GETTING STARTED GUIDE

Network Performance Monitor

Version 2024.4

Part 1 of 2: Get Started

Last Updated: Tuesday, October 15, 2024

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS, OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON THE DOCUMENTATION, INCLUDING WITHOUT LIMITATION NONINFRINGEMENT, ACCURACY, COMPLETENESS, OR USEFULNESS OF ANY INFORMATION CONTAINED HEREIN. 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.

Table of Contents

Network Performance Monitor Getting Started Guide

Welcome to the Getting Started Guide: Part 1.

To learn how to start monitoring your network, complete the following tasks:

☑ **Install NPM**.

See the SolarWinds Orion Installer for system requirements, planning checklists, and installation instructions. The Getting Started Guide expects that you have already installed NPM.

□ **Discover the devices** on your network and select devices **to monitor**.

- What should you monitor?
- How to discover the network, add discovered devices or a single node for monitoring.

□ **Investigate** devices with **issues**:

- Meet the user interface - the SolarWinds Platform Web Console.
- Troubleshoot a node that has a problem.
- Troubleshoot an interface that has a problem.

□ Resolve an **alert** that was triggered.

□ Run a predefined **report** and schedule the report to run regularly.

When you have finished this guide, see Getting Started Guide: Customize to get familiar with basic customization procedures and Beyond Getting Started for information about other features.

Existing customers: Access your licensed software from the SolarWinds Customer Portal. If you need any help, contact our Support Reps.

Evaluators: Download your free 30-day evaluation from www.solarwinds.com. If you need assistance with your evaluation, contact sales@solarwinds.com.

What should I monitor on my network?

Before you begin monitoring, identify the devices to monitor in your environment.

Use the Discovery wizard to scan your network for nodes and associated entities. You can review found nodes and elements and add the devices to the SolarWinds Platform database for monitoring.

> The first time you discover your network, add a limited number of edge routers or switches, firewalls and load balancers, and critical physical or virtual servers and hosts. After you have the monitoring, alerts, and reports set up, SolarWinds recommends adding more nodes.

Discovery checklist

Before you run the Discovery wizard, gather the IP addresses and credentials for the devices you want to monitor.

☐	Determine the devices to monitor.

□ Determine the method used to monitor your devices, and make sure it is enabled on the devices.

- SNMP: primarily used to monitor network devices, such as routers, firewalls, and switches. To enable SNMP, consult the device documentation.
  SNMP requirements
  - For correct device identification, monitored devices must allow access to the SysObjectID.
  - Unix-based devices should use the version of Net-SNMP (5.5 or later) specific to the Unix-based operating system in use.
  - You can monitor VMware ESX and ESXi Servers versions 4.0 and later with VMware Tools installed.
  - If SNMPv2c is enabled on a device, by default, SNMPv2c is used to poll the device for performance information. To poll using only SNMPv1, you must disable SNMPv2c on the polled device.
- WMI: usually enabled on Windows devices by default. If the polling engine and device are separated by a firewall, SolarWinds recommends that you deploy an optional agent to securely monitor Windows servers and applications by WMI.

> ⓘ For Windows servers, SolarWinds recommends using WMI polling. For a non-Windows server, SolarWinds recommends using SNMP.

The following table outlines the pros and cons of using SNMP and WMI.

	SNMP	WMI
Bandwidth, CPU, memory usage on the host/poller	✓	⚠ Uses more bandwidth, CPU, and memory than SNMP per poll.
Monitoring across firewall/NAT-ed WAN connection	✓	⚠ Requires an agent for secure monitoring over one port.
Windows mount points and application metrics	❗ Cannot collect Windows mount point statistics or application level metrics.	✓

□ Determine IP ranges or individual IP addresses you want the system to scan as it discovers your network.

□	Determine SNMP v1/2 community strings and SNMP v3 community strings and credentials of the devices to monitor.
□	Determine log in credentials for each monitored device.
□	Determine VMware host credentials. The system requires read-only permissions.
□	Determine Windows credentials: domain or local admin.

Discover your network with NPM

After you have installed and configured NPM, log in to the SolarWinds Platform Web Console and scan your network for devices to monitor.

Log in to the SolarWinds Platform Web Console

In a web browser, navigate to `http://HostnameOrIPaddress:port`, where

- `HostnameOrIPaddress` the hostname or IP address of the server where NPM is installed
- `port` is the port defined for the website, specified in the Configuration wizard. By default, this is 8787.

Discovery is a term used to describe the process to identify network elements.

Before you discover your network, go through the Discovery checklist.

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 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. A network discovery job can take a long time to complete, and so 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 the discovery can use the devices specified in Active Directory instead of scanning every IP address.

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.

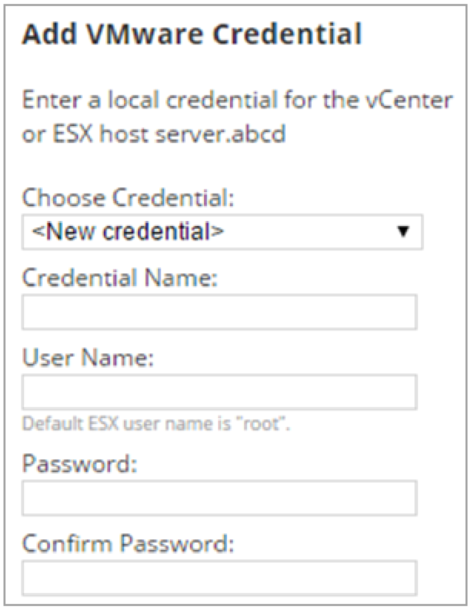
   This setting ensures that any agents you deploy, including the one on your SolarWinds Platform server, are up-to-date. If there are no nodes using agents, you can leave this option unchecked.

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, the virtual machines (VMs) on the host are still discovered. 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".

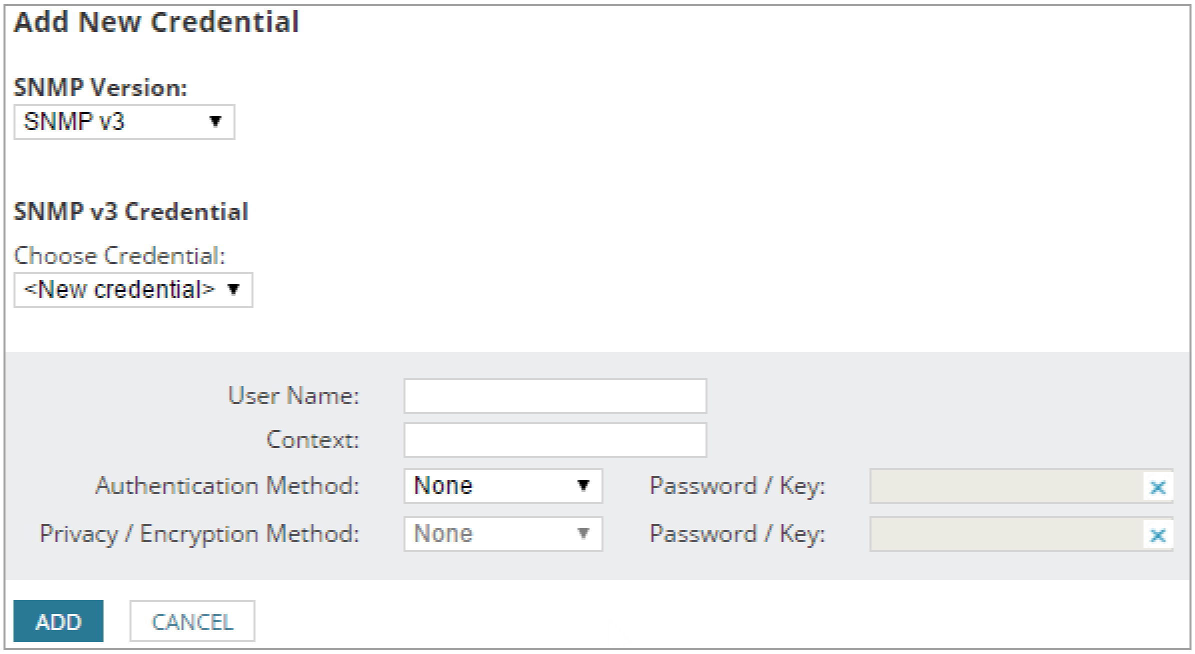
Password:

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 stings, 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 ▼

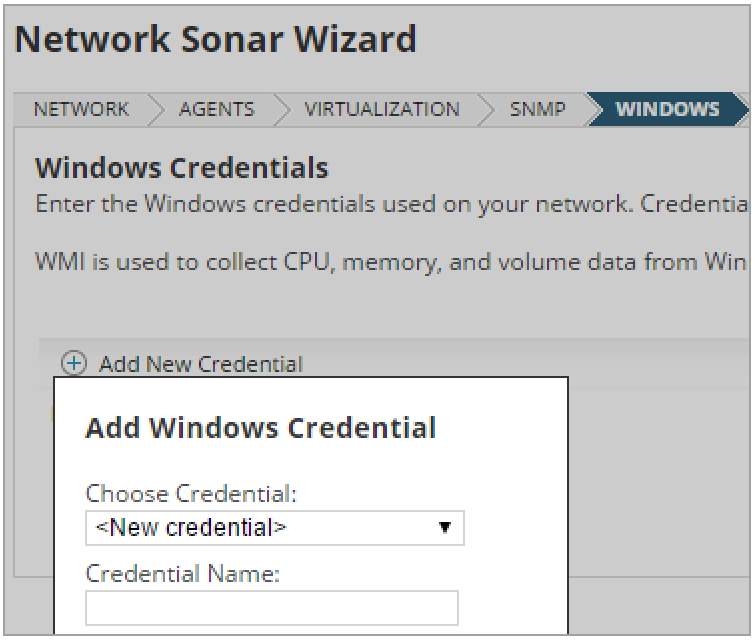
SNMP v3 Credential

Choose Credential:
<New credential> ▼

User Name:
Context:
Authentication Method: None ▼ Password / Key:
Privacy / Encryption Method: None ▼ Password / Key:

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

Windows Credentials

Enter the Windows credentials used on your network. Credentia

WMI is used to collect CPU, memory, and volume data from Win

⊕ Add New Credential

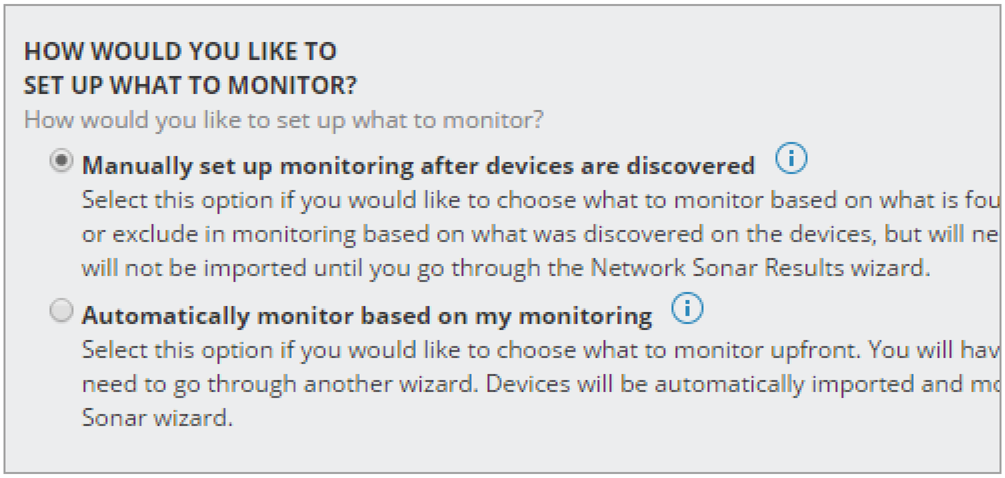
Add Windows Credential

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?

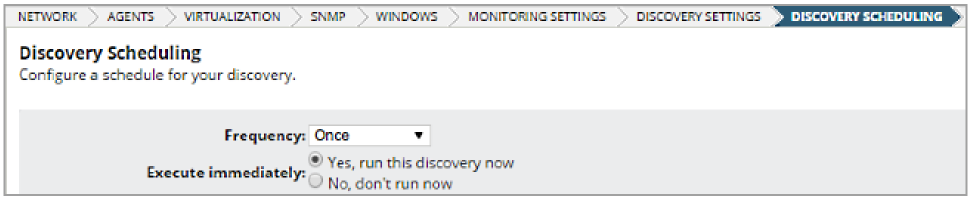
How would you like to set up what to monitor?

● **Manually set up monitoring after devices are discovered** ⓘ
Select this option if you would like to choose what to monitor based on what is fou
or exclude in monitoring based on what was discovered on the devices, but will ne
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 hav
need to go through another wizard. Devices will be automatically imported and mo
Sonar wizard.

9. On the Discovery Settings panel, click Next.

10. Accept the default frequency and run the discovery immediately.



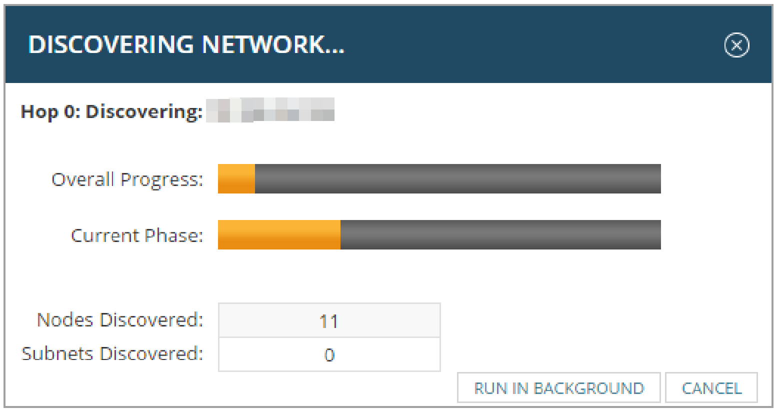
Discovery Scheduling

Configure a schedule for your discovery.

Frequency: Once

Execute immediately:
● Yes, run this discovery now
○ No, don't run now

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



DISCOVERING NETWORK...

Hop 0: Discovering: [redacted]

Nodes Discovered: 11

Subnets Discovered: 0

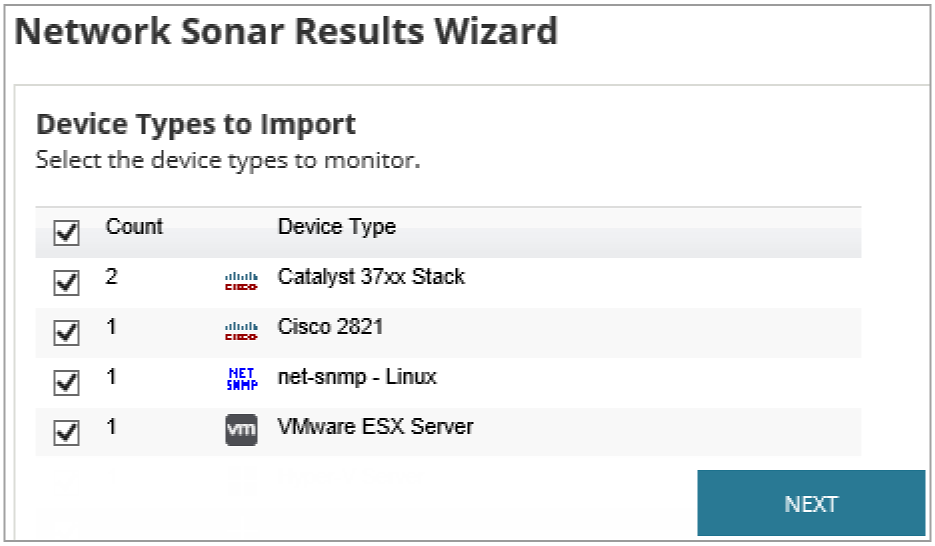
Add discovered devices to NPM

After you have discovered your network with the Network Sonar wizard, select network elements to import to the SolarWinds Platform database in the Network Sonar Results wizard. Discovered elements do not count against your license count; only elements that you import into the Orion database count against your license.

When you manually run discovery, by default, the system automatically selects all network elements to be monitored. 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. Ensure that only the device types you want to monitor are selected, and click Next.



Network Sonar Results Wizard

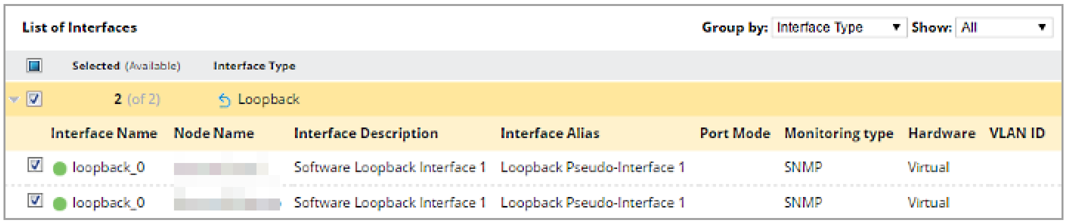
Device Types to Import

Select the device types to monitor.

☑	Count		Device Type
☑	2	CISCO	Catalyst 37xx Stack
☑	1	CISCO	Cisco 2821
☑	1	NET SNMP	net-snmp - Linux
☑	1	vm	VMware ESX Server

2. 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

Group by: Interface Type ▾ Show: All ▾

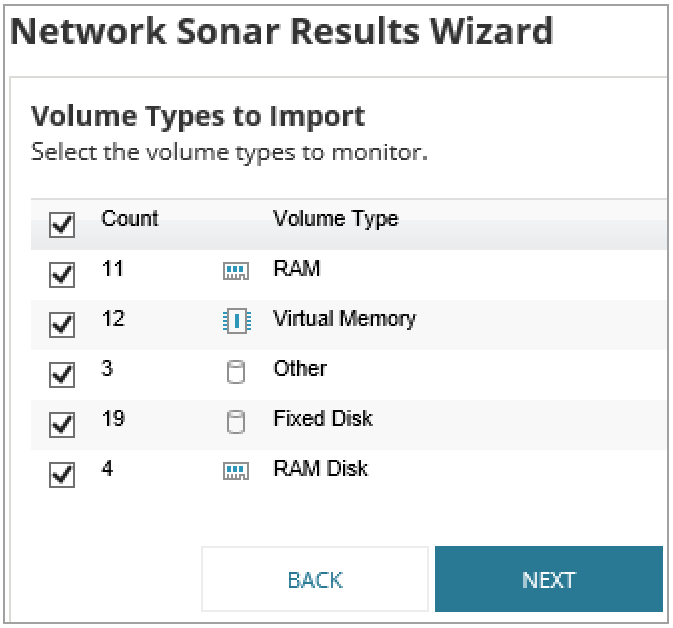
■	Selected (Available)	Interface Type
☑	2 (of 2)	Loopback

	Interface Name	Node Name	Interface Description	Interface Alias	Port Mode	Monitoring type	Hardware	VLAN ID
☑	● loopback_0	[redacted]	Software Loopback Interface 1	Loopback Pseudo-Interface 1		SNMP	Virtual	
☑	● loopback_0	[redacted]	Software Loopback Interface 1	Loopback Pseudo-Interface 1		SNMP	Virtual	

> By default, SolarWinds Platform imports interfaces discovered in an Operationally Up state. Interfaces may cycle off and on, and so you can also select Operationally Down or Administratively Shutdown states for import.

3. Ensure the volume types to monitor are selected, and click Next.

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



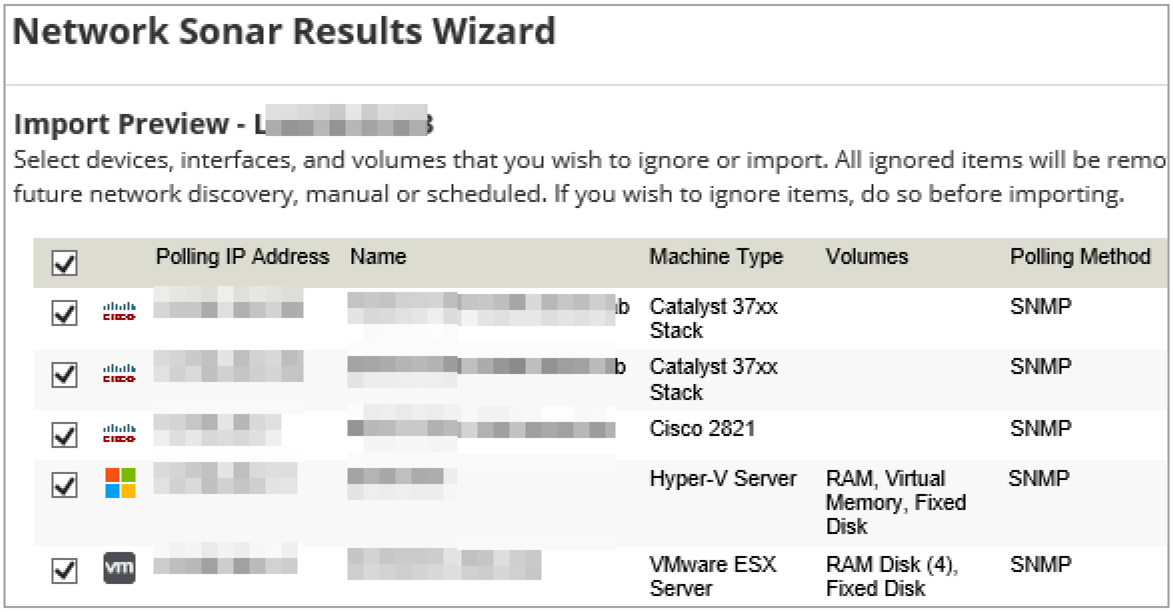
Network Sonar Results Wizard

Volume Types to Import

Select the volume types to monitor.

☑	Count		Volume Type
☑	11		RAM
☑	12		Virtual Memory
☑	3		Other
☑	19		Fixed Disk
☑	4		RAM Disk

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



Network Sonar Results Wizard

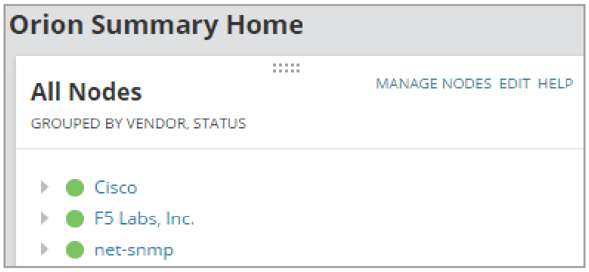
Import Preview - L[redacted]

Select devices, interfaces, and volumes that you wish to ignore or import. All ignored items will be remo future network discovery, manual or scheduled. If you wish to ignore items, do so before importing.

☑		Polling IP Address	Name	Machine Type	Volumes	Polling Method
☑	CISCO	[redacted]	[redacted]b	Catalyst 37xx Stack		SNMP
☑	CISCO	[redacted]	[redacted]b	Catalyst 37xx Stack		SNMP
☑	CISCO	[redacted]	[redacted]	Cisco 2821		SNMP
☑		[redacted]	[redacted]	Hyper-V Server	RAM, Virtual Memory, Fixed Disk	SNMP
☑	vm	[redacted]	[redacted]	VMware ESX Server	RAM Disk (4), Fixed Disk	SNMP

5. When the import completes, click Finish.

6. Click the Home tab to begin exploring your network.



Orion Summary Home

All Nodes

GROUPED BY VENDOR, STATUS

- ● Cisco
- ● F5 Labs, Inc.
- ● net-snmp

ⓘ If the status of a node is Unknown after discovery, you may need to check a few settings in NPM. See Troubleshoot Unknown Nodes for more information.

When you finish the initial discovery and import, consider adding discoveries for other segments of your IT environment.

Plan to scale network monitoring

You installed and configured your NPM, discovered part of your IT environment, and have monitoring statistics displayed in SolarWinds Platform Web Console views. As you continue the deployment, consider the following questions:

- Are there any gaps in your monitoring coverage?
- Is there an essential device whose failure could affect your environment?
- Are there less important devices or applications that you want to monitor?
- Are there other groups or locations that you might want to monitor?

As you deploy monitoring across your environment, you can:

- Add discoveries to include other segments of your IT environment.
- Add individual nodes for monitoring. This is the recommended approach when you have a node with high latency.

Add a single node for monitoring

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 recommended for nodes 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.
- Specify how often the node status, monitored statistics, or topology details are updated.
- Add custom properties.
- Edit alert thresholds.

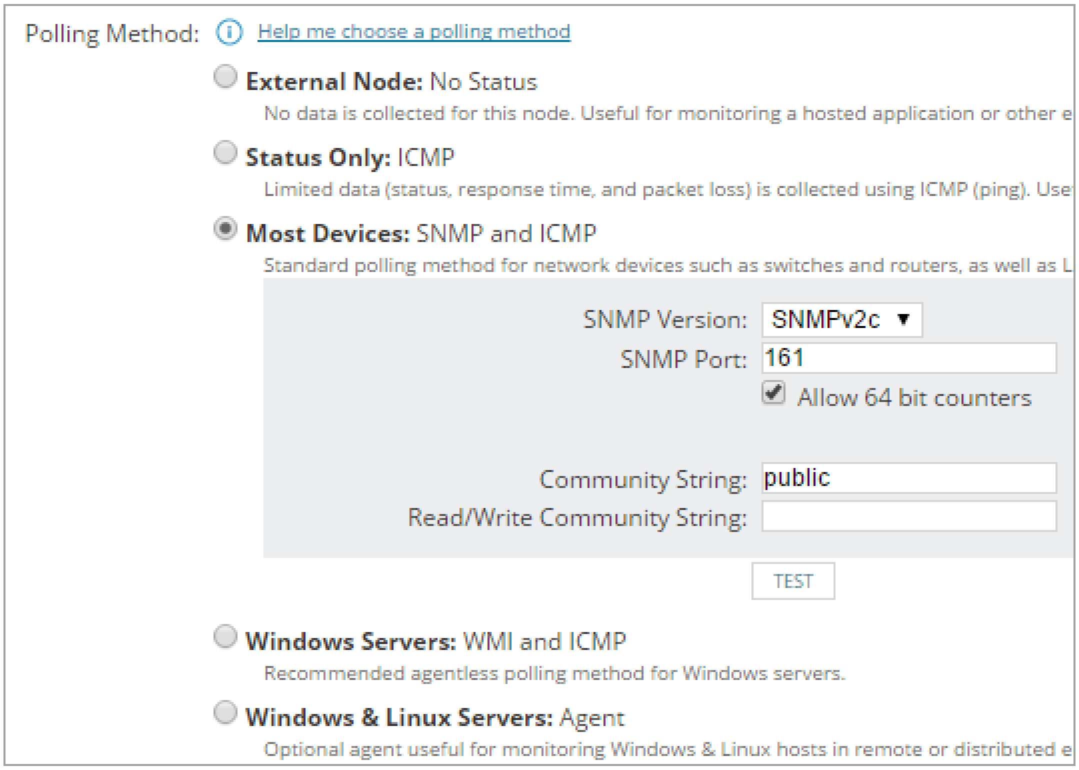
To add a single node for monitoring:

1. Log in to the SolarWinds Platform Web Console as 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.



Polling Method: Help me choose a polling method

○ **External Node:** No Status
No data is collected for this node. Useful for monitoring a hosted application or other e

○ **Status Only:** ICMP
Limited data (status, response time, and packet loss) is collected using ICMP (ping). Use

● **Most Devices:** SNMP and ICMP
Standard polling method for network devices such as switches and routers, as well as L

SNMP Version: SNMPv2c ▼
SNMP Port: 161
☑ Allow 64 bit counters

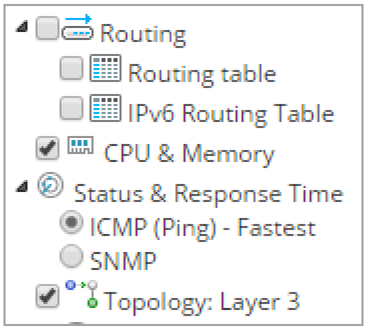
Community String: public
Read/Write Community String:

TEST

○ **Windows Servers:** WMI and ICMP
Recommended agentless polling method for Windows servers.

○ **Windows & Linux Servers:** Agent
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.



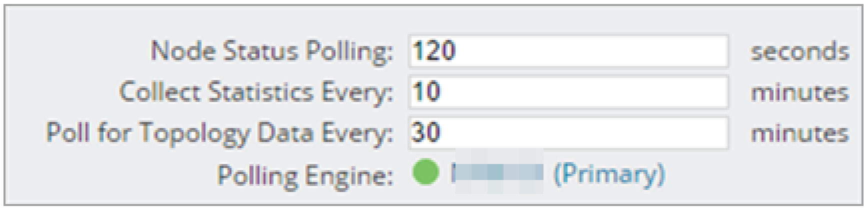
- ☐ Routing
  - ☐ Routing table
  - ☐ IPv6 Routing Table
- ☑ CPU & Memory
- Status & Response Time
  - ● ICMP (Ping) - Fastest
  - ○ SNMP
- ☑ Topology: Layer 3

5. If you have defined a custom poller and want to monitor the metric on the node, 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.



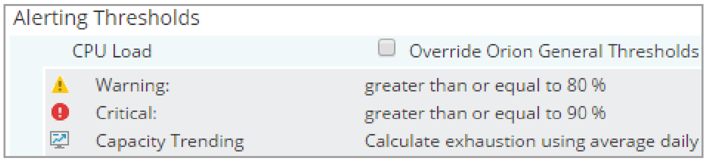
Node Status Polling:	120	seconds
Collect Statistics Every:	10	minutes
Poll for Topology Data Every:	30	minutes
Polling Engine:	● [redacted] (Primary)	

> 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 is 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.



Alerting Thresholds

CPU Load	□ Override Orion General Thresholds
⚠ Warning:	greater than or equal to 80 %
❗ Critical:	greater than or equal to 90 %
Capacity Trending	Calculate exhaustion using average daily

7. Click OK, Add Node.

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

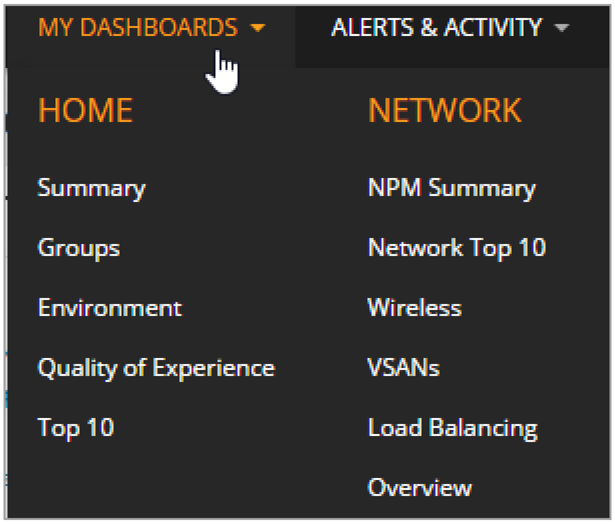
Navigate NPM

After you have installed and configured NPM and specified the devices to monitor, you need to wait a few minutes for the SolarWinds Platform to collect data from the devices.

In the meantime, see the following terms that might be helpful when you explore NPM:

- SolarWinds Platform The common backend platform used by the SolarWinds Platform suite of products, including NPM, SAM, NCM, NTA, and more. The platform provides the backbone for navigation, settings, and common features like alerts and reports. It also provides a consistent look-and-feel across products, giving you a “single pane of glass” for your monitoring tools.
- **SolarWinds Platform Web Console:** The web interface you see when you log in to the SolarWinds Platform. It is used to view, configure, and manage all of your monitored objects. You can access the SolarWinds Platform Web Console from any computer connected to the Internet.
- **View:** An individual page in the web console.
- **Widget:** The informational blocks that make up a view.
- **Entity:** Anything that can be monitored by the SolarWinds Platform.

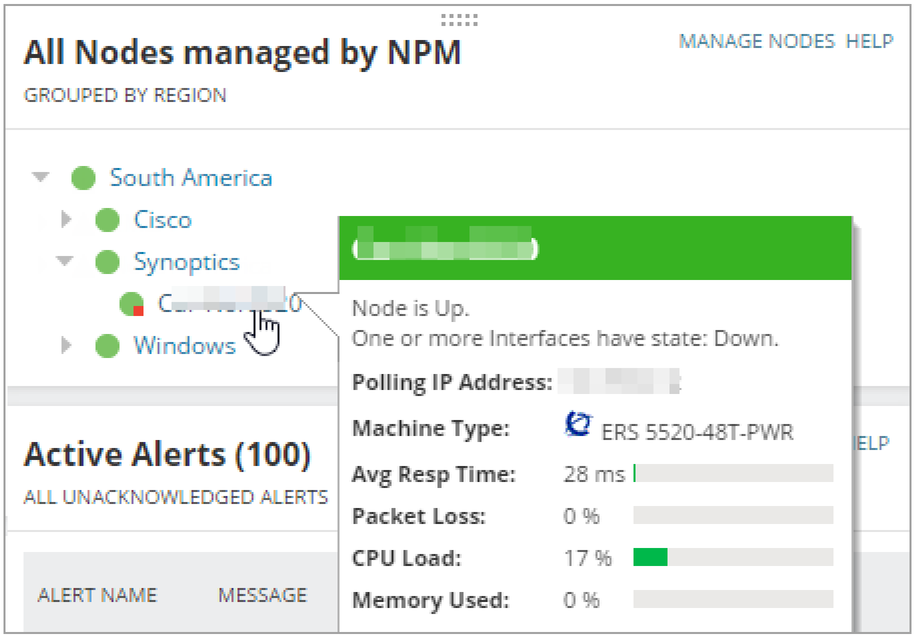
When you first log in, The Orion Summary Home view is displayed by default. The My Dashboards menu includes a submenu for each Orion module. If you have installed only NPM, this menu includes a Home submenu and a Network submenu.



Overview of an entity

Within a view, entities that appear in green are up and working as expected. Entities that appear red or partially red need attention. In this example, all nodes are up, but node Cur-Nor5520 has an issue as indicated by the red square next to the node name. The red square indicates that the system is monitoring a child of that node, for example, an interface.

To explore a node, place your cursor over the entity to see more details. In this example, one or more interfaces are down. Click the node to drill down to the node details page.



All Nodes managed by NPM

MANAGE NODES HELP

GROUPED BY REGION

- South America
  - Cisco
  - Synoptics
    - Cu[redacted]0
  - Windows

[redacted]

Node is Up.
One or more Interfaces have state: Down.

Polling IP Address: [redacted]

Machine Type: ERS 5520-48T-PWR

Avg Resp Time: 28 ms

Packet Loss: 0 %

CPU Load: 17 %

Memory Used: 0 %

Active Alerts (100)

ALL UNACKNOWLEDGED ALERTS

ELP

ALERT NAME	MESSAGE

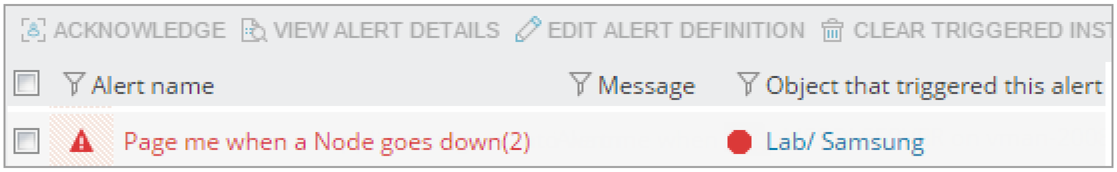
Identify and troubleshoot a node that has a problem

ⓘ By default, devices monitored by NPM are polled for data every nine minutes. It might take some time before all the nodes you added have data you can review.

Step 1: Determine there is a problem

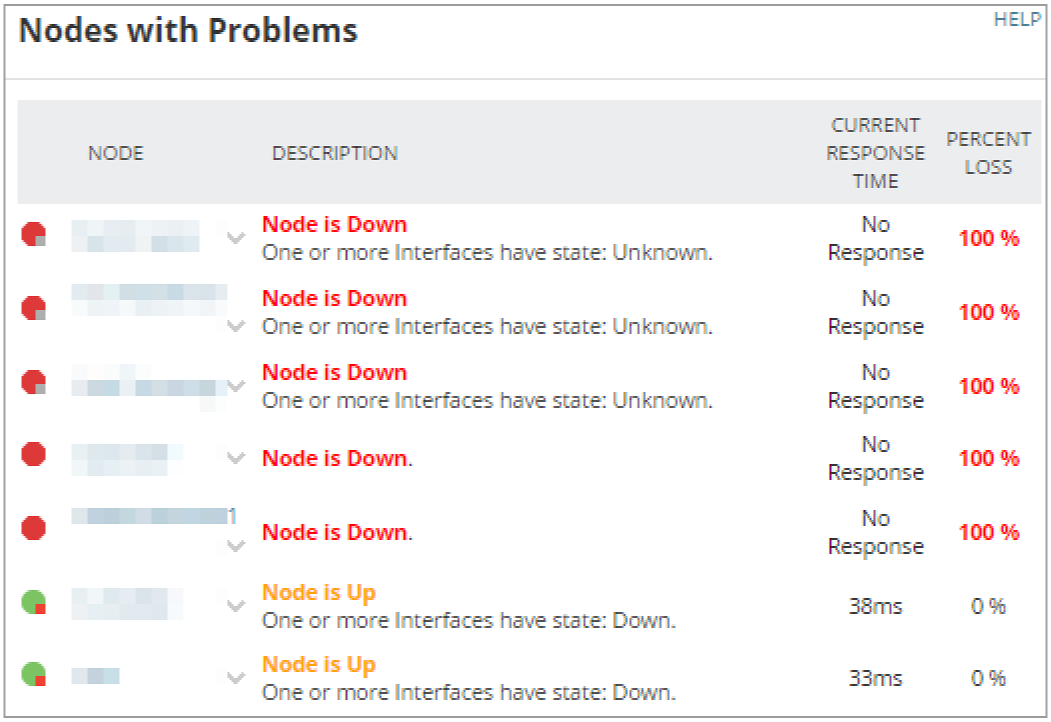
The easiest way to identify a problem is to have an alert notify you.

Some alerts are enabled by default, such as the Node Down alert. Therefore, if a node goes down (that is, it does not respond to a ping), you will see it immediately in the Active Alerts widget on the Home page.



□	Alert name	Message	Object that triggered this alert
□	⚠ Page me when a Node goes down(2)		● Lab/ Samsung

Down nodes appear in widgets as red (down) or yellow (warning).

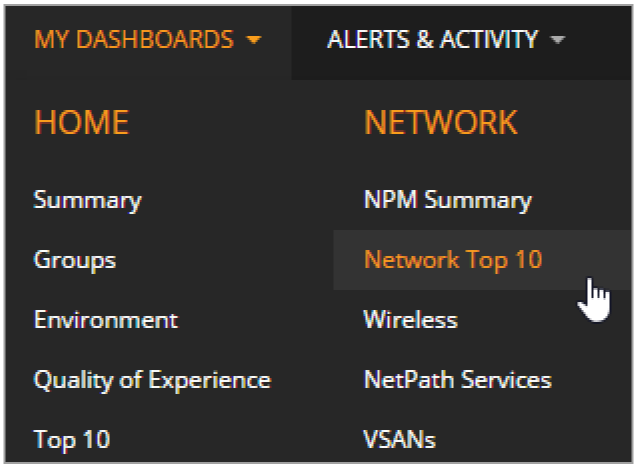


Nodes with Problems

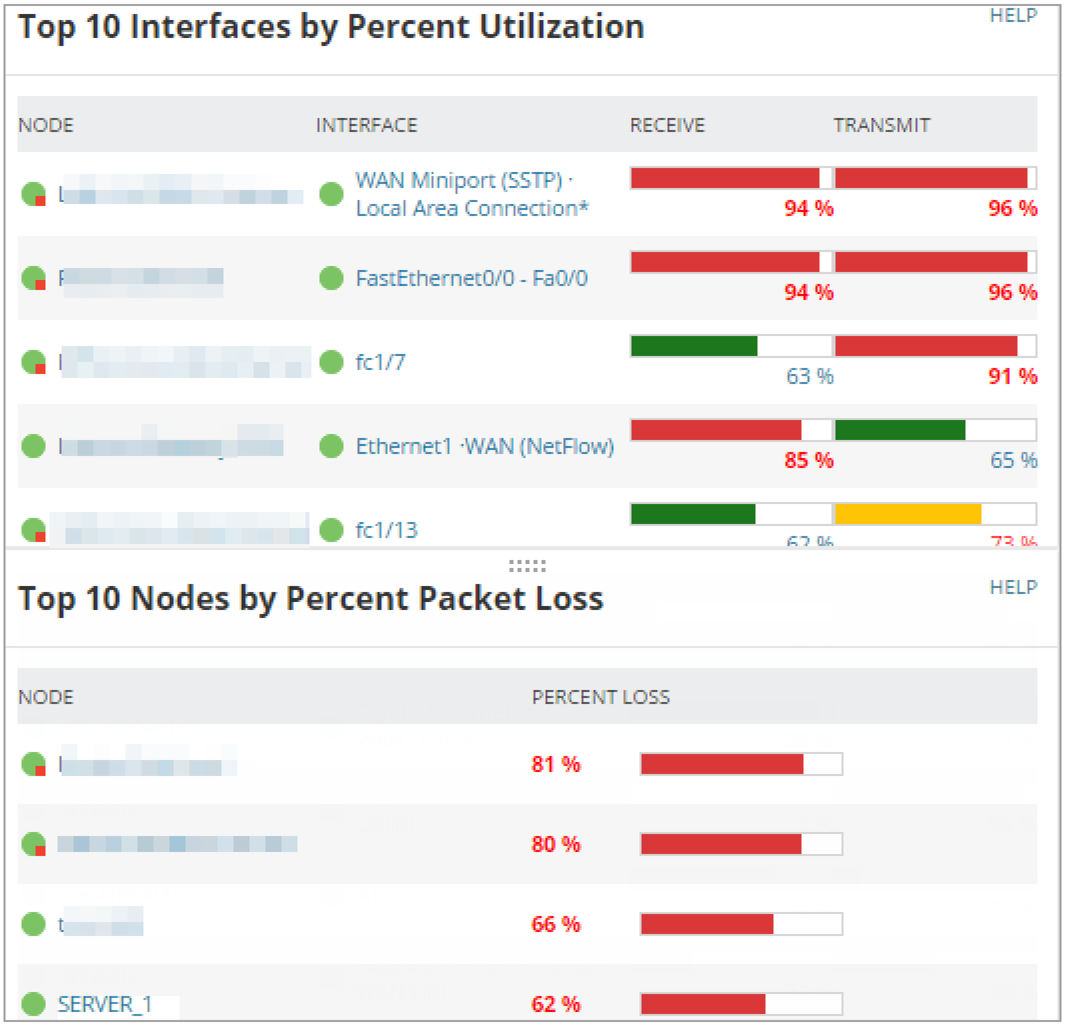
	NODE	DESCRIPTION	CURRENT RESPONSE TIME	PERCENT LOSS
●	[redacted]	Node is Down One or more Interfaces have state: Unknown.	No Response	100 %
●	[redacted]	Node is Down One or more Interfaces have state: Unknown.	No Response	100 %
●	[redacted]	Node is Down One or more Interfaces have state: Unknown.	No Response	100 %
●	[redacted]	Node is Down.	No Response	100 %
●	[redacted]	Node is Down.	No Response	100 %
●	[redacted]	Node is Up One or more Interfaces have state: Down.	38ms	0 %
●	[redacted]	Node is Up One or more Interfaces have state: Down.	33ms	0 %

If you have configured your alerts to send email, you get an email when a node goes down.

If you do not see any alerts, click My Dashboards > Network > Network Top 10.



The widgets on this page help identify nodes that respond to a ping but have other health problems.



Top 10 Interfaces by Percent Utilization

HELP

NODE	INTERFACE	RECEIVE	TRANSMIT
[redacted]	WAN Miniport (SSTP) · Local Area Connection*	94 %	96 %
[redacted]	FastEthernet0/0 - Fa0/0	94 %	96 %
[redacted]	fc1/7	63 %	91 %
[redacted]	Ethernet1 ·WAN (NetFlow)	85 %	65 %
[redacted]	fc1/13	62 %	73 %

Top 10 Nodes by Percent Packet Loss

HELP

NODE	PERCENT LOSS
[redacted]	81 %
[redacted]	80 %
[redacted]	66 %
SERVER_1	62 %

Step 2: Get more details about the node

When you find a node with a problem, click the node name in any widget to open the Node Details page.

If a node is down (red), this means it does not respond to a ping. To resolve an issue of this severity:

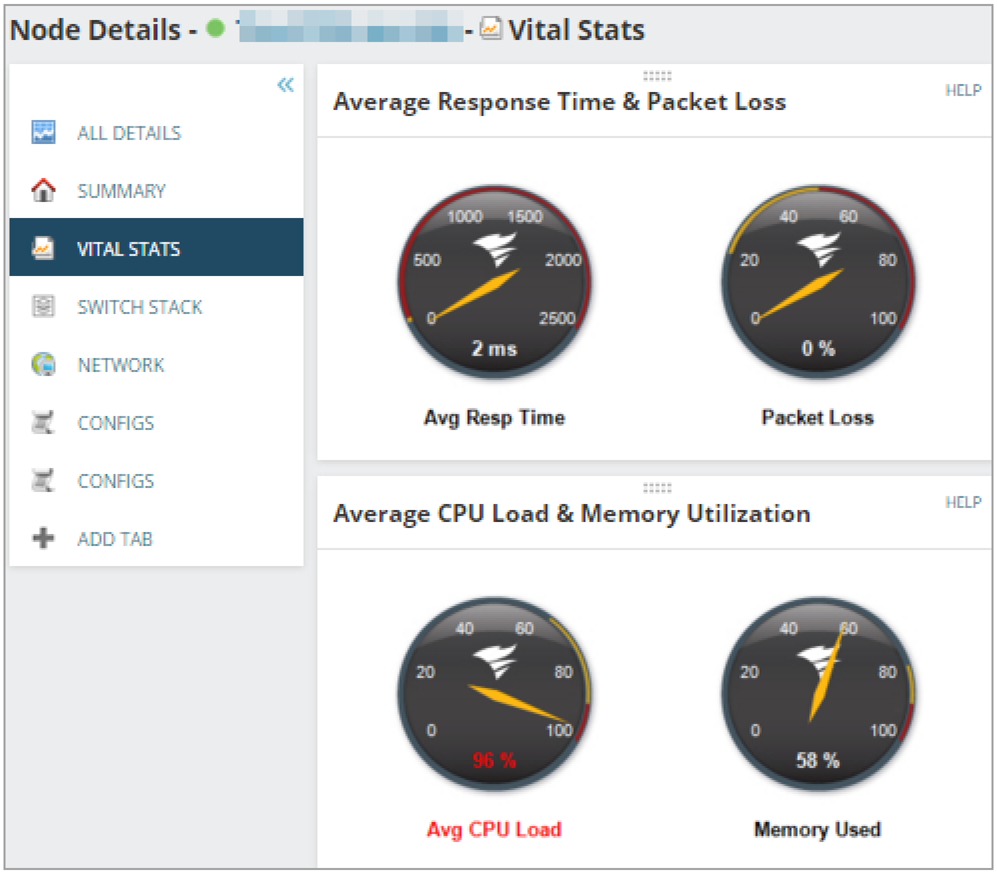
1. Check the power. Is it plugged in?

2. Check the LAN link light. Is it connected to the network?

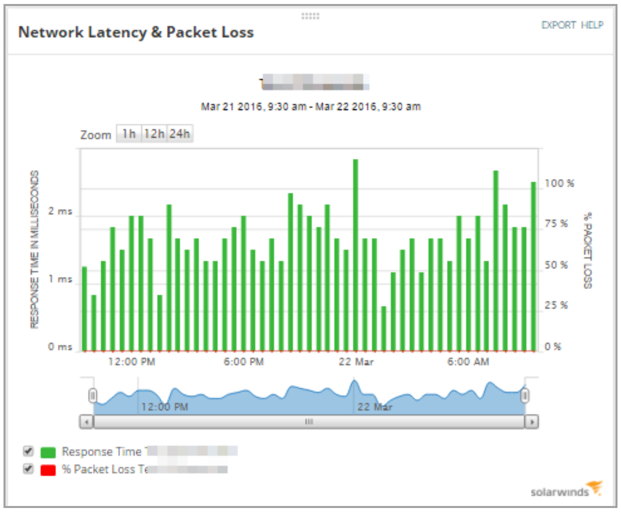
3. Log in to the device and begin troubleshooting it.

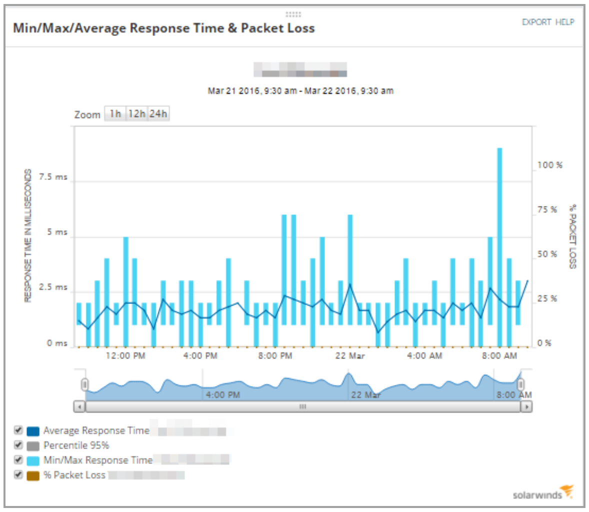
   If a node responds to a ping but shows signs of health or performance issues, use the information on the Node Details page to help troubleshoot.

   - Check the Response Time, Packet Loss, CPU load, and Memory Utilization widgets. Usually, those statistics are the first indicators of a problem. In our example, the CPU load on this node is high.



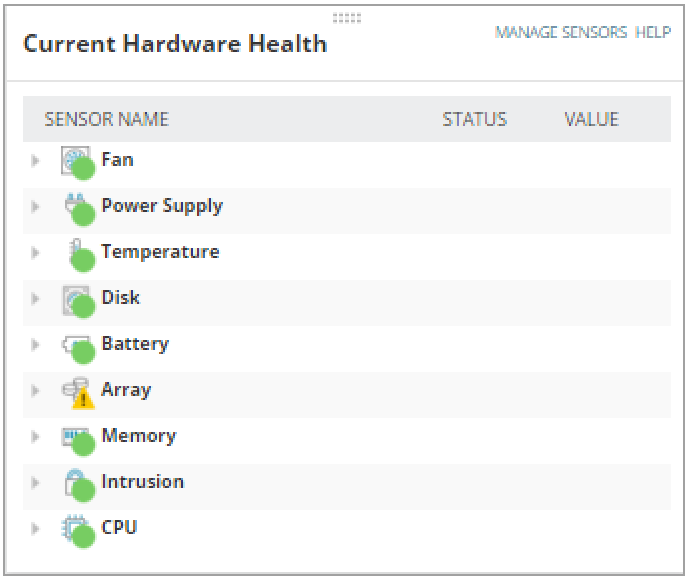
- Use the Network Latency & Packet Loss, as well as the Min/Max/Average Response Time charts, to see if this is a momentary problem or a continuing issue.





- Depending on what type of node you are monitoring, you may see additional widgets specific to that type of device. For example:

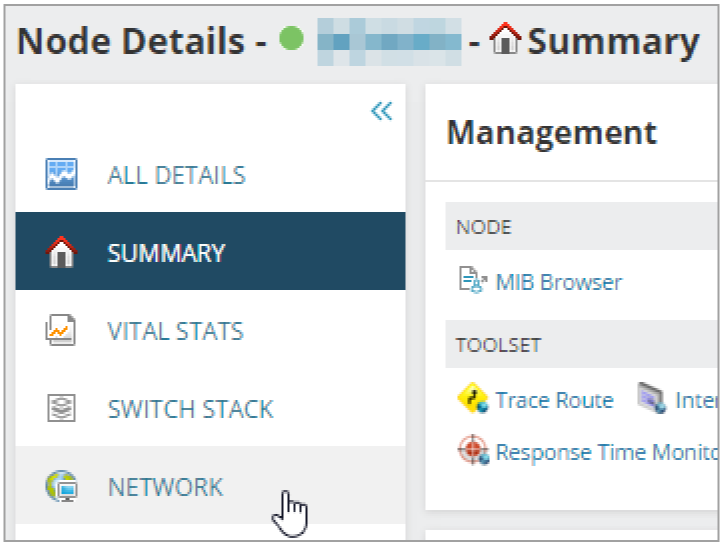
  Hardware health: Reports on physical elements of the hardware for Cisco, Dell, F5, HP, and Juniper.

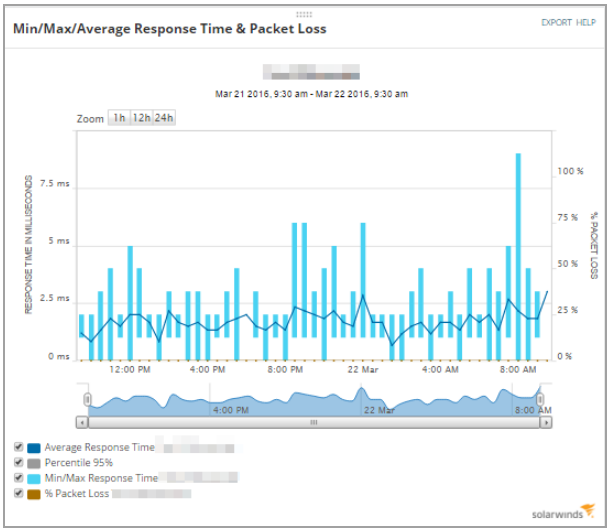


Current Hardware Health

SENSOR NAME	STATUS	VALUE
Fan		
Power Supply		
Temperature		
Disk		
Battery		
Array		
Memory		
Intrusion		
CPU		

Routing table information: For routers and switches, multiple widgets show a variety of route-related information. Look under the Network subview for routing widgets, such as Routing Neighbors, Routing Table, or Default Route Changes.





Step 3: Get more details about the alert

When a problem causes an alert to be triggered, that alert appears on the Node Details page in the Alerts for this Node widget. Click the alert name to go to the Alert Details page. Use the widgets on this page to investigate the cause of the alert.

Identify and troubleshoot an interface that has a problem

ⓘ By default, devices monitored by NPM are polled for data every nine minutes. It might take some time before all the nodes you added have data you can review.

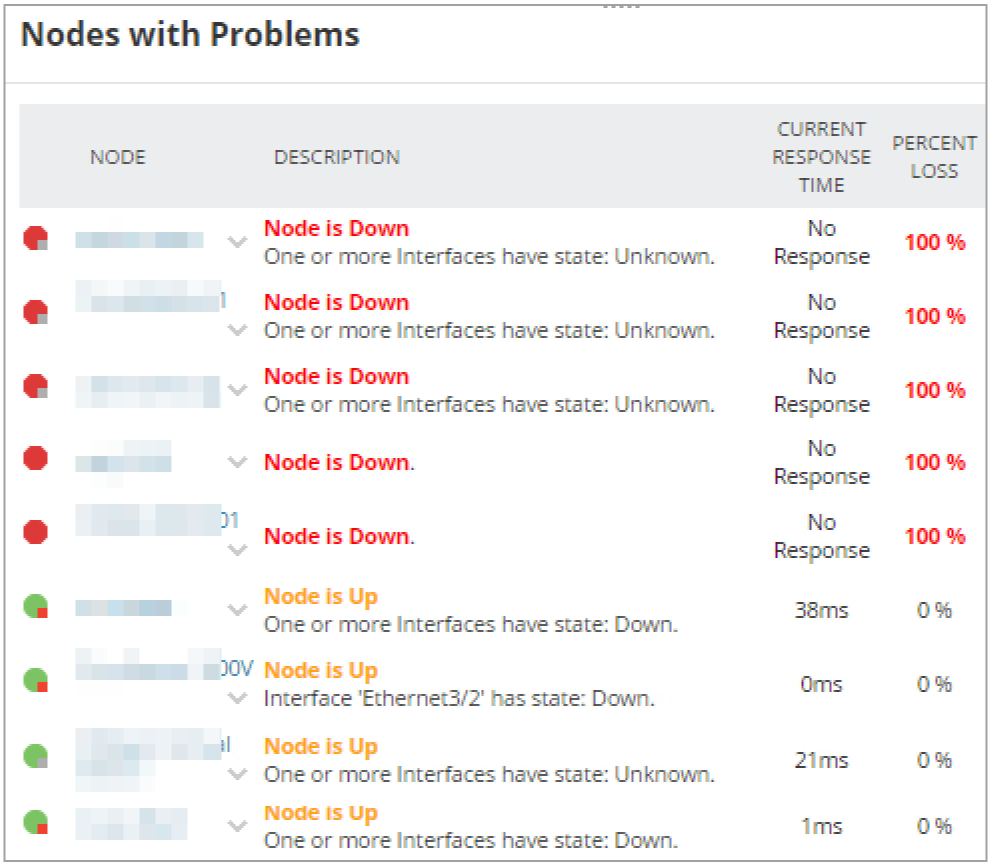
Step 1: Determine there is a problem

In the topic Identify and troubleshoot a node that has a problem, alerts are triggered when a node goes down. Alerts can also be triggered when an interface has a problem, such as high utilization or the interface going down.

The Nodes with Problems widget provides information about the interfaces associated with each node. A square in the bottom-right corner of the node icon indicates that the node has an interface with a problem:

● - In this example, a red square indicates that one or more interfaces are down.

● - In this example, a gray square indicates that the status of one or more interfaces is unknown.



Nodes with Problems

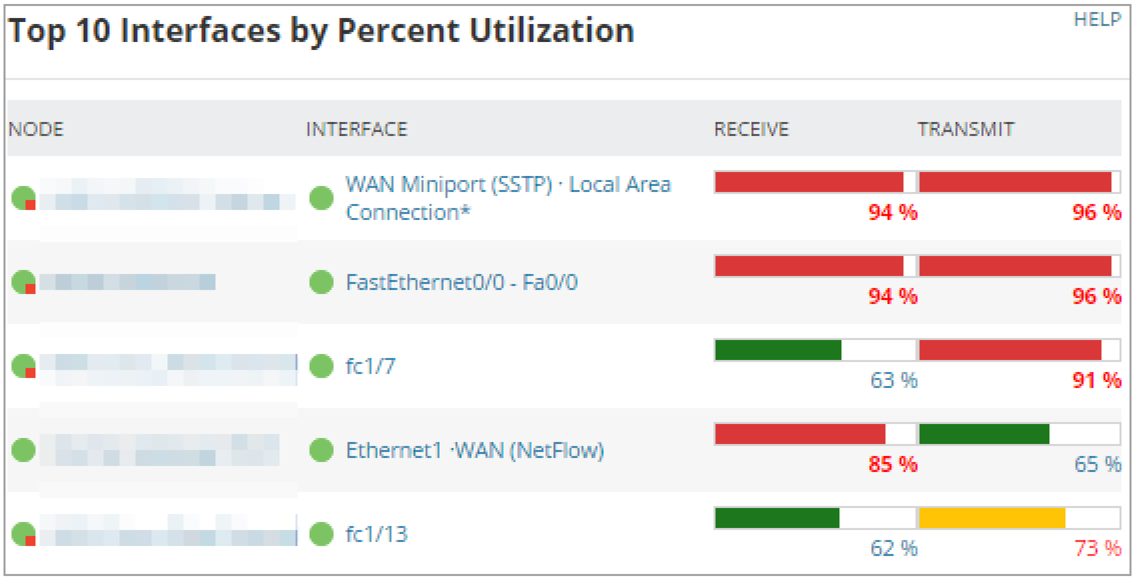
	NODE	DESCRIPTION	CURRENT RESPONSE TIME	PERCENT LOSS
●	[redacted]	Node is Down One or more Interfaces have state: Unknown.	No Response	100 %
●	[redacted]	Node is Down One or more Interfaces have state: Unknown.	No Response	100 %
●	[redacted]	Node is Down One or more Interfaces have state: Unknown.	No Response	100 %
●	[redacted]	Node is Down.	No Response	100 %
●	[redacted]	Node is Down.	No Response	100 %
●	[redacted]	Node is Up One or more Interfaces have state: Down.	38ms	0 %
●	[redacted]	Node is Up Interface 'Ethernet3/2' has state: Down.	0ms	0 %
●	[redacted]	Node is Up One or more Interfaces have state: Unknown.	21ms	0 %
●	[redacted]	Node is Up One or more Interfaces have state: Down.	1ms	0 %

In your environment, you might not have any down interfaces. To find an interface with issues that need to be investigated, click My Dashboards > Network > Network Top 10 to open the Network Top 10 view. Review the following widgets on this page.

Top 10 Interfaces by Percent Utilization

This widget shows the interface's transmit and receive utilization as a percent of total interface speed. By default, utilization rates from 70 - 90% are yellow (warning), and utilization over 90% is red (danger). These thresholds are configurable.

Any interface with high utilization deserves more investigation.

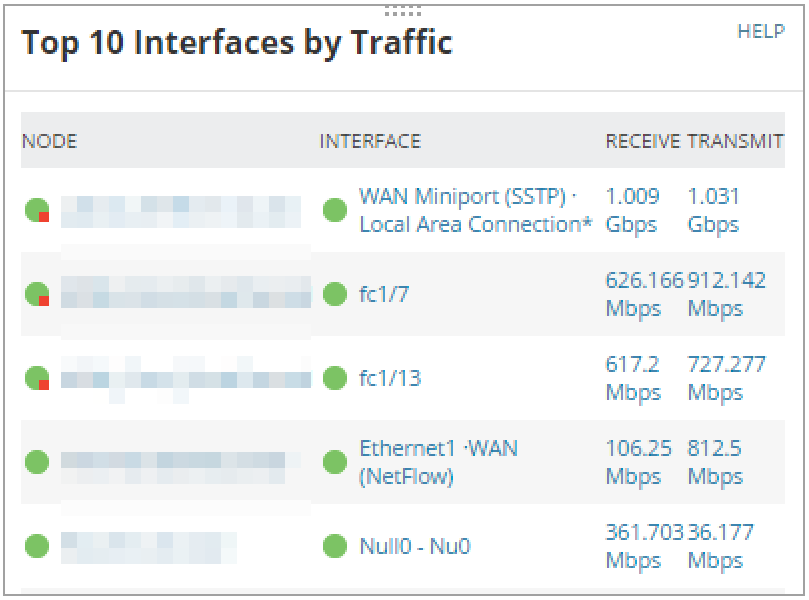


Top 10 Interfaces by Percent Utilization

NODE	INTERFACE	RECEIVE	TRANSMIT
[redacted]	WAN Miniport (SSTP) - Local Area Connection*	94 %	96 %
[redacted]	FastEthernet0/0 - Fa0/0	94 %	96 %
[redacted]	fc1/7	63 %	91 %
[redacted]	Ethernet1 -WAN (NetFlow)	85 %	65 %
[redacted]	fc1/13	62 %	73 %

Top 10 Interfaces by Traffic

This widget shows how much actual traffic is on an interface. Usually, WAN interfaces will be on this list because of the volume of traffic they process.



Top 10 Interfaces by Traffic

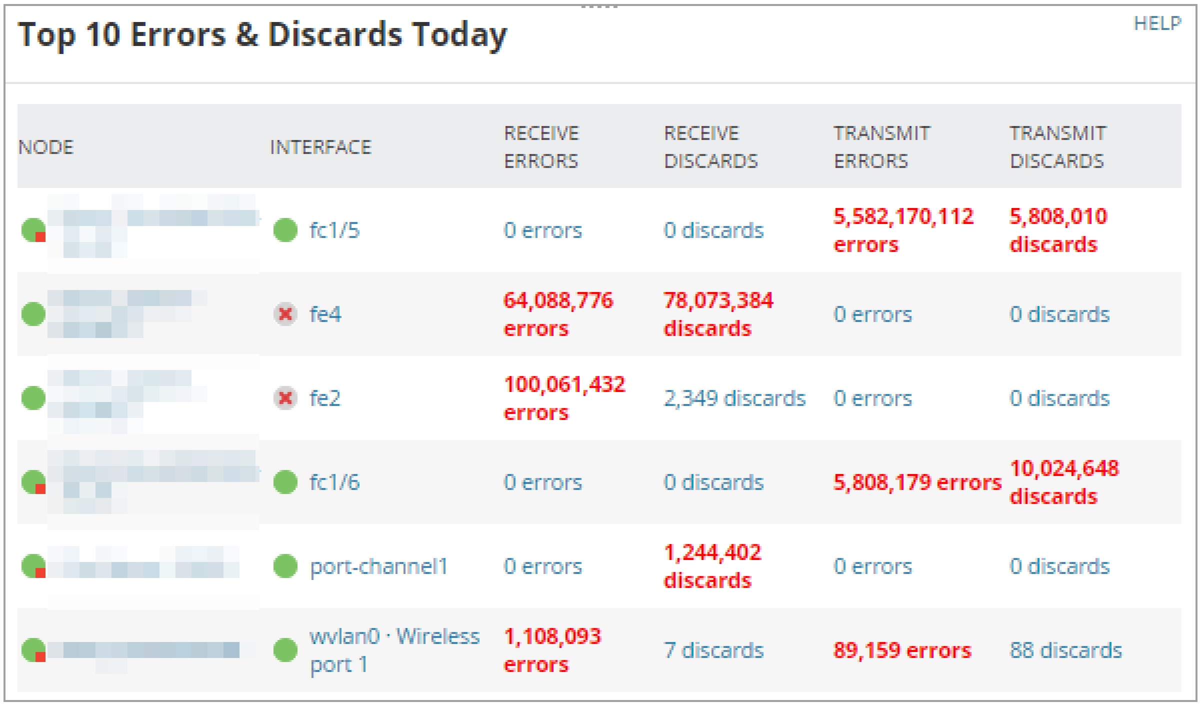
NODE	INTERFACE	RECEIVE	TRANSMIT
[redacted]	WAN Miniport (SSTP) · Local Area Connection*	1.009 Gbps	1.031 Gbps
[redacted]	fc1/7	626.166 Mbps	912.142 Mbps
[redacted]	fc1/13	617.2 Mbps	727.277 Mbps
[redacted]	Ethernet1 ·WAN (NetFlow)	106.25 Mbps	812.5 Mbps
[redacted]	Null0 - Nu0	361.703 Mbps	36.177 Mbps

Top 10 Errors & Discards Today

This widget shows:

- Errors: A packet that was received but could not be processed because there was a problem with the packet.

- Discards: A packet that was received without errors but was dropped, usually because interface utilization is near 100%.



Top 10 Errors & Discards Today

NODE	INTERFACE	RECEIVE ERRORS	RECEIVE DISCARDS	TRANSMIT ERRORS	TRANSMIT DISCARDS
● [redacted]	● fc1/5	0 errors	0 discards	5,582,170,112 errors	5,808,010 discards
● [redacted]	✖ fe4	64,088,776 errors	78,073,384 discards	0 errors	0 discards
● [redacted]	✖ fe2	100,061,432 errors	2,349 discards	0 errors	0 discards
● [redacted]	● fc1/6	0 errors	0 discards	5,808,179 errors	10,024,648 discards
● [redacted]	● port-channel1	0 errors	1,244,402 discards	0 errors	0 discards
● [redacted]	● wvlan0 · Wireless port 1	1,108,093 errors	7 discards	89,159 errors	88 discards

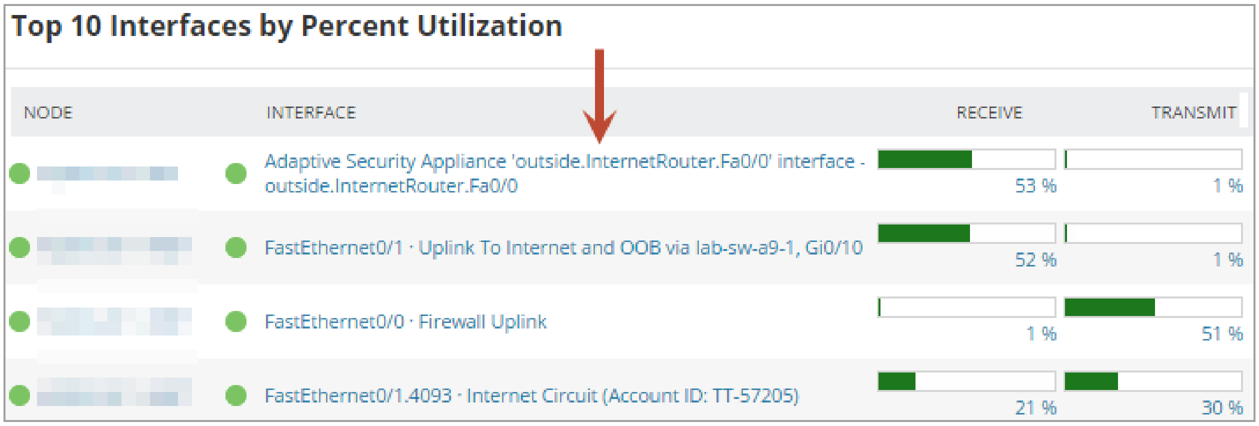
Step 2: Get more details about the interface

If an interface is down (red), that generally means there is no connection:

1. Check the parent device to ensure it is operating.
2. Check the cable for physical connectivity problems.

When you have found an interface with a problem (or, if all your interfaces are healthy, an interface with high utilization, errors, or discards), troubleshoot the issue:

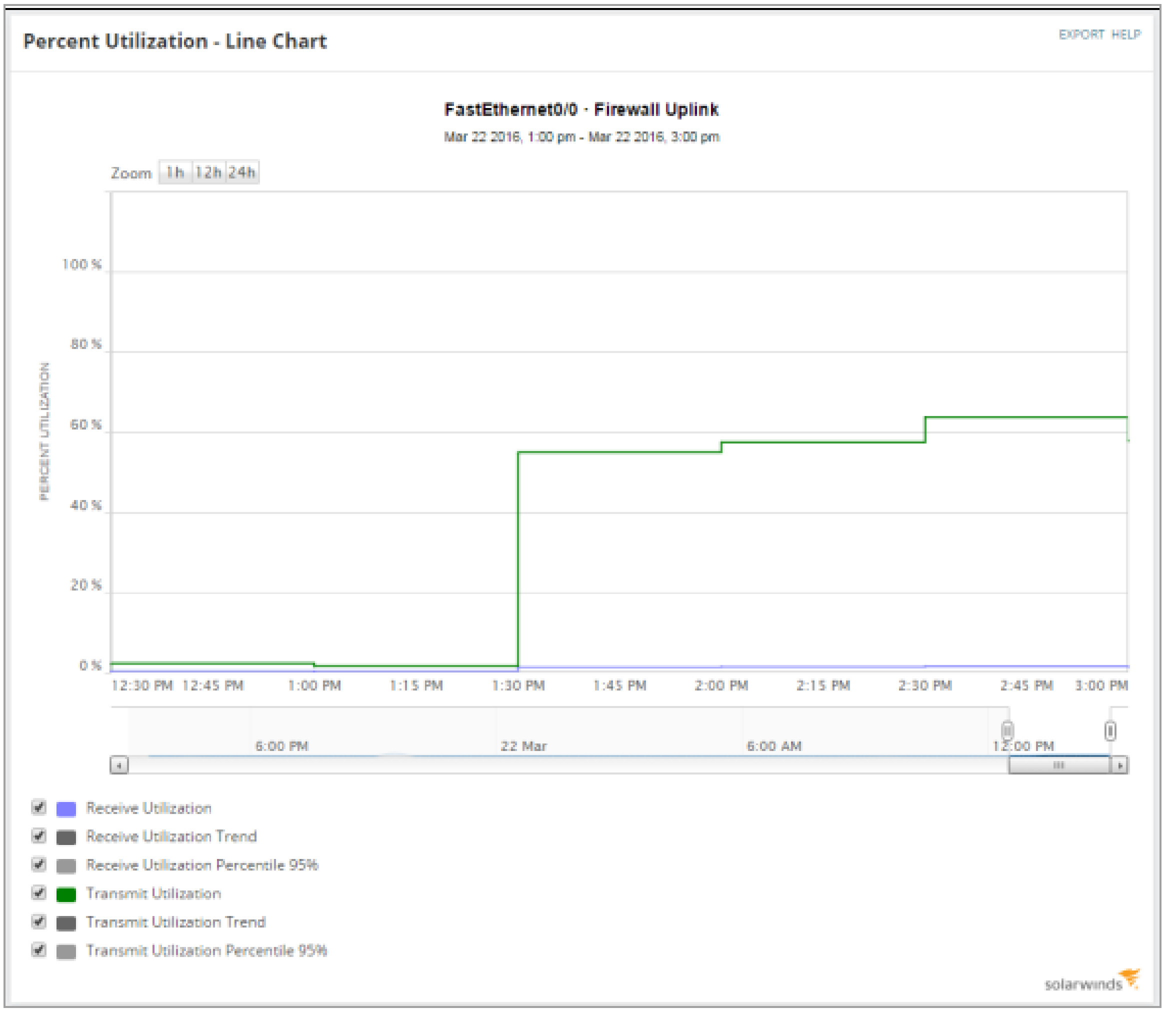
- Click the interface name in any widget. The Interface Details page opens.



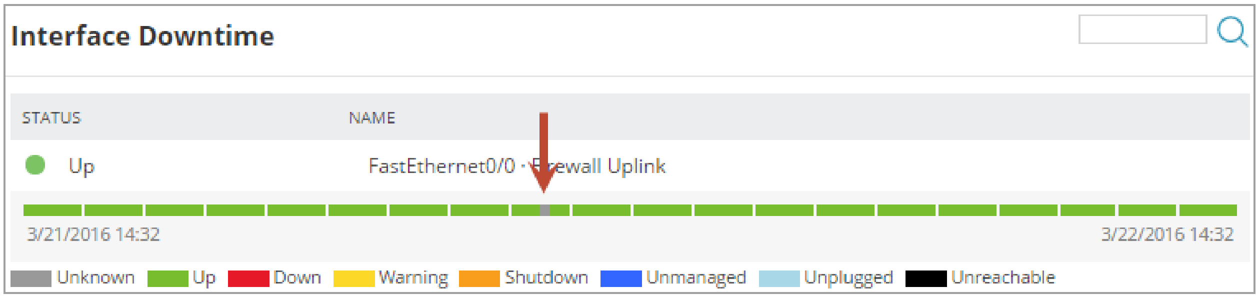
Top 10 Interfaces by Percent Utilization

NODE	INTERFACE	RECEIVE	TRANSMIT
● [redacted]	● Adaptive Security Appliance 'outside.InternetRouter.Fa0/0' interface - outside.InternetRouter.Fa0/0	53 %	1 %
● [redacted]	● FastEthernet0/1 · Uplink To Internet and OOB via lab-sw-a9-1, Gi0/10	52 %	1 %
● [redacted]	● FastEthernet0/0 · Firewall Uplink	1 %	51 %
● [redacted]	● FastEthernet0/1.4093 · Internet Circuit (Account ID: TT-57205)	21 %	30 %

- Check the Percent Utilization widget for the last-polled value of transmit and receive utilization. If those values are high, you can also check the Percent Utilization – Line Chart to see the duration of the problem.



- The Interface Downtime widget displays the interface status for the last 24 hours. If the interface status changed, you can see it in this widget. In the following example, the interface had one period when its status was unknown during the last 24 hours, but it is currently up.



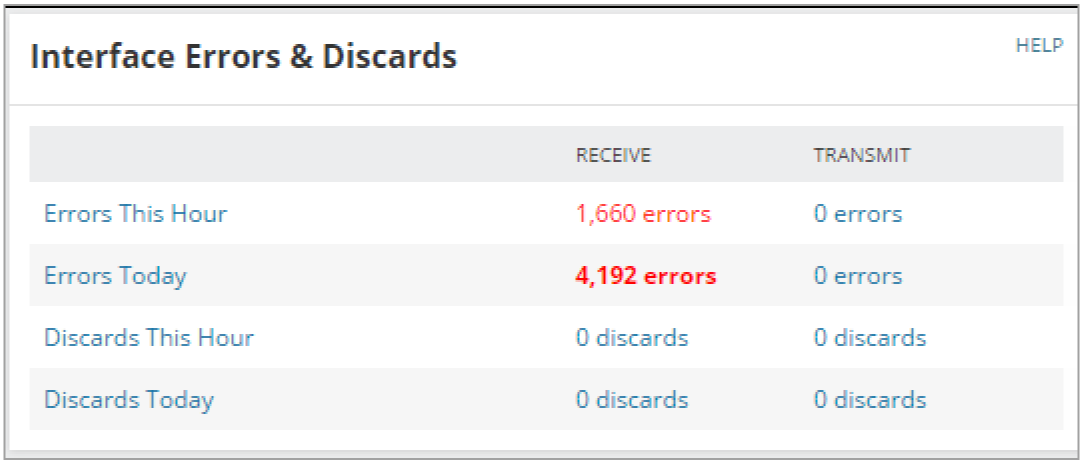
Interface Downtime

STATUS	NAME
● Up	FastEthernet0/0 · Firewall Uplink

3/21/2016 14:32 3/22/2016 14:32

▨ Unknown 🟩 Up 🟥 Down 🟨 Warning 🟧 Shutdown 🟦 Unmanaged ▨ Unplugged ■ Unreachable

- The Interface Errors & Discards widget can also indicate problems. Since this device has high discards, and high discards are generally caused by a full buffer, check the Node Details for this device and determine if the buffer is full.

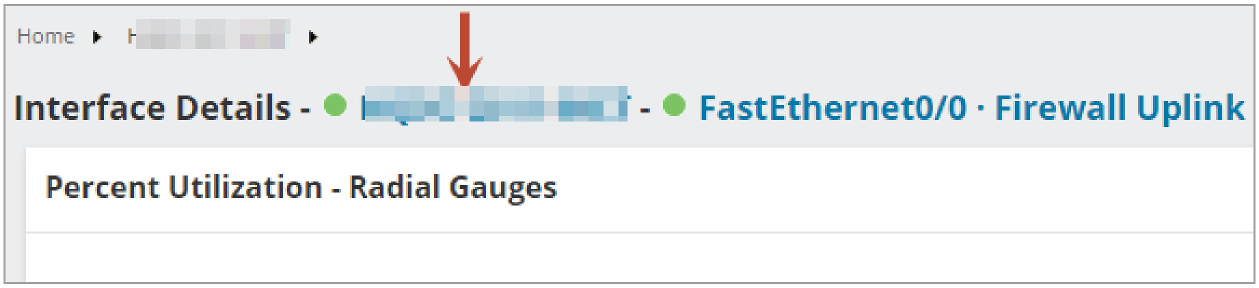


Interface Errors & Discards

	RECEIVE	TRANSMIT
Errors This Hour	1,660 errors	0 errors
Errors Today	**4,192 errors**	0 errors
Discards This Hour	0 discards	0 discards
Discards Today	0 discards	0 discards

Step 3: Get more details about the problem

The Node Details page can help you diagnose an interface problem. Click the node name at the top of the Interface Details page to open the Node Details page.



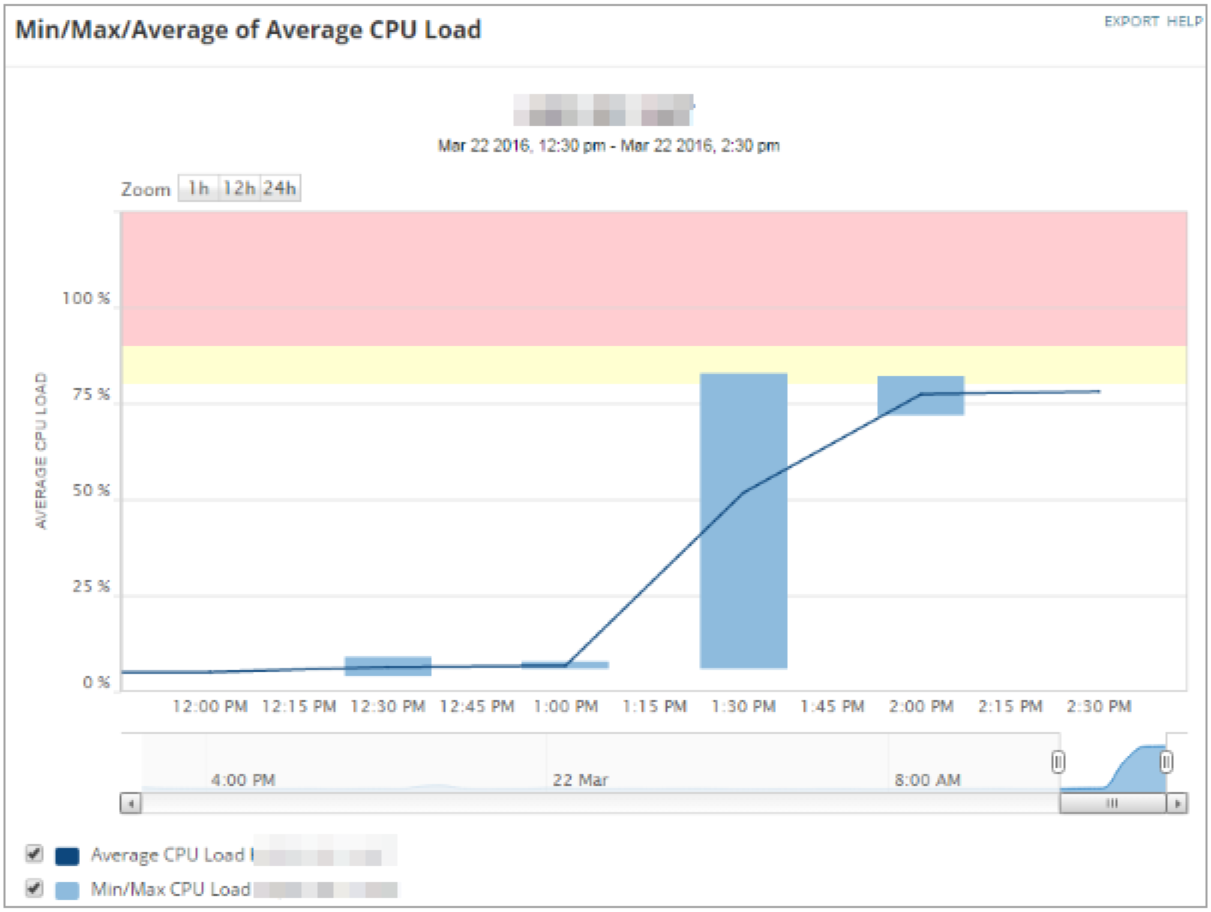
Interface Details - ● [redacted] - ● FastEthernet0/0 · Firewall Uplink

Percent Utilization - Radial Gauges

Examine the following widgets.

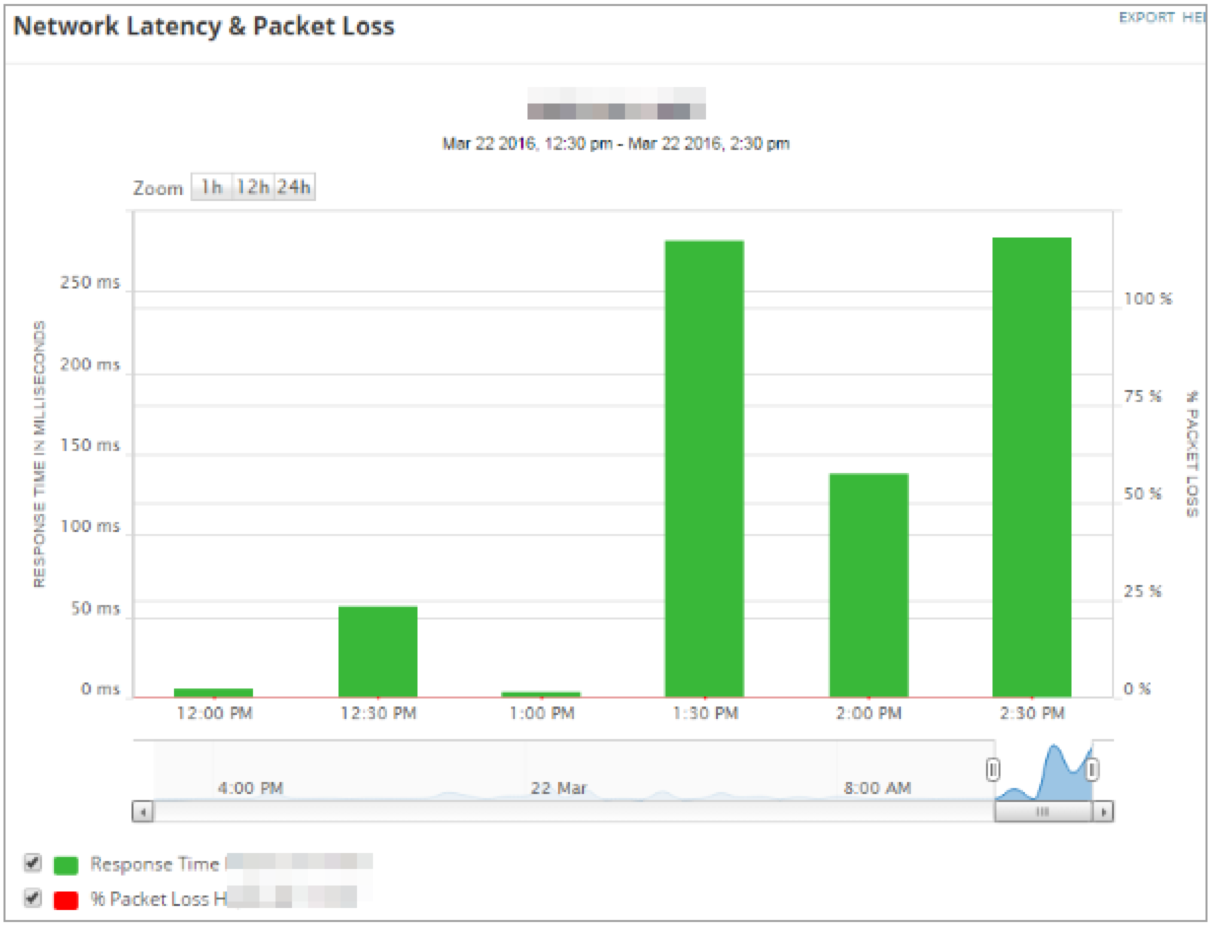
Min/Max/Average Response Time & Packet Loss

This widget shows the average load on the CPU for this node. In this case, the load spiked dramatically around 1:30 PM, which warrants further investigation.



Network Latency & Packet Loss

This widget shows the latency (response time) and packet loss for the entire node. A spike in response time occurred at the same time as the spike in the average CPU load (shown above), implying correlation between the events.



These widgets indicate an unknown increase in traffic that occurred at approximately 1:30 PM, leading to higher interface utilization, CPU load, and dropped packets. Values are not yet critical and no alerts have been triggered, and so it might not be a concern, but if you wanted to continue troubleshooting, you could perform the following actions:

- Determine if there were any configuration changes around that time. If you have Network Configuration Manager, you can use it to look up configuration changes.
- If you are monitoring traffic (for example, with NetFlow Traffic Analyzer), explore the cause of the traffic spike.

How alerts work

An alert is a notification that there is a problem with a monitored entity. The SolarWinds Platform comes with hundreds of predefined alerts for common problems, such as a node or application going down, high interface utilization, or packet loss.

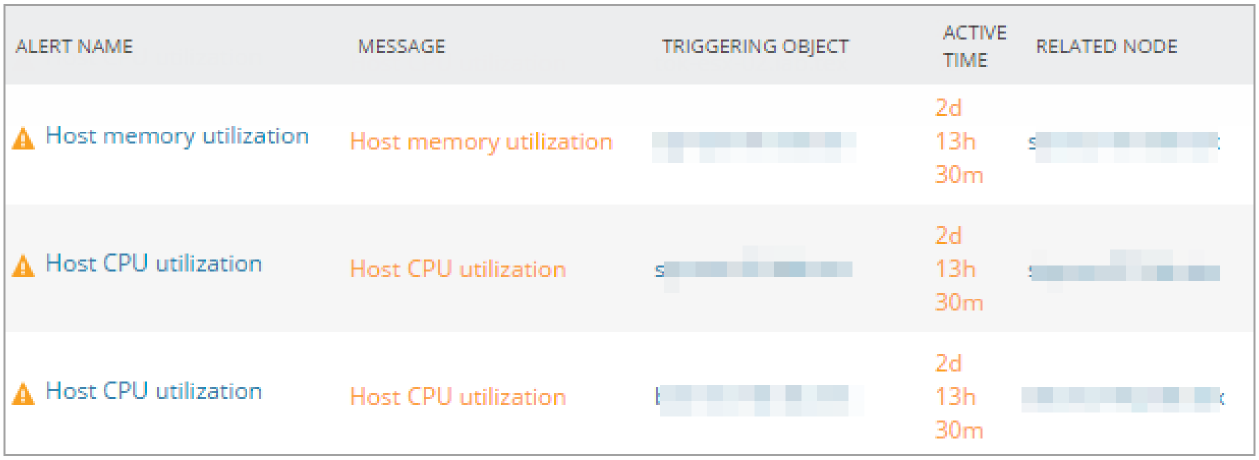
Many predefined alerts are enabled by default, so if there are problems, you are alerted as soon as you discover your network and add discovered devices toSolarWinds Platform.

SolarWinds recommends that you identify who will receive warning or critical alerts.

By default, alerts do not send emails and text messages. You need to configure the default information in the email action first.

You can also integrate alerts with SolarWinds Help Desk.

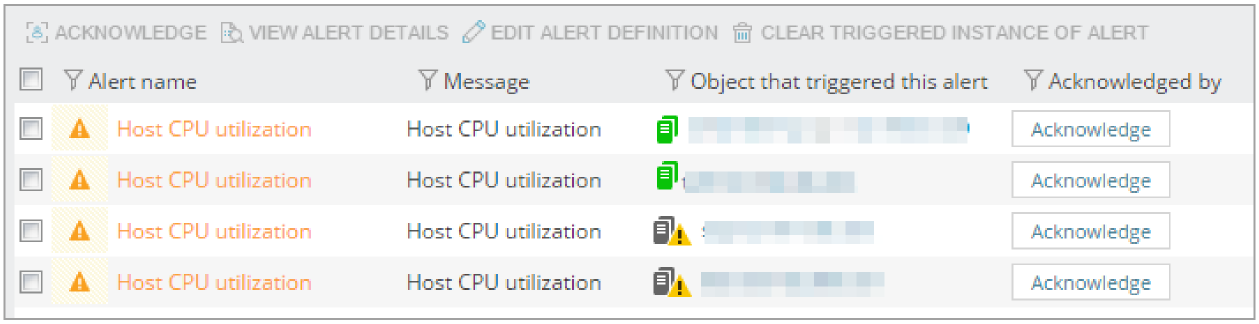
By default, alerts appear in the Active Alerts widgets on the Orion Home page.



ALERT NAME	MESSAGE	TRIGGERING OBJECT	ACTIVE TIME	RELATED NODE
⚠ Host memory utilization	Host memory utilization	[redacted]	2d 13h 30m	[redacted]
⚠ Host CPU utilization	Host CPU utilization	[redacted]	2d 13h 30m	[redacted]
⚠ Host CPU utilization	Host CPU utilization	[redacted]	2d 13h 30m	[redacted]

To see all alerts, click the All Active Alerts button in the Active Alerts widget, or go to Alerts & Activity > Alerts. On this page, you can:

- Acknowledge an alert that you are working on
- Click on any alert to go to the Alert Details page for more information
- Click Manage Alerts to enable/disable, add, or edit any alert



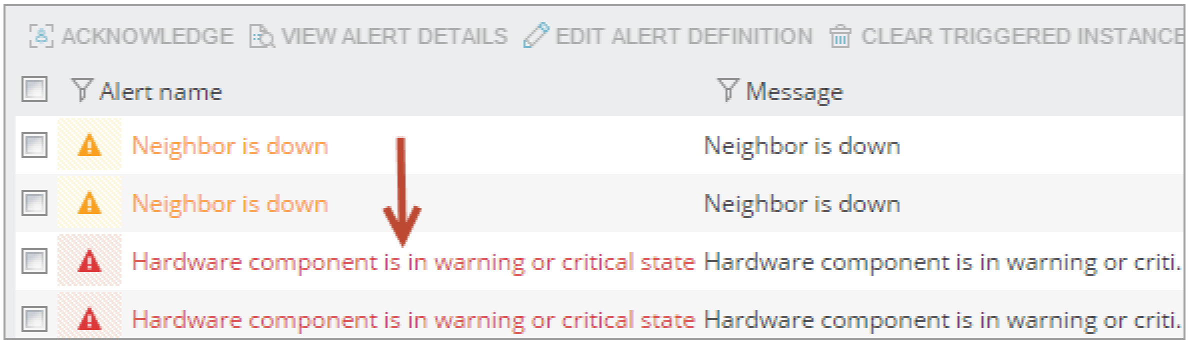
□	Alert name	Message	Object that triggered this alert	Acknowledged by
□	Host CPU utilization	Host CPU utilization	[redacted]	Acknowledge
□	Host CPU utilization	Host CPU utilization	[redacted]	Acknowledge
□	Host CPU utilization	Host CPU utilization	[redacted]	Acknowledge
□	Host CPU utilization	Host CPU utilization	[redacted]	Acknowledge

You can create your own alerts, either by modifying a predefined alert, or by creating a custom alert. See Getting Started Guide 2 - Customize.

Work with preconfigured alerts

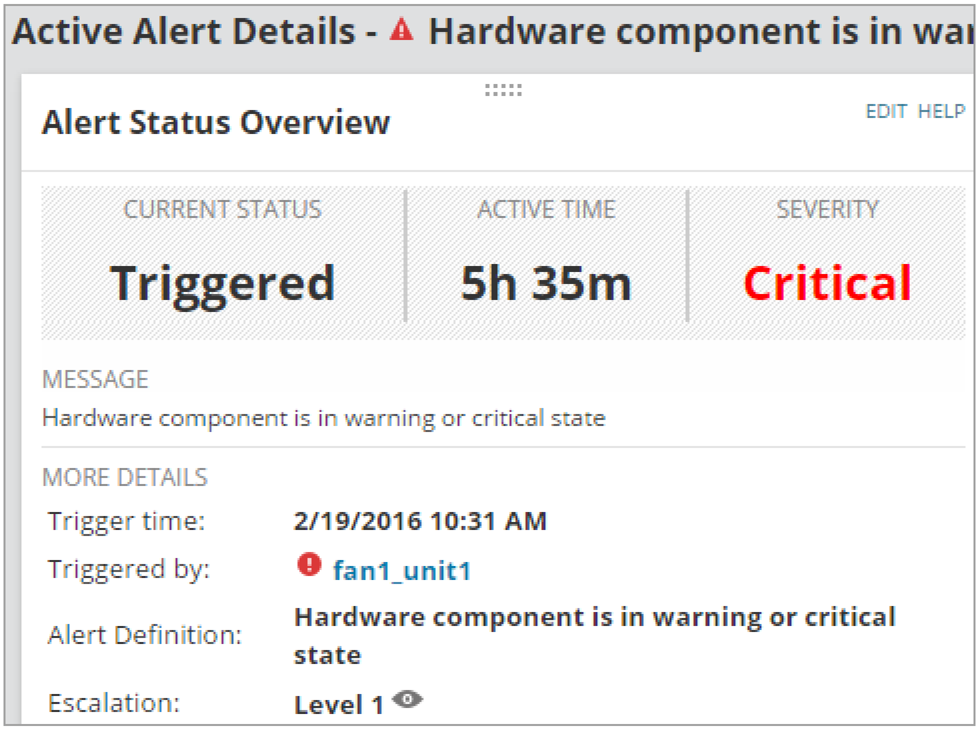
When an alert is triggered, any associated actions are executed, and the alert appears on the All Active Alerts page.

1. To view the alert details, click the alert.



□	Alert name	Message
□	Neighbor is down	Neighbor is down
□	Neighbor is down	Neighbor is down
□	Hardware component is in warning or critical state	Hardware component is in warning or criti.
□	Hardware component is in warning or critical state	Hardware component is in warning or criti.

The Active Alert Details page appears.



Active Alert Details - ⚠ Hardware component is in wa

Alert Status Overview

CURRENT STATUS	ACTIVE TIME	SEVERITY
Triggered	5h 35m	Critical

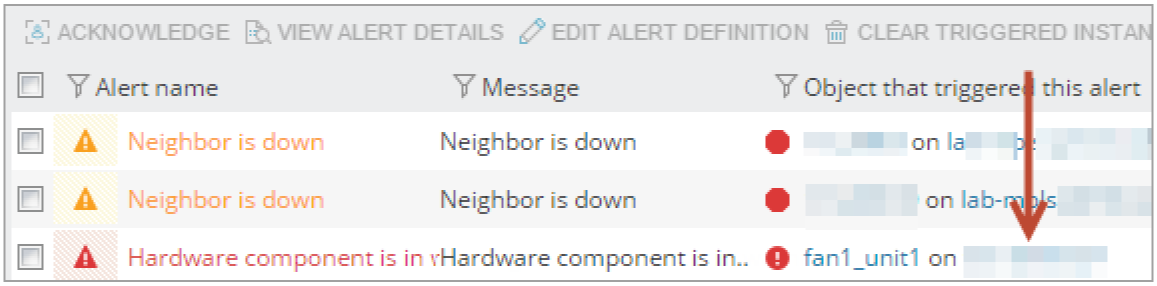
MESSAGE

Hardware component is in warning or critical state

MORE DETAILS

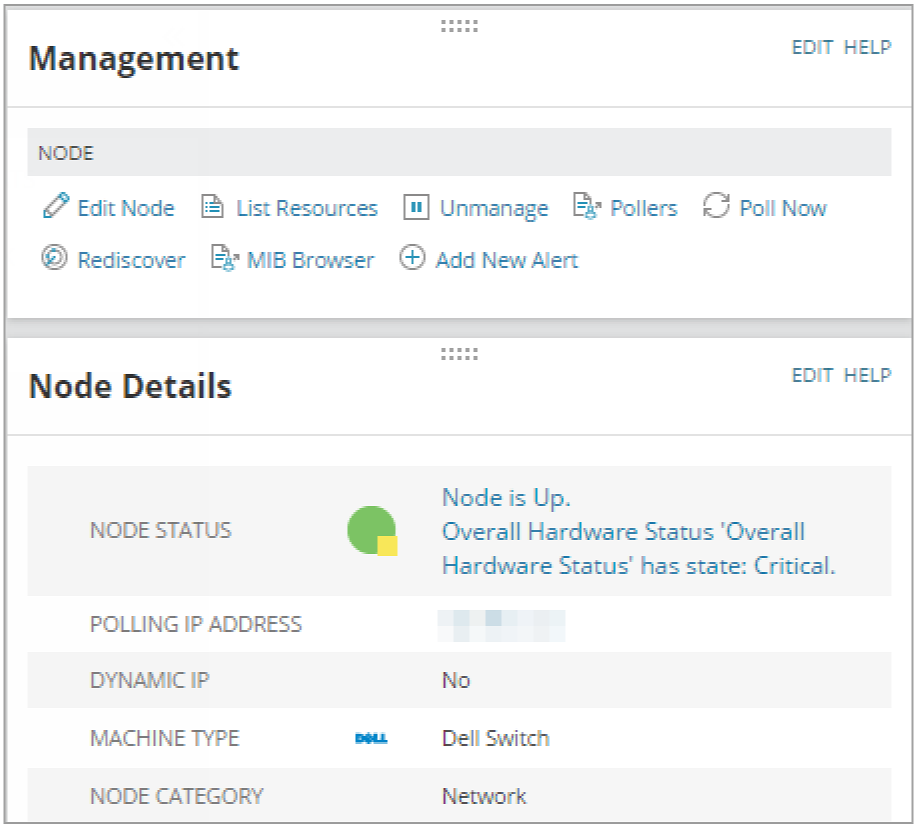
Trigger time:	2/19/2016 10:31 AM
Triggered by:	● fan1_unit1
Alert Definition:	Hardware component is in warning or critical state
Escalation:	Level 1

2. To view the details of the network object that triggered the alert, click an object.



□	Alert name	Message	Object that triggered this alert
□	⚠ Neighbor is down	Neighbor is down	● [redacted] on la[redacted]
□	⚠ Neighbor is down	Neighbor is down	● [redacted] on lab-mpls[redacted]
□	⚠ Hardware component is in v	Hardware component is in..	● fan1_unit1 on [redacted]

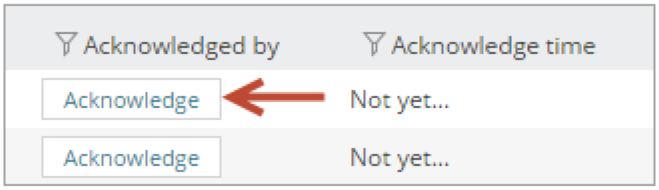
The details page of the selected object appears.



NODE STATUS	Node is Up. Overall Hardware Status 'Overall Hardware Status' has state: Critical.
POLLING IP ADDRESS	[redacted]
DYNAMIC IP	No
MACHINE TYPE	Dell Switch
NODE CATEGORY	Network

3. To acknowledge an alert:

    a. Click Acknowledge.

Acknowledged by	Acknowledge time
Acknowledge	Not yet...
Acknowledge	Not yet...

    b. Enter a note and click Acknowledge.

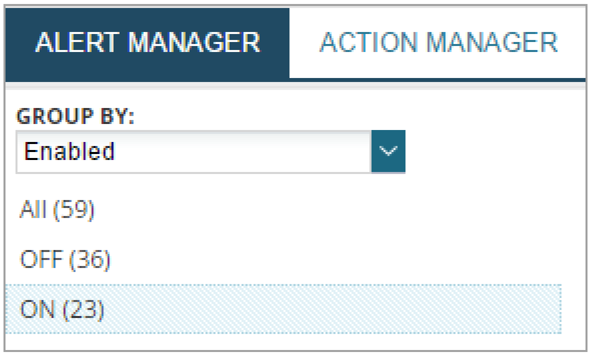
    Acknowledging the alert stops the escalation process. Acknowledgment also provides an audit trail and prevents multiple people from working on the same issue.

List preconfigured, enabled alerts

NPM ships with preconfigured, enabled alerts, and a number of alerts that you can enable and make operational. To see the list of preconfigured, enabled alerts:

1. Click Alerts & Activity > Alerts.
2. Click Manage Alerts.

3. In the Group by field, select Enabled.

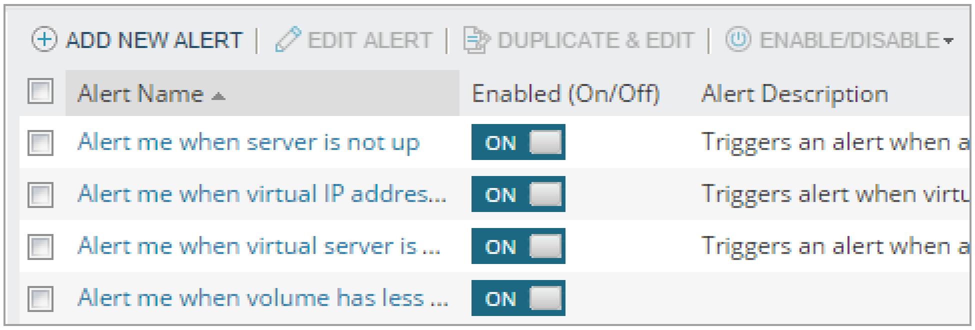


GROUP BY: Enabled

- All (59)
- OFF (36)
- ON (23)

4. In the Type field, sort by Out-of-the-box.

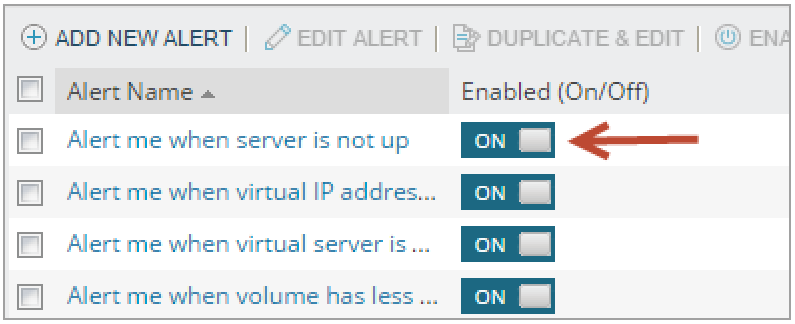
5. Review the list of preconfigured, enabled alerts.



□	Alert Name ▲	Enabled (On/Off)	Alert Description
□	Alert me when server is not up	ON	Triggers an alert when a
□	Alert me when virtual IP addres...	ON	Triggers alert when virtu
□	Alert me when virtual server is ...	ON	Triggers an alert when a
□	Alert me when volume has less ...	ON	

Enable and disable alerts

To enable or disable alerts, on the Manage Alerts page, click On or Off in the Enabled column.



□	Alert Name ▲	Enabled (On/Off)
□	Alert me when server is not up	ON
□	Alert me when virtual IP addres...	ON
□	Alert me when virtual server is ...	ON
□	Alert me when volume has less ...	ON

Action types

You can configure an alert to trigger one or more actions, such as send an email including a web page, power a virtual machine on or off, or log the alert and send a file.

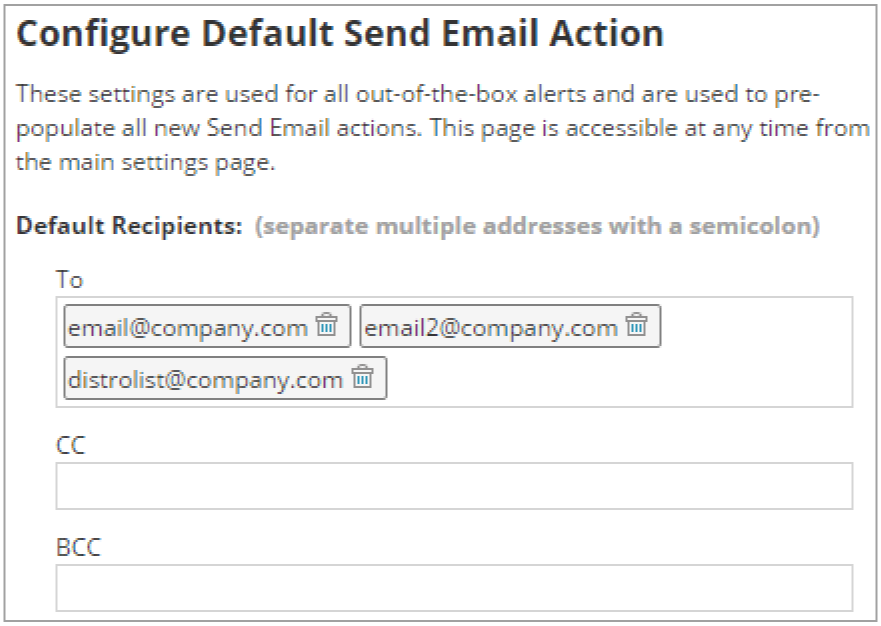
> ⓘ A complete list of alert actions is available on the Add Action dialog box that you see when you configure an alert.

Configure the default email action

A common alert action for the SolarWinds Platform is sending an email to one or more responsible parties who can open the SolarWinds Platform Web Console directly from the email, and begin troubleshooting.

This alert action requires that you configure a designated SMTP server. When you configure a default email action, you can reuse the action for all alerts, which means that you do not need to enter email parameters for each alert.

1. Click Settings > All Settings > Configure Default Send Email Action.
2. In the Default Recipients section, provide the email addresses of default recipients, separated by a semicolon.



Configure Default Send Email Action

These settings are used for all out-of-the-box alerts and are used to pre-populate all new Send Email actions. This page is accessible at any time from the main settings page.

Default Recipients: (separate multiple addresses with a semicolon)

To

email@company.com email2@company.com distrolist@company.com

CC

BCC

3. Under the Default Sender Details heading, provide the default Name of Sender and the default Reply Address.

4. Under the Default SMTP Server section:

   a. Provide the Host name or IP Address of the SMTP Server and the designated SMTP Port Number.

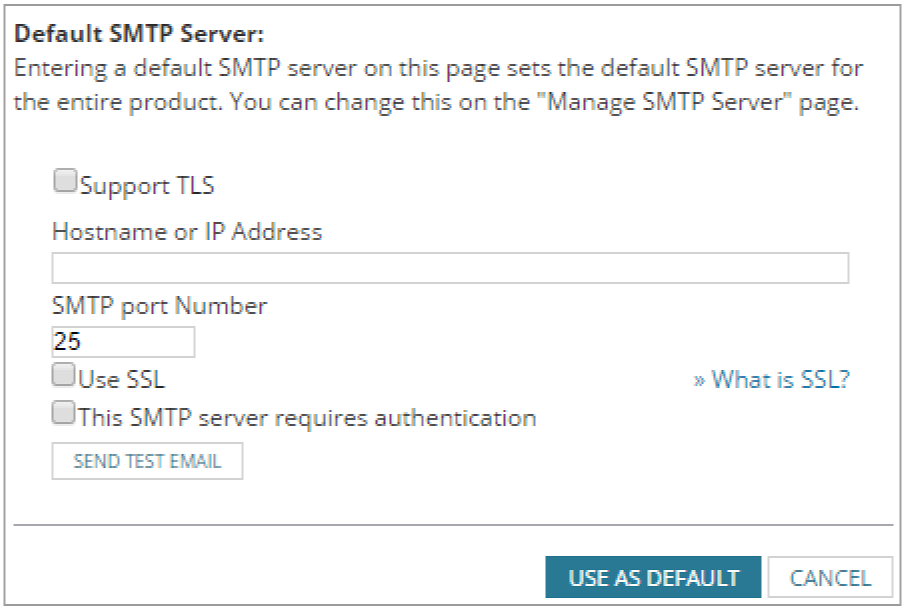
      For example, `192.168.10.124`, port `25`.

   b. If you want to use SSL encryption for your alert emails, select Use SSL.

      Selecting SSL automatically changes the SMTP port number to `465`.

   c. If your SMTP server requires authentication, select This SMTP Server requires Authentication, and then provide the credentials.

   d. Click Use as Default.



Default SMTP Server:
Entering a default SMTP server on this page sets the default SMTP server for the entire product. You can change this on the "Manage SMTP Server" page.

☐ Support TLS

Hostname or IP Address

SMTP port Number

25

☐ Use SSL

☐ This SMTP server requires authentication

How reports work

Reports provide a bridge between detailed views (which provide point-in-time information) and alerts (which tell you there is a problem). Reports can contain detailed, current state information, or they can contain historical data.

You can run an ad-hoc report, or schedule reports to be sent to you automatically, as a PDF, a web page, or email. For example, use a schedule when you want to receive the bandwidth usage from the last 7 days report every Monday morning.

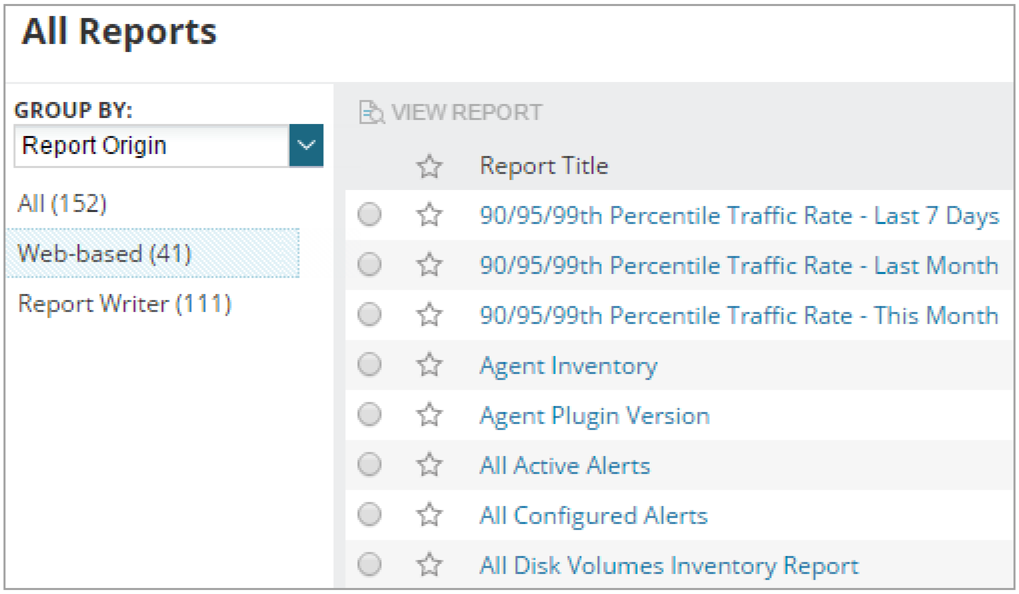
SolarWinds recommends that you identify who needs to receive performance or status reports, and how often they should receive them.

Run a report

SolarWinds provides predefined reports for each SolarWinds Platform product.

To provide meaningful data, some reports require that you monitor the devices for a certain time period. For example, it takes two weeks for baseline reports to populate.

1. Click Reports > All Reports to see the available predefined reports.



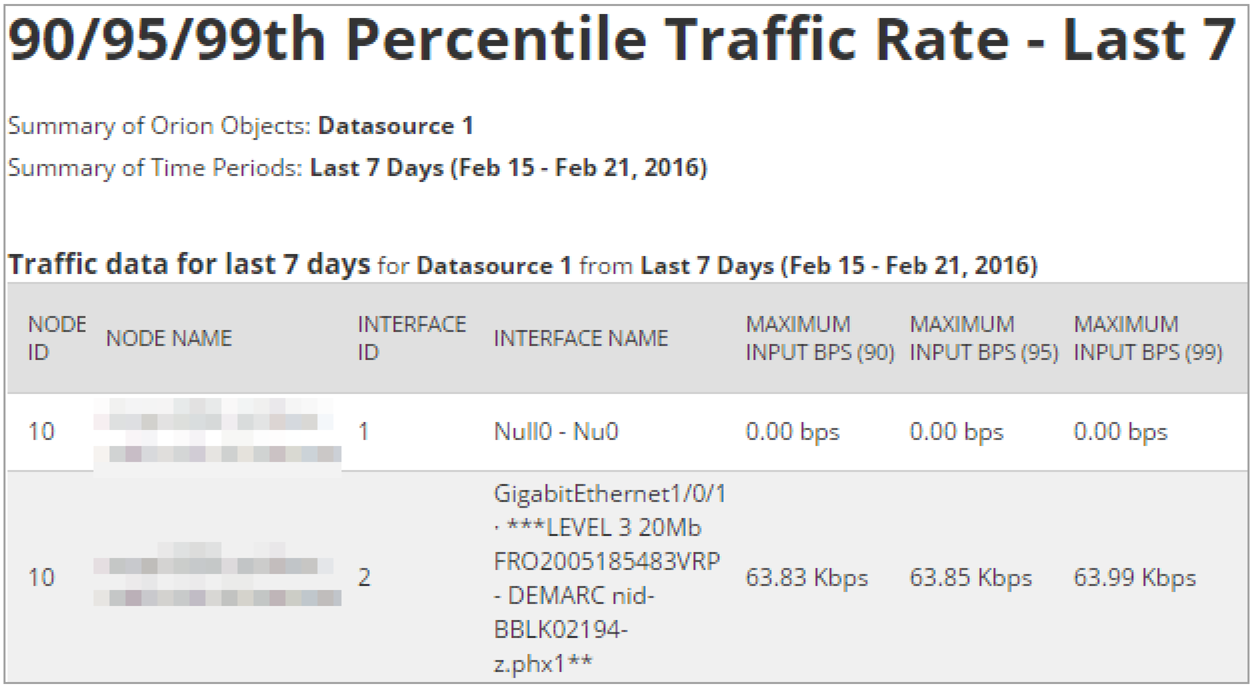
All Reports

GROUP BY: Report Origin

- All (152)
- Web-based (41)
- Report Writer (111)

	☆	Report Title
○	☆	90/95/99th Percentile Traffic Rate - Last 7 Days
○	☆	90/95/99th Percentile Traffic Rate - Last Month
○	☆	90/95/99th Percentile Traffic Rate - This Month
○	☆	Agent Inventory
○	☆	Agent Plugin Version
○	☆	All Active Alerts
○	☆	All Configured Alerts
○	☆	All Disk Volumes Inventory Report

2. On the All Reports page, click the report title to run it immediately. The report populates with data. To share the report, click Export or Print in the top right corner.



90/95/99th Percentile Traffic Rate - Last 7

Summary of Orion Objects: **Datasource 1**

Summary of Time Periods: **Last 7 Days (Feb 15 - Feb 21, 2016)**

Traffic data for last 7 days for **Datasource 1** from **Last 7 Days (Feb 15 - Feb 21, 2016)**

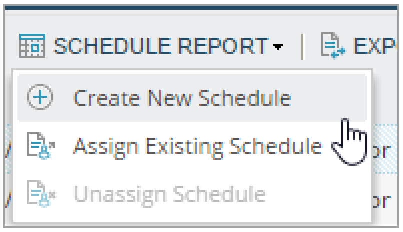
NODE ID	NODE NAME	INTERFACE ID	INTERFACE NAME	MAXIMUM INPUT BPS (90)	MAXIMUM INPUT BPS (95)	MAXIMUM INPUT BPS (99)
10	[redacted]	1	Null0 - Nu0	0.00 bps	0.00 bps	0.00 bps
10	[redacted]	2	GigabitEthernet1/0/1 · ***LEVEL 3 20Mb FRO2005185483VRP - DEMARC nid-BBLK02194-z.phx1**	63.83 Kbps	63.85 Kbps	63.99 Kbps

Schedule a web-based report

1. Click Settings > All Settings > Manage Reports.

> ⓘ To access the Report Scheduler and the Report Manager, your user account needs to have the Report Management rights.
>
> You can also access the view from Reports: Click Reports > All Reports, and then click Manage Reports in the top right corner of the view.

2. Select a web-based report, and click Schedule Report > Create New Schedule.



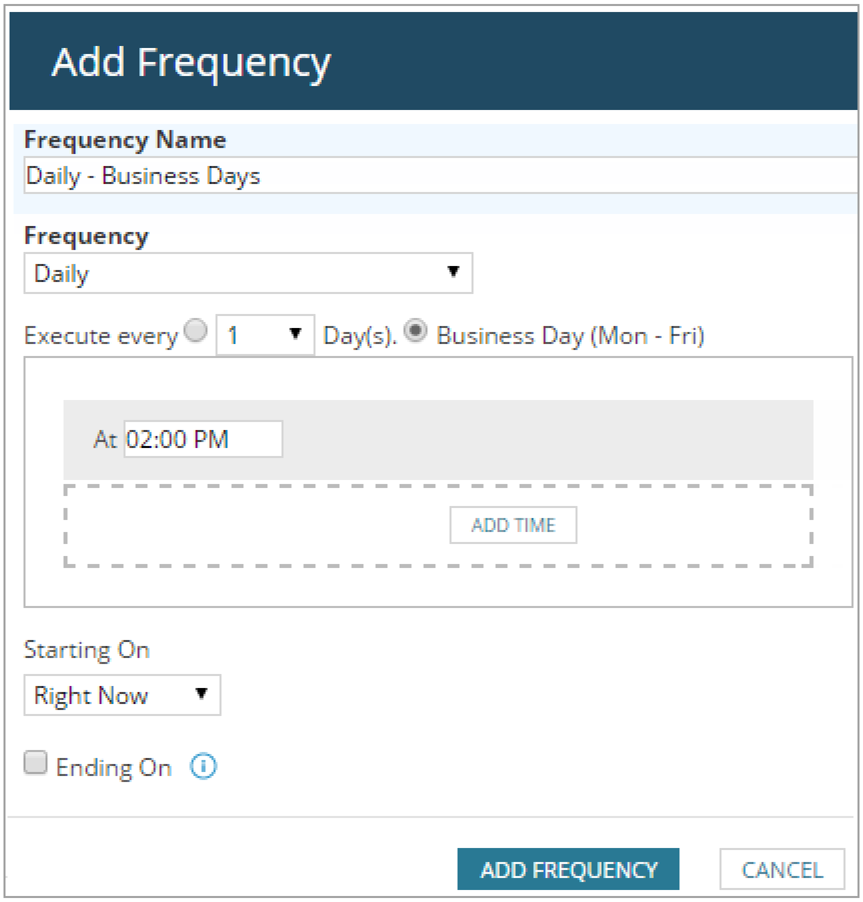
3. On the Schedule Properties panel, type a name and description and click Next.

4. On the Schedule Frequency panel, click Add Frequency.

5. On the Add Frequency dialog box, type a name and select a time interval.

6. Select the days when you want to execute the report.

7. Enter a time and click Add Frequency.



Add Frequency

Frequency Name

Daily - Business Days

Frequency

Daily ▼

Execute every ○ 1 ▼ Day(s). ● Business Day (Mon - Fri)

At 02:00 PM

Starting On

Right Now ▼

□ Ending On

8. On the Schedule Frequency panel, click Next.

9. On the Actions to Execute panel, click Add Action and specify whether you want to email the report, print it, or save it to a disk. Click Next.

10. On the Schedule Configuration Summary panel, review the schedule and click Create Schedule. The SolarWinds Platform will execute the specified action (email the report, print it, or save it for you) according to the schedule.

Beyond Getting Started

NPM is a SolarWinds Platform product. The SolarWinds Platform is the core of the SolarWinds IT Management Portfolio. It ensures data collection, processing, storage, and presentation. It provides common features, such as user accounts and groups, views, dashboards, reporting, alerting, and more that you can use across all SolarWinds Platform products and access from the SolarWinds Platform Web Console.

Now that you've gotten started with NPM, check out the SolarWinds Platform Administrator Guide and NPM Administrator Guide for more information about using other features.

SolarWinds Platform Administrator Guide

Learn more about common features and administrative procedures in the SolarWinds Platform Administrator Guide (PDF), such as:

- Manage users
- Troubleshoot environmental issues with Performance Analysis dashboards
- Make your SolarWinds Platform highly available
- Manage alerts
- Manage reports
- Customize SolarWinds Platform Web Console, for example change SolarWinds logo for the logo of your company, or change the color scheme of the SolarWinds Platform Web Console.
- Customize views, widgets, and charts
- Use thresholds to specify when your nodes change status
- Monitor Hardware health
- Monitor SNMP traps and syslogs in the SolarWinds Platform
- Review events
- Use Quality of Experience
- Protect your environment with High Availability
- Scale your environment

NPM Administrator Guide

Check out the NPM Administrator Guide (PDF) to find out more about other NPM features, such as:

- Discover your network paths with NetPath™
- Monitor custom metrics on your devices

- Use Network Insight for F5 BIG-IP, Cisco Nexus devices, Cisco ASA, and Cisco ACI
- Forecast capacity

You can also connect with the NPM user community on THWACK, where you'll find training videos, blog posts, and information about what the team is working on.