end date and time for the chart in one of the formats shown. If you do not enter a time, this will default to 12:00:00 AM.

Sample Interval

Select the sample interval. Each sample interval is represented on a chart by a single point or bar. Data within a selected sample interval is summarized automatically.

Chart Size: Width

Enter a custom width, in pixels, for this chart. The default is 640.

Chart Size: Height


Enter a custom height, in pixels, for this chart. Enter 0 to maintain the original width/height ratio.

Font Size

Select the font size for the chart from the drop-down list.

Trend Line: Show Trend

Select the box to display a trend line on the graph. This shows potential future results as extrapolated from collected historical data.

 Due to the broad array of factors that can affect the performance of devices, trend lines are intended as approximate predictions of future data only.

Display Chart Data: Raw Data

Click to display or save the data being used in this report as an xls file.

Display Chart Data: Chart Data

Click to display the data in this report as a HTML table in the web browser.

Maintain the SolarWinds Orion database

All Orion Platform products use a Microsoft SQL Server database to store Orion Web Console settings and collected network performance and configuration data.

There are two utilities that allow you to perform the most commonly required database tasks without having to access either the Microsoft SQL Server or its associated tools.

Database Manager

Add SQL servers to your Orion configuration, view database information, perform queries or edit database values. See [View database details and data in the Database Manager](#).

Database Maintenance


Summarize, clean, and compact your SolarWinds Orion database. See [Run the database maintenance](#).

Back up and restore the database

You should use the SQL Server Management Studio to create and restore backups on your servers. The application should have been installed with the Microsoft SQL Server. You typically will manage backups when performing SolarWinds product upgrades, migrating to a new server, or as part of a maintenance schedule.

See the [Microsoft Support page](#) for information about creating backups with your version of the MS SQL Studio.

After performing a restore, you will need to [update the database location](#) through the console.


 While restoring the database, use the Restore with Recovery option.

For more information, search for "restore a database backup" on the Microsoft TechNet web portal at <https://technet.microsoft.com>, and consult the help for the appropriate SQL Server Management Studio version.

View database details and data in the Database Manager

The Database Manager is used to add additional servers to your Orion configuration, perform queries, view database and table details, export data, and edit database values.

For more advanced database maintenance, SolarWinds recommends that you use the Server Management Studio provided with Microsoft SQL Server to back up, clear historical maintenance records, and perform other maintenance.

 If you need to backup or restore a database, you should use the SQL Server Management Studio. For details, see [Creating a Database Backup](#).

Add a server to Database Manager

If you have not already designated a backup or supplementary database for use with your Orion Platform product, add a SQL server.


1. Start the Database Manager in the SolarWinds Orion > Advanced Features program folder.
2. To add a default server, click Add Default Server.
3. To select a server:
 - a. Click Add Server.
 - b. Select or enter the SQL Server instance you want to use in the `server/instance` format.
 - c. Select the appropriate authentication method, enter your credentials, and click Connect.

You can now see the server and associated databases in the tree structure of the Database Manager.

View database details

The Database Manager provides details per database to review current information. If the SQL server hosting your database is not listed, you should [add the database](#).

1. Start the Database Manager in the SolarWinds Orion > Advanced Features program folder.
2. If the SQL Server hosting your SolarWinds Orion database is not listed in the left pane, [add the SQL Server](#) hosting your Orion database.
3. Click + in the left pane to expand the SQL Server hosting your SolarWinds Orion database, and right-click the database.

 The default database name is `SolarWindsOrion`.


4. Click Database Details.
 - The Properties tab shows general statistics and descriptions of the selected database.
 - The Tables tab lists the tables and their respective sizes.
 - If you have not yet made a backup of the database, the Last Backup field on the Properties tab is blank.

View table details

You can view the Table details for a selected database including the include property, column, and index information through the Database Manager. You can also query the selected table directly from the Table Details window for specific or additional data.

1. Start the Database Manager in the SolarWinds Orion > Advanced Features program folder.
2. If the SQL Server hosting your SolarWinds Orion database is not listed in the left pane, [add the SQL Server](#) hosting the database.


3. Expand the SQL Server hosting your SolarWinds Orion database in the left pane, and expand the SolarWinds Orion database.

 The default database name is SolarWinds Orion.

4. From the tables displayed for the database, right-click any table to view the Table Details.
 - The Properties tab includes general statistics relating to the selected table size and creation date.
 - The Columns tab lists keys, column names, size and data types in the selected table.
 - The Indexes tab shows indexes used in the table.
5. To execute a query:
 - a. Right-click the table name, and click Query Table.
 - b. Adjust the default SQL query or create a new one, and click Execute.
The default SQL query lists the contents of the table.
6. To export a table, right-click the table name, and click Export to CSV. You will be asked to enter a name for the comma separated value file created.


Edit database fields

You can edit database fields in the Database Manager. We do not recommend changing values directly in the database unless clearly directed to do so by Support or as completed by a DBA. As you make changes and capture data through the Orion Web Console, this data saves safely to the database.

 Table editing should only be performed by a database administrator (DBA) or other expert user. Changes made directly in your database can jeopardize the integrity of your data.

SolarWinds recommends that you change database settings and values using the Settings with your Orion Web Console.

1. Start the Database Manager in the SolarWinds Orion > Advanced Features program folder.
2. If the SQL Server hosting your SolarWinds Orion database is not listed in the left pane, add the SQL Server hosting the database. See [Add a server to Database Manager](#).
3. Expand the SQL Server hosting your SolarWinds Orion database in the left pane, and expand the SolarWinds Orion database.


 The default database name is SolarWinds Orion.

4. Right-click a table, and click Table Details.
5. Adjust the default SQL query or create a new one, and click Execute.
The default SQL query lists the contents of the table.
6. To edit the data in a table, click Enable Table Editing, and edit the fields in the table.

Run the database maintenance

Database maintenance optimizes the size of your SolarWinds Orion database by repeated summarizations of data. Data summarization gathers the collected network data for a defined period, calculates statistics from the data, and discards the data itself while retaining the statistics.

Database maintenance runs every day at a specified time.

 To set time for database maintenance or to run it manually, you need administrator privileges.

Specify when the maintenance runs:

1. Click Settings > All Settings in the menu bar.
2. In the Thresholds and Polling section, click Polling Settings.
3. Scroll down to the Database Settings section, and enter the time to run the database maintenance in Archive Time.

Launch data maintenance manually:

1. Start Database Maintenance in the SolarWinds Orion > Advanced Features program folder.
2. Click Start.

Best practices and troubleshooting for SolarWinds Orion database

As your SQL database matures, or after adding Orion Platform products, your database may become larger than you originally estimated or might slow unexpectedly. Most common database issues are related to storage capacity and database performance. These best practices and troubleshooting tips provide preventive steps to take to ensure your database stability and performance.

Adjust how long you want to keep historical data

Consider how long you need to archive monitored data. You can reduce the amount of data in the database by shortening retention periods.

1. Log in to the Orion Web Console as an administrator.
2. Click Settings > All Settings in the menu bar.
3. In the Thresholds & Polling section, click Polling Settings, and scroll down to Database Settings.
4. Adjust the retention settings for containers, interfaces, wireless, or UnDP.



When adjusting a data retention period, make small changes, and examine the impact on size and performance.

5. Click Submit to apply the changes.

How does altering data retention affect database size?

In the SolarWinds Orion database, detailed data are summarized into hourly data increments and then into daily data increments.

The shorter the data interval, the greater the effect the setting will have on the database size.

- Extending the detailed data retention will have the largest potential impact on database size and performance.
- Extending hourly retention will have a lesser effect.
- Extending daily retention will have the least effect.

Design a database maintenance plan

The database maintenance should include:

- A tested backup and restore plan. Use the Microsoft SQL Studio to back up and restore your database.
- Database maintenance within your Orion. Specify an off-peak hour to run the maintenance. See [Run the database maintenance](#).
- An analysis of white space within the database files. This is analogous to data fragmentation.
- A general data integrity check.
- A re-indexing routine
- Detection of index fragmentation. This causes index searches to slow or fail.

Prevent fragmentation problems


- Do not use auto grow or auto shrink when possible. Auto grow and auto shrink can result unnecessary database tasks and index fragmentation.
- Do not manually shrink your database to recover disk space. If you shrink a database with insufficient space to update index files, the index may become fragmented and incomplete so that indexed searching is not possible. Orion Web Console will time out constantly.
- Include re-indexing in your maintenance routine.

Troubleshooting

Bad performance

In the SolarWinds Orion database, the most important SQL server performance measurement is disk queue length.

Queue length is a measurement of the SQL writes that are waiting to be written to disk. When disk queues start lengthening and there is a steady load on the SQL writes, the queues may grow so large that write requests get dropped. This may lead to gaps in data and will affect the overall performance of the SQL server.

 The disk queue length should not exceed two times the number of effective spindles in the SQL storage. The effective spindle count is the number of striped spindles.

For a RAID 10 direct attached storage unit with eight total disks, the effective spindle count is four. Four of the spindles in this array are the primary striped array and the other four are a secondary striped mirror of the four primary spindles. Since no performance gain is achieved by mirroring disks, only the primary striped set is used to measure performance.

Lost connection to the database

- Ping the SQL server from the Orion server to check network connectivity.
- Open SQL Server Management Studio or the Orion Database Manager, and attempt to connect to the database.
- If both of the above are successful, start the Configuration Wizard in the SolarWinds Orion > Configuration and Auto-Discovery program folder, select Database in the first screen, and complete the wizard. Make sure you are using the proper database credentials.
- Open the Orion Web Console to test connectivity again.
- Test opening an ODBC connection from the Orion server using a Microsoft utility, such as ODBCping.

If all of this fails, the issue is a failure of the SQL server. Consult the [Microsoft Support site](#), and search for information pertaining to your SQL server version.


Prepare to upgrade or migrate the SolarWinds Orion database

At some point, you may need to upgrade or move your SolarWinds Orion database. For example, you may have to change your version of Microsoft SQL Server or migrate your data to a different server. New versions of SolarWinds products may require a new SQL version or merge databases with other products. Refer to your product documentation, release notes, and the [Solarwinds Success Center](#) to verify changes and requirements.

Requirements

Before you attempt to modify or back up your existing database, ensure the following:

- The new database server is installed correctly and meets all requirements for CPU, hard drive space, software, and additional settings. Refer to your product requirements (in documentation or release notes) for the listed SQL database system requirements.


 Due to the size and usage of the Orion database, we recommend having this database on a dedicated server. Depending on your current environment, database location, and upgrade SQL server requirements, you may need to migrate to a new server. Migrating allows you to keep all relevant data and history without having to start with a fresh database on a new server.

- The SQL Browser Service is running on the new target server. This service runs on UDP port 1434, and it may be blocked by internal firewalls.

- You have the `sa` password for both your existing SolarWinds Orion database server and your new database server.
- You have the credentials to an account with administrator rights on both your existing SolarWinds Orion database server and your new database server. For migrations, make sure you have the local administrator credentials.
- Schedule a maintenance window during off peak hours. During an upgrade or migration, you will need to stop your Orion services, ensuring polling data does not attempt writing to the database. This also ensures your backup file matches your last active database state.
- When migrating, stop all Orion services before creating a backup.
- Include your DBA in the installation of a new database version or migration to a new server.
- Notify your company of the changes and maintenance window.


Upgrade your SQL Database

Upgrading a database means migrating from one version of SQL to another. We recommend following the detailed instructions from your database software vendor for migrating between versions. Database migrations may require following an upgrade path specific to the vendor. For more information, refer to Microsoft TechNet web portal at <https://technet.microsoft.com> and search SQL migration.

 You may also need to migrate your SQL database to a new version. Due to database size, you may want to migrate to a new version after migrating to a new server.

Update Orion Platform products to use the new database

After you have restored your SolarWinds Orion database backup file on the new server, you must update the database location for the Orion server to access the restored database on the new database server.

 SolarWinds recommends that you use SQL Server Authentication with the `sa` login and password to ensure that Orion can always access the SolarWinds Orion database, even if it is hosted remotely on a separate server.

1. Log in to your Orion server.
2. Start the Configuration Wizard in the SolarWinds Orion > Configuration and Auto-Discovery program folder.
3. Select Database, and click Next.
4. Specify your new database server in the SQL Server field.
5. To use SQL authentication, select Use SQL Server Authentication, provide the credentials, and click Next.
6. Select Use an Existing Database, select or type the existing database name, and click Next.
7. If you are prompted to use the existing database, click Yes.

8. Select Create a New Account, and provide a New Account name.




- Creating a new account ensures that Orion has required access to your migrated database.
- The New Account must be a member of the `securityadmin` server role.
- The `sysadmin` role and the `sa` user account are always members of `securityadmin`.

9. Provide and confirm an account Password, and click Next.

10. Click Finish to exit the Configuration Wizard.

Create and view reports

SolarWinds provides predefined reports for each Orion Platform product. Use the web-based interface to customize these predefined reports and create your own reports.


 You must use the Orion Report Writer to maintain legacy reports created with Orion Report Writer.

Predefined reports

Your SolarWinds installation comes with many predefined reports that can be used as soon as there is data to be reported on. View a list of predefined reports by clicking Reports > All Reports in the menu bar.

These predefined reports are sufficient for most needs, but can be further customized. You can also create new reports.

Create, schedule, export, and import reports in the Orion Web Console

 The Orion Web Console does not allow you to edit legacy reports created with the Orion Report Writer.

Create reports in the Orion Web Console

Highly customizable reports, featuring the same charts, tables, gauges, and resources available in your views, can be created directly from the Orion Web Console.

There are two ways to create a new report:


- **Modify an existing web-based report (recommended).** Add new content to or edit the existing content of an existing report. This is the recommended approach for new users.
- **Create a completely new report.** Select the layout and contents for the report.

Modify an existing web-based report

Modifying an existing web-based report is often the simplest way to generate a new report. You can add pre-existing resources or create a custom table or chart. You can also edit information about each resource.

1. Click Reports > All Reports in the menu bar, and click Manage Reports.
2. Select Report Origin in the Group by drop-down menu in the left pane, and select Web-based from the list.
3. Select the report to use as the basis for your new report, and click Duplicate & Edit.
4. Click Add Content.


5. Select the resource to add to the report, and click Select and Continue.

 Some resources require you to choose a specific object to report on. For example, if you want to track how many people use a specific application, you must choose the application when adding the resource.

6. Click the Edit button on the resources to make changes such as filtering the objects, group columns, or setting a sample interval. Available options depend on the type of resource you add.
7. Click Next to display the Preview view, and click Next.
8. Add report properties, such as categories or custom properties. Use the [report limitation](#) category to restrict the report to specific user accounts. Click Next.
9. Schedule the report by clicking Schedule this report to run regularly, and creating a new schedule or adding the report to an existing schedule. Click Next.
10. Review the Summary and click Submit to save the report.

Create a new web-based report

Web-based reports are created in the Orion Web Console, and can be restricted to specific users through [report limitations](#). Users may be assigned specific report limitation categories and can only view reports that are in the same report limitation category.

 SolarWinds recommends that you duplicate and edit an existing web-based report instead of creating a new one.

1. Click Reports > All Reports > Manage Reports > Create New Report.
2. On the Layout Builder panel, click Add Content. You may be prompted to add content as soon as you click Create New Report.

3. Select the first resource to add to the report and click Select and Continue.

Some resources require you to choose a specific object to report on. For example, if you want to track how many people use a specific application, you must choose the application when adding the resource.

The Layout Builder view is displayed with the selected resource added.

Add Content

1. Please select particular resource...

Available Resources:

GROUP BY:
Type
Alerts
Inventory Lists
Network Maps
Page Formatting
Pie Charts
Reports

Resource name
<input type="radio"/> Advisors
<input type="radio"/> Advisors from all Databases with the Highest Wait Time
<input type="radio"/> Applications Using All My Databases
<input type="radio"/> Applications Using My Databases
<input type="radio"/> Applications Using This Database
<input checked="" type="radio"/> Availability of Each Node
<input type="radio"/> Component Volumes

2. Select objects

SELECT AND CONTINUE

CANCEL

4. In the Content area, add resources and sections to the report. You can also [modify the layout](#).
 - a. Click Add content to add resources to your report. For more information, see [Add content to a web-based report](#).

- b. Click Add section to add more rows of content to this report.

The screenshot shows a 'Content' panel with a header bar. Below the header, there is a 'Layout columns' dropdown set to '1' with up and down arrows. A '100%' width indicator is visible. The main area contains two resource cards. The first card is titled 'Availability of Each Node' and has an 'EDIT RESOURCE' button. The second card is titled 'Active Group Alerts' and has an 'EDIT RESOURCE' button. Below the second card, there is a 'For' dropdown menu showing 'New York IT Department' and an 'Edit' button. At the bottom of the panel, there is a dashed box containing an 'Add Content' button, and another dashed box below it containing an 'ADD SECTION' button.

5. To filter a resource to include a specific set of data, click Edit Resource. Not all resources can be filtered.

This screenshot shows the 'Content' panel with the 'Availability of Each Node' resource card selected. The 'EDIT RESOURCE' button is highlighted with a blue border. The 'Active Group Alerts' card is no longer visible, and the 'Add Content' and 'ADD SECTION' buttons are also absent.

6. Filter the resource and click Submit.

Each resource has different filter options.

Edit Resource: Availability of Each Node

Title:
Availability of Each Node

Subtitle:

Time Period:
Select a Time Period: Today ▼
- or -
Beginning Date/Time:
Ending Date/Time:

Filter Nodes (SQL)
Device_Owner Like 'New*'

Filters are optional and can be used to limit the list of Nodes displayed.
This is an advanced feature. We recommend you have a basic understanding of SQL Queries.
▶ [Show Filter Examples](#)

SUBMIT

7. After adding and filtering the resource, enter a report name, and click Next.
8. On the Preview panel, click Next.
9. Add report properties, such as categories, custom properties, or limitations, and click Next.
10. To schedule the report, click Schedule this report to run regularly, create a new schedule or assign a schedule, and click Next.
You can schedule a report to be generated, emailed, saved, or printed.
11. Review the Summary and click Submit to save the report.

Customize a web-based report layout

You can customize how the report looks, such as the width, header, or number of columns. By default a report is 960 pixels wide with a header and footer, and a single column for content.

1. Select a report to edit from the Report Manager.
2. In the Layout Builder page, change the width of your new report by doing one of the following:
 - Click Fit to window width so the content of the report expands to the width of the browser window.
 - Enter a new value, in pixels (px), in the Report width field.
3. Click Browse for logo to change the default logo. The Logo check box **must** be selected in the Header area. Changing the logo does not affect other reports.


The maximum image size is 600 pixels wide and 240 pixels high.

4. In the Content area, change the number of columns or rows. You can select a predefined page layout or manually add columns and rows.
 - Enter a number in the Layout columns field to change the number of columns.
 - Click Add section to add more rows
5. Select the Footer check box to include a footer in your report. Select each option you want included.


Add content to a web-based report

You can include any Orion Web Console resource, including charts and graphs, in a report.


The following procedure assumes you are already [creating](#) or [editing](#) a report in the Orion Web Console.

 Resources can be dragged between columns and sections.

1. On the Layout Builder page, click Add Content in the column to which you want to add a new resource.
2. Use the Group by field to filter the available resources or search for a specific resource.

 The Classic category grouping provides the most comprehensive list of available resources.


3. Select the resource from the list in the main pane.

 If you are an advanced user and want to add a Custom Chart or Table, see [Add a custom chart or table to a web-based report](#).

4. Click Select and Continue.
5. If the resource requires you to select specific objects:
 - a. Select the required objects from the left pane.
 - b. Click Add to Layout.
6. You can edit the resource if you want to change the title or subtitle.
7. If you want to add another row to your report, click Add section. You can now add content to this row as described above.


Add a custom chart or table to a web-based report

You can create custom charts or tables for inclusion in web-based reports. Custom charts or tables are usually added when you are familiar with your SolarWinds Orion database or are comfortable creating SQL or SWQL queries. Because the Orion Platform generates so much data, you need to ensure that you know exactly what data you are using, from which instances it originates, and what you do with them to ensure that your custom charts and tables show meaningful results.


 You can reuse customized charts or tables by clicking Use previously specified objects when adding the chart or table and then selecting the object.

1. Click Add Content in the column to which you want to add a custom chart.
2. Group by Reports to find the Custom Chart or Custom Table resources.
3. Select Custom Chart or Custom Table, and click Select and Continue.

4. Use one of the following methods to configure the objects displayed in the chart or table:
 - Specific Objects (static selection) - use when you know which objects you want to include in your chart or table.
 - a. Filter or search for the objects you want to include.
 - b. Select the objects' check boxes.

 This is the most straightforward selection method, and recommended for new users. It is also the preferred method for relatively permanent network objects.

- Dynamic Query Builder - use to select objects based on object properties.
 - a. Select Basic Selector to create and/or queries or select Advanced Selector to create complex queries.
 - b. Choose the object type you want to include.
 - c. Enter your [conditions](#).

 This is the preferred selection method for groups of objects of a specified type that may change over time. "All Cisco nodes in Austin" is an example of a group best defined using the Dynamic Query Builder.

- Advanced DataBase Query (SQL, SWQL) - only use if you are comfortable querying your SolarWinds database directly using SQL or SWQL.
 - a. Select SQL or SWQL, and enter your query.
 - b. Click Preview Results to test your query.


5. Enter a name for this selection in the Selection Name field, and click Add to Layout.

You must now edit the [chart](#) or [table](#) to choose the data series or columns you want to use and modify display and filtering settings.

Add a data series and customize a chart


Once you have specified the objects for your custom chart, you need to select the data series. You can also change the sample interval and filter the results.

1. If you have just added a custom chart, the Edit Resource page opens. Click Edit Chart on the resource in the Layout Builder page to open this page.
2. Click Add Data Series in Left Y-axis.
3. Filter or search for the data series, and select the one you want to use.


 The groups available and the data series within these groups will depend on the object selected.

4. Click Add Data Series. The data series is added to the Left Y-axis.
5. For additional settings for each data series, click More. Here you can:
 - Edit the Display name for this data series.
 - Select a custom Color for this data series.
 - Show the 95th percentile line for this data series.
 - Show Trend for this data series.
6. Enter a Custom label for the Left axis.
7. Select the Units displayed, Chart type, and select the Show the sum of all data series, if required.

8. Select the Sample Interval. This can be as frequent as once a minute to once a week. Data within each sample interval are summarized so that a single point or bar is plotted for each of these periods.

 It is possible to select a sample interval that is longer than the reporting period.

9. Choose how you want to filter your report.
 - a. Select how you want to sort this selection of records from the Sort records by drop-down menu. The choices depend on the data series selected.
 - b. Select either Ascending or Descending from the Sort order drop-down.
 - c. Select the Data aggregation method required to summarize your data by time period.
 - d. Click Advanced if you want to sort records using a secondary field.
10. Set up additional data series using the right axis to superimpose two charts using different labels, units, and chart type.


 You cannot use a separate time period or filter results settings for the right axis series.

11. Click Submit to return to the Add Report page.

Add a data series and customize a table


After you have specified the objects to be reported on for a custom table, select the data series. You can also sort and filter the results.

1. If you have just added a custom table, the Edit Resource page opens. You can open this page by clicking Edit Table on the resource in the Layout Builder page.
2. Click Add Column.
3. Filter or search for the column, and select the column you want to use.

 The columns and options available depend on the objects selected.

4. Click Add Column.
5. For additional settings for a column, click Advanced. Here you can:
 - Edit the Display name for this column.
 - Select Hide this column in the resulting table, if you want to use this column when querying the database but do not want to show it. For example, you may want to use this column's data in the time-based settings but not show the data in the table.
 - Select Allow HTML tags, if you want to use any HTML tags retrieved from the database for this column.
 - Select the Display settings to be used for this column. This applies the selected formatting to the data in this column.
 - Select the Data aggregation method to use for this column, to summarize your data by time period.
 - Select the Alignment for this data. This can be left, right, or center.
6. Click the plus sign in the table layout section to add more columns.
7. Filter the number of records shown in the table by either a specific number or a percentage.


8. Restrict data in your table to a specific time period by selecting Yes from the Time-based settings drop-down menu.

 You can only do this if your table contains a column with historical data.

- a. Select the column used to specify the time period from the Date/Time column in this table drop-down menu.
 - b. Select the Sample Interval. This is used to summarize your data by time period.
9. Use the Group results by option to organize the table by the values in the columns you select.
10. Click Submit to return to the Add Report page.

Build conditions


Use the Dynamic Query Builder selection when objects may change over time. For example, as your network ages, you will replace or upgrade various pieces of equipment. You can select each piece of equipment individually, or you can create a dynamic query that adds objects to the custom chart or table based on the properties you select.


 The Advanced Selector provides access to all network object characteristics, and the Basic Selector provides access to a smaller subset of the most frequently used network object characteristics.

1. Select the type of selector query you want to use (Basic or Advanced).
2. Select the type of objects to report on from the I want to report on drop-down menu.
3. For the Basic Selector:
 - a. Click Add Condition.
 - b. Select All child conditions must be satisfied (AND) or At least one child condition must be satisfied (OR).
 - c. Select a property of the monitored object, a conditional relation, and provide a value.
 - d. Click Add Simple Condition if you want to add another condition.
4. For the Advanced Selector:
 - a. Select All child conditions must be satisfied (AND) or At least one child condition must be satisfied (OR).
 - b. Select which field you want to evaluate, a conditional relation, and provide a value.
 - c. Click the + sign to add child conditions.
 - Add Single Value Comparison (Recommended) - The child condition evaluates a single field, like Status
 - Add Double Value Comparison - The child condition evaluates two conditions, such as Status and OS
 - Add And/Or block - Adds a sub condition block

Restrict who can access reports


Use report limitation categories to limit access to any SolarWinds report created on SolarWinds Orion Platform versions 2013.1 and later. Users with a report limitation category set can only see reports that are in the same report limitation category.

 The No Reports limitation is a special report limitation category that removes all access to reports when applied to a user account. You do not need to add No Reports as a limitation in the report properties.

-  ■ If you are running SolarWinds Orion Platform versions 2012.2.X or earlier, reports are stored in a folder on the primary SolarWinds server (default location C:\Program Files\SolarWinds\Orion\Reports). Place reports into subfolders and restrict user access to the file system to limit user access.
- If you are running SolarWinds Orion Platform version 2013.1.X or later, reports are stored in the SolarWinds database, and both users and reports may be assigned a report limitation category to restrict who can access the report.

Create or add a report limitation category

When you create or edit a report, expand Report Limitation on the Properties page to add a report limitation. Choose an existing limitation or enter a new one.

 Each report can have only one limitation.

After the report limitation is created and the report saved, the limitation is available in the user settings.

Restrict user access to the report

After the report limitation is saved, it is available in the user account's [Define Settings page](#).

In the Report Limitation Category, select the limitation, and save your changes.

Generate reports on a schedule

Schedules enable you to set up report actions to occur at specific times. These actions let you generate reports and print them, save them to disk, or email them to selected recipients. You can create schedules for single or multiple reports, or assign reports to existing schedules. In addition, you can add URLs to the schedules so that screen captures of specific websites at the time the reports were generated are included.


- Reports can be assigned to schedules when they are being edited, created, or in the Schedule Manager.
- Schedules can be created from the Report Manager, the Schedule Manager, or when you create or edit a report.

Schedule a report to run automatically while creating or editing a report

You can directly assign a report to a schedule while [editing](#) the report.

1. Navigate to the Schedule Report page.
2. Click Schedule this report to run regularly, and select Create new schedule.

3. Click Add Frequency, and then select when you want to run the report.

 Click Add Time to select additional dates and times.

- To delay when the report runs, select Specific Date in the Starting On field, and then select the date and time when you want the schedule to start.
 - To stop the report from running automatically, select Ending On, and then select the date and time when you want the schedule to end.
4. Click Add Frequency.
 5. Click Add Action, and select the action (Email, Print, or Save to Disk) to be executed on the configured schedule.
 6. Click Configure Action.
 - For email actions, enter the recipients, the message, and the SMTP server.
Select Include Report's URL to allow recipients to access the report remotely.
 - For print actions, enter the Windows credentials necessary to access your printer, the printer, and print settings.
 - For save actions, enter the location you want to save the report to, the credentials in `domain\username` format, and the file type you want to save the report as. The location must be accessible from the Orion Web Console server.
 7. Click Add Action.

The action is added to the Actions list. You can add multiple actions.

Create and assign report schedules in Report Manager


The Report Manager provides a list of all reports that have been set up for your SolarWinds Orion web-based reports. You can create schedules and assign reports to schedules.

Create a report schedule

1. Select a report.
2. Click on Schedule Report > Create New Schedule to display the Properties view.
3. Add additional reports to this schedule by clicking Assign another Report.
4. Click Assign Webpage to include a snapshot of the selected website, and enter the URL in the field displayed. You can assign multiple webpages.

 Start each URL with `http://` or `https://`.

5. Expand Advanced Settings to specify a user account so that its limitations are applied to this schedule. Click Another User, and enter the User name or Account ID and Password.
6. Click Next to display the Frequency view.
7. Click Add Frequency, and then select when you want to run the report.

 Click Add Time to select additional dates and times.

- To delay when the report runs, select Specific Date in the Starting On field, and then select the date and time when you want the schedule to start.
- To stop the report from running automatically, select Ending On, and then select the date and time when you want the schedule to end.

8. Click Add Frequency, and then click Next to display the Actions view.
9. Click Add Action, and select the action (Email, Print, or Save to Disk) to be executed on the configured schedule.
10. Click Configure Action.
 - For email actions, enter the recipients, the message, and the SMTP server.
Select Include Report's URL to allow recipients to access the report remotely.
 - For print actions, enter the Windows credentials necessary to access your printer, the printer, and print settings.
 - For save actions, enter the location you want to save the report to, the credentials in `domain\username` format, and the file type you want to save the report as. The location must be accessible from the Orion Web Console server.
11. Click Add Action.
12. Click Next to display the Summary view.
13. If the schedule summary is correct, click Create Schedule.

The schedule is displayed in the Schedule Manager.

Assign a report to a schedule or multiple schedules

1. Select one or more reports.
2. Click Schedule Report > Assign Existing Schedule.
3. Select the schedule or schedules in the Assign existing schedule list and clicking Assign Schedule(s) to confirm that you want to assign the report.

Schedule reports from the Schedule Manager

The Report Scheduler provides a list of all report schedules that have been set up for your SolarWinds Orion web-based reports. You can create, edit, run and delete schedules from this page, and assign reports to schedules.

1. Click Reports > All Reports in the menu bar, and then click Manage Reports in the upper right.
2. Click the Schedule Manager tab.
3. Click Create New Schedule to [add a new schedule](#).
4. Select the schedule and click Run Now. The selected schedule runs, which includes the associated reports and report actions.
5. Select the schedule and click Assign to a Report.

Export reports

The most appropriate format for exporting a report depends on how you want to use the exported file. The different formats in which reports can be exported are shown below. The most common formats for exporting reports have their own icons on the Orion Web Console report page. Report Writer is a legacy feature that you can access on your SolarWinds Orion server.


Formats	Orion Web Console	Report Writer
XML	✓	
Excel	✓	✓
PDF	✓	✓
HTML and MHTML		✓
Image (BMP, GIF, JPG, PNG, etc.)		✓

Export reports as XML

You can save reports from the Orion Web Console in XML format and import them back.

1. Click Reports > All Reports in the menu bar, and click Manage Reports in the upper right corner.
2. Display the web-based reports.
3. Click the report > Export/Import, and then click Export Report.
4. Click Save.

Import XML reports


 If you import a report with the same name as an existing report, it will be prefixed with "Copy of".

1. Click Reports > All Reports in the menu bar, and click Manage Reports in the upper-right corner.
2. Display the web-based reports.
3. Click Export/Import, and then click Import Report.
4. Navigate to the required XML file on a network drive, and then click Open.
5. The file will be imported and its name displayed at the top of the list of reports.

Export Excel and PDF reports from the Orion Web Console

You can view and edit Excel files as spreadsheets. You can create read-only files using the PDF export that retain the exact formatting used in the original report.

1. Click Reports > All Reports in the menu bar, and click Manage Reports in the upper-right corner.
2. Open the report.
3. Click either Export as Excel or Export as PDF.

 The Export to Excel button is only displayed if the report contains only custom table resources. Other resources cannot be converted to the Excel format.