GETTING STARTED GUIDE

Network Performance Monitor

Version 12.2

Part 1 of 2: Get Started

Last Updated: September 12, 2017

Retrieve the latest version from: *https://support.solarwinds.com/Success_Center/Network_Performance_Monitor_(NPM)/NPM_Documentation*

Table of Contents

Network Performance Monitor Getting Started Guide

> To install NPM, see the NPM Installation Guide. You should install NPM before using the Getting Started Guide.

Welcome to the SolarWinds Network Performance Monitor (NPM) Getting Started Guides.

These guides will take you from setting up your NPM to full implementation, including customization. It is divided into two progressive objectives:

1. **Get started.** Configure SolarWinds NPM, begin collecting data, and alert and report on your mission-critical environment.

   Quickly identify performance issues and problems before your customers call the help desk. Depending on your workload, you should be able to get started in five days or less.

2. **Customize.** Customize views, alerts, and reports.

   Tailor SolarWinds NPM to your internal processes so you can more effectively respond to performance issues. Depending on your workload, you should be able to customize SolarWinds NPM in five or fewer days.

Existing customers: Following the recommendations in this guide will ensure your system capabilities are appropriate and your production environment is sized correctly. Minimum system requirements used during evaluation are not sufficient for a production environment. Access your licensed software from the SolarWinds Customer Portal. If you need any implementation help, contact our Support team.

Read this SolarWinds Customer Support article to learn how to properly open a support case and get your case the right level of visibility.

Evaluators: If you are evaluating SolarWinds NPM, download and install a free 30-day evaluation. The evaluation version of SolarWinds NPM is a full version of the product, functional for 30 days. After the evaluation period, you can easily convert your evaluation license to a production license by obtaining and applying a license key. If you need assistance with your evaluation, contact sales@solarwinds.com.

Product terminology

Orion Platform: The common backend platform used by the SolarWinds Orion 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 Orion monitoring tools.

Orion Web Console: The web interface you see when you log on to Orion that is used to view, configure, and manage all of your monitored objects.

Check out this video on navigating the Web Console.

Orion Application Server: A Windows server that runs the Orion Web console and collects data from monitored objects. Also called the Orion Main Poller.

Orion Database Server: A Windows SQL server that should be hosted on a dedicated server in a production environment, separately from the Orion Application Server. It stores Orion configuration data and all collected performance and syslog data.

Polling Engine (Poller): A Polling Engine controls polling job scheduling, data processing, and queries your monitored devices for performance metrics like CPU, memory, and up/down status. Additional Polling Engines can be licensed to provide additional scalability and capacity. By default, the Orion Server provides one Polling Engine (often referred to as the Main Poller).

Related Guides

- Network Performance Monitor Installation Guide
- Network Performance Monitor Getting Started Guide: Customize (Part 2 of 2)

Discover

This section contains the following network discovery topics:

- What should I monitor?
- Discover your network
- Add discovered devices to SolarWinds Orion
- Add a single node for monitoring
- Advanced discovery

What should I monitor?

Discovery is the term used to describe the process SolarWinds Orion uses to identify network elements. During discovery, SolarWinds Orion scans the network for nodes, and when a node and associated elements are found, you can you can add them to the SolarWinds Orion database for monitoring.

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. After you have the monitoring, alerts, and reports set up, SolarWinds recommends adding more nodes.

Discovery checklist

When you run the Discovery Wizard, you will be asked to provide IP addresses and credentials for the devices you want to monitor. SolarWinds recommends that you gather this information before running the Discovery Wizard.

□	Determine the devices to monitor.
□	Determine the protocol used to monitor your devices. If you are monitoring devices using SNMP, you must enable SNMP on those devices because it is not enabled by default. SNMP is primarily used to monitor network devices, for example, routers, firewalls, and switches. To enable SNMP, consult the device vendor documentation. If you are monitoring Windows servers, use WMI. WMI is usually enabled on Windows devices by default. Agentless monitoring using WMI is not recommended when the poller and the device are separated by a firewall. To overcome this limitation, SolarWinds provides an optional agent that allows you to securely monitor Windows servers and applications by WMI. The following table outlines the pros and cons of using SNMP and WMI.

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

	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.	✓

For additional information, see Polling methods used by Orion on the SolarWinds Customer Success Center.

When configuring your SNMP-enabled network devices for monitoring:

- 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) that is specific to the Unix-based operating system in use.
- SolarWinds NPM can monitor VMware ESX and ESXi Servers versions 4.0 and later with VMware Tools installed.
- If SNMPv2c is enabled on a device you want to monitor, by default, SolarWinds NPM attempts to use SNMPv2c to poll the device for performance information. To poll using only SNMPv1, you must disable SNMPv2c on the polled device.

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

□ SNMP v1/2c community strings and SNMP v3 community strings and credentials of the devices you want to monitor.

□ Log in credentials for each monitored device.

□ VMware host credentials. The system requires read-only permissions.

□ Windows credentials: domain or local admin.

Discover your network

Check out this video on discovering your network.

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

Before you discover your network:

- Ensure that you determine what to monitor
- Enable the networking devices you want to monitor for SNMP
- Enable Windows devices for WMI

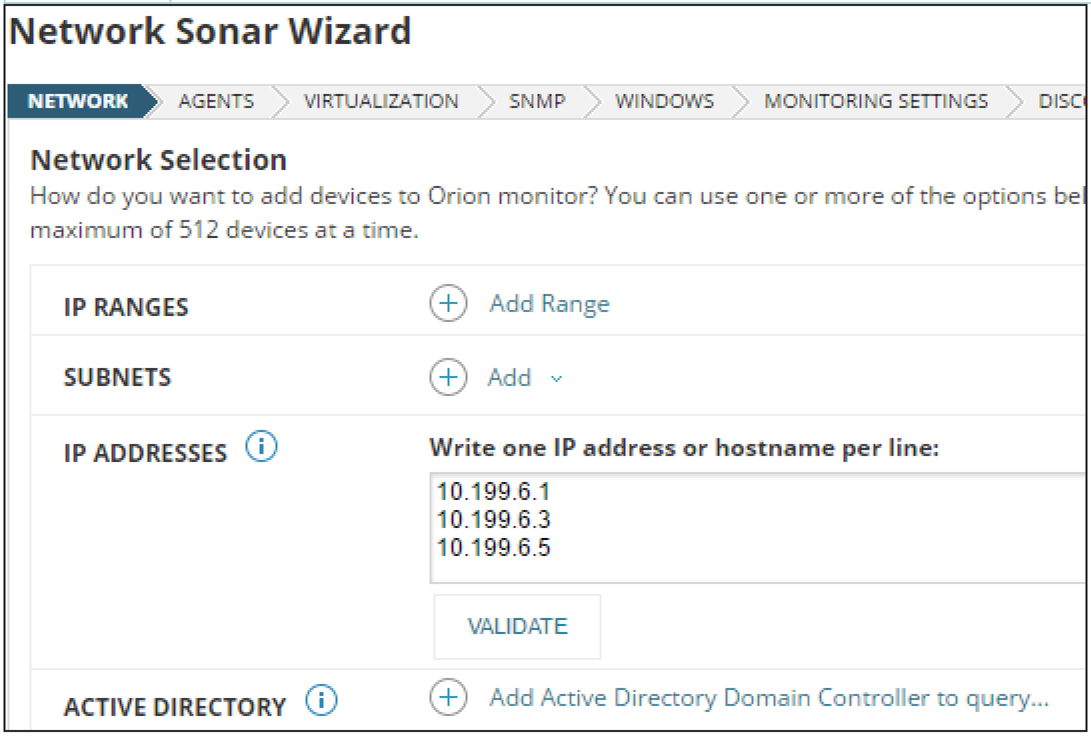
The first time you discover your network, SolarWinds recommends adding a limited number of edge routers or switches, firewalls, load balancers (if you have them), and critical physical or virtual servers and hosts.

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

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.



Network Sonar Wizard

Network Selection

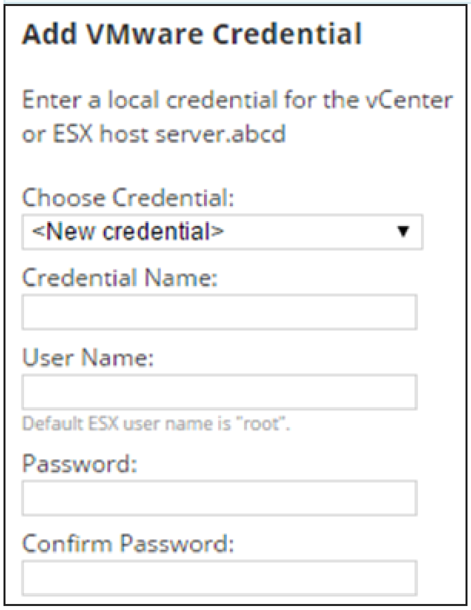
How do you want to add devices to Orion monitor? You can use one or more of the options bel
maximum of 512 devices at a time.

Write one IP address or hostname per line:

```
10.199.6.1
10.199.6.3
10.199.6.5
```

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:

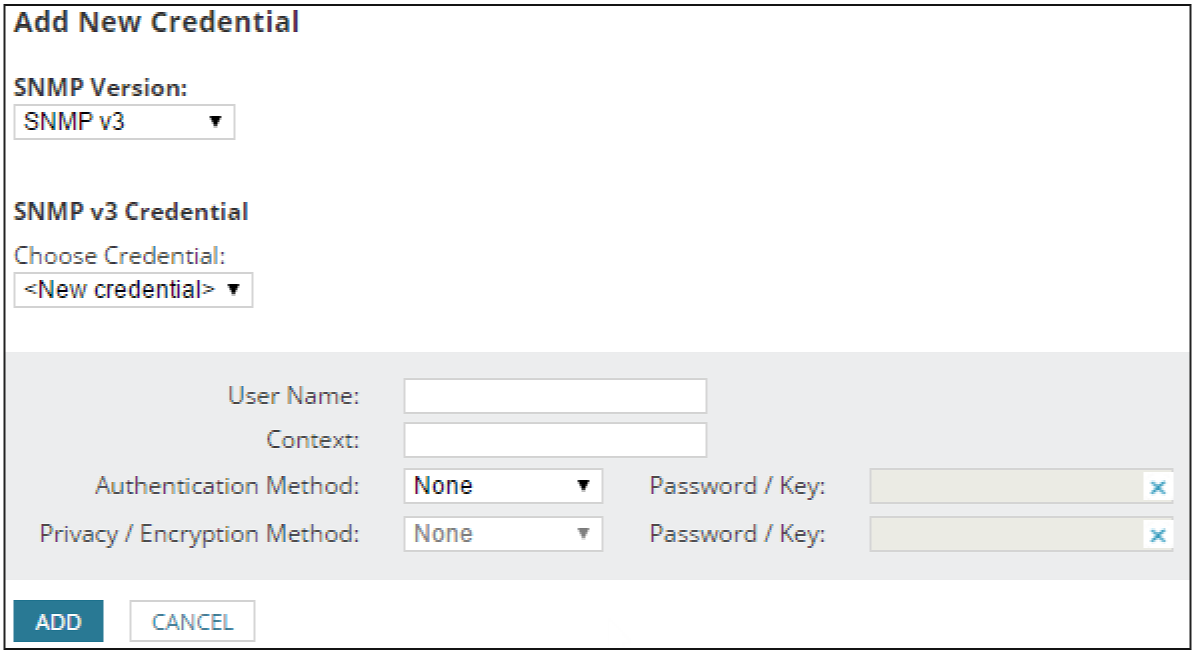
User Name:

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 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:

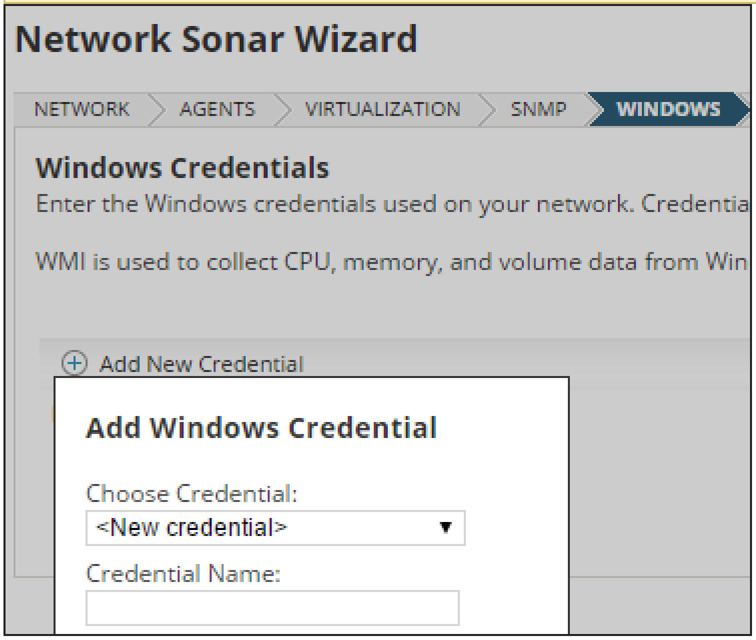
Context:

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

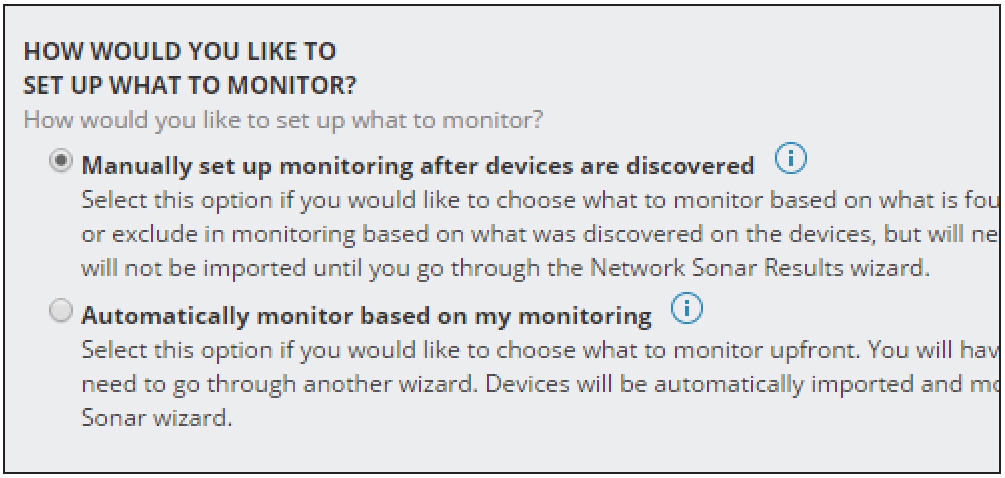
WMI is used to collect CPU, memory, and volume data from Win

Add 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.



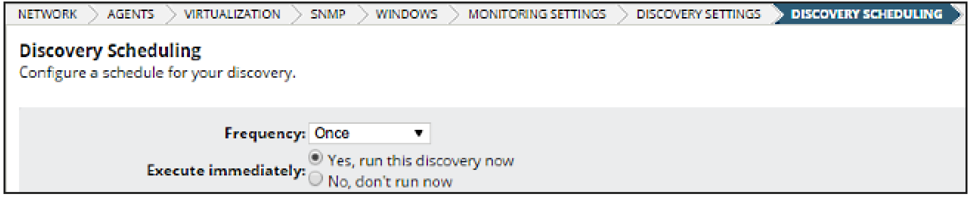
HOW WOULD YOU LIKE TO
SET UP WHAT TO MONITOR?

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.

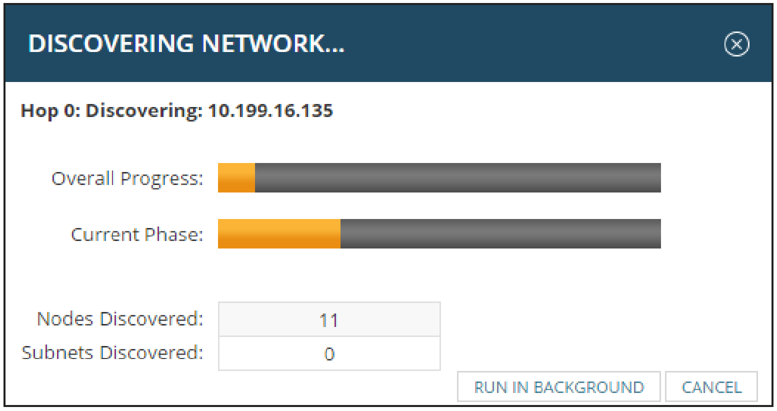
9. On the Discovery Settings panel, click Next.
10. Accept the default frequency and run the discovery immediately.



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: 10.199.16.135

Nodes Discovered: 11
Subnets Discovered: 0

Add discovered devices to SolarWinds Orion

Check out this video on adding devices to SolarWinds NPM.

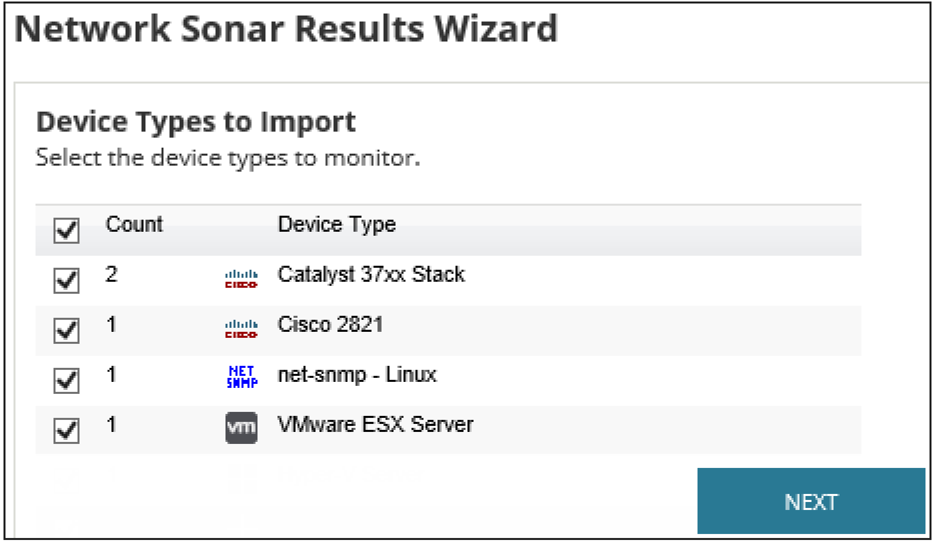
After the Network Sonar Wizard discovers your network, the Network Sonar Results Wizard opens, allowing you to import network elements into the SolarWinds Orion database. Discovered elements do not count against your license count; only elements that you import into the Orion database count against your license.

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

Before you begin, ensure that you Discover your network.

> 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

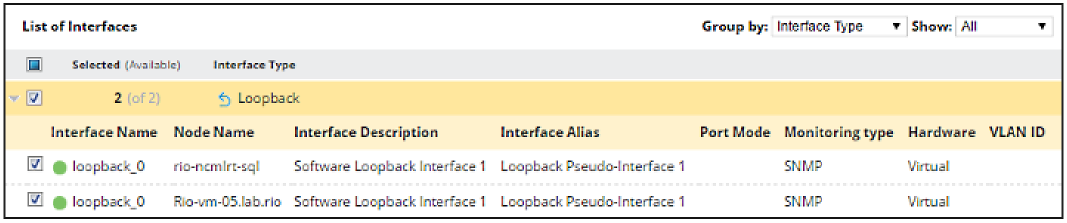
Device Types to Import

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

> After discovery, if the status of a node is Unknown, you may need to check a few settings in SolarWinds NPM. See Troubleshoot Unknown Nodes for more information.

2. Ensure the interfaces you want monitor are selected, and click Next.
   SolarWinds recommends that you do not monitor VoIP interfaces or NULL interfaces.



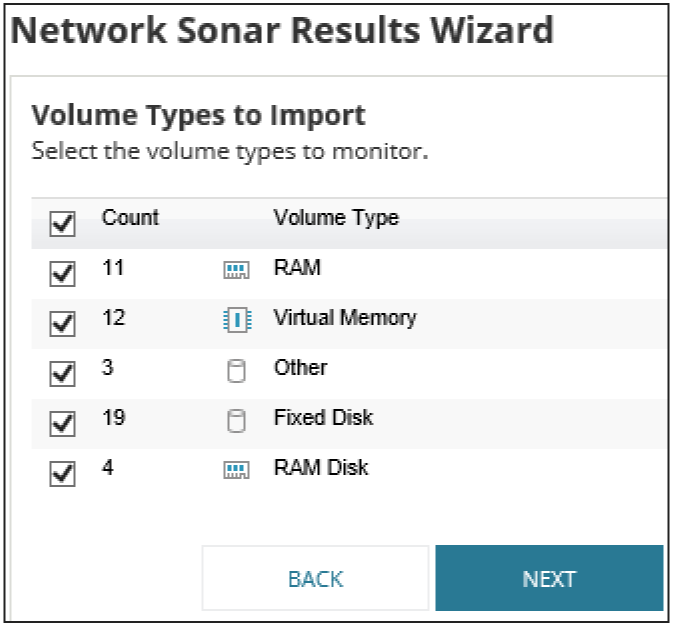
List of Interfaces — Group by: Interface Type ▾ Show: All ▾

☑	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	rio-ncmlrt-sql	Software Loopback Interface 1	Loopback Pseudo-Interface 1		SNMP	Virtual	
☑	● loopback_0	Rio-vm-05.lab.rio	Software Loopback Interface 1	Loopback Pseudo-Interface 1		SNMP	Virtual	

> By default, SolarWinds Orion 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.

3. 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.



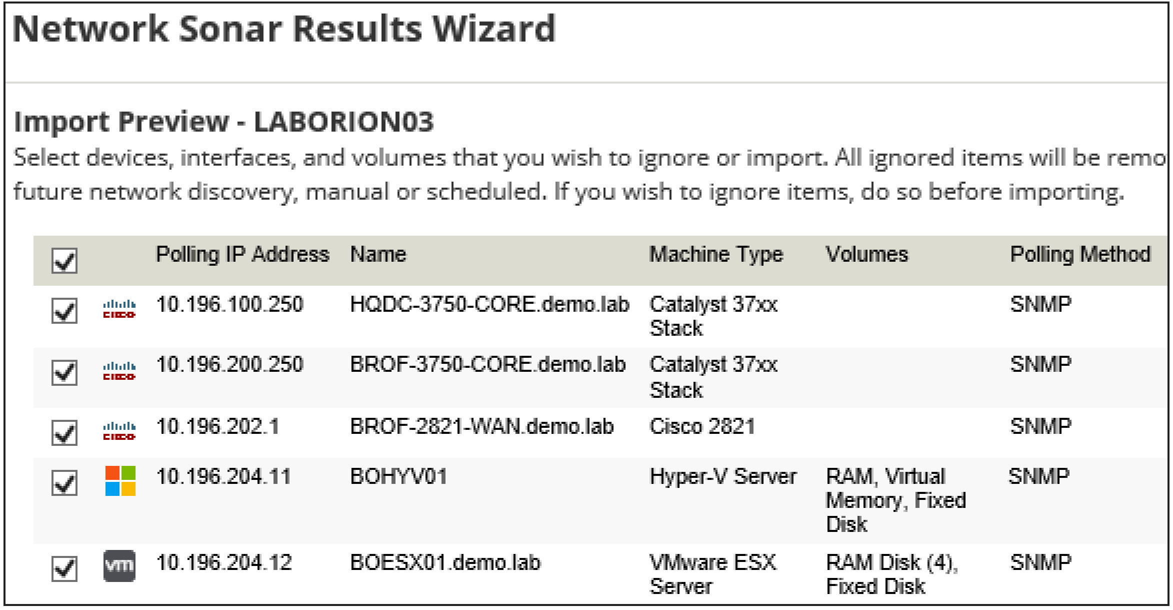
Network Sonar Results Wizard

Volume Types to Import

Select the volume types to monitor.

☑	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.



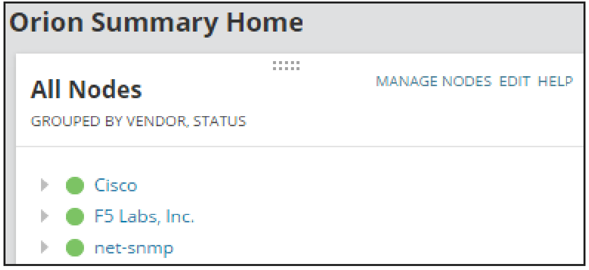
Network Sonar Results Wizard

Import Preview - LABORION03

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	10.196.100.250	HQDC-3750-CORE.demo.lab	Catalyst 37xx Stack		SNMP
☑	CISCO	10.196.200.250	BROF-3750-CORE.demo.lab	Catalyst 37xx Stack		SNMP
☑	CISCO	10.196.202.1	BROF-2821-WAN.demo.lab	Cisco 2821		SNMP
☑		10.196.204.11	BOHYV01	Hyper-V Server	RAM, Virtual Memory, Fixed Disk	SNMP
☑	vm	10.196.204.12	BOESX01.demo.lab	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

MANAGE NODES EDIT HELP

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

Add a single node for monitoring

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

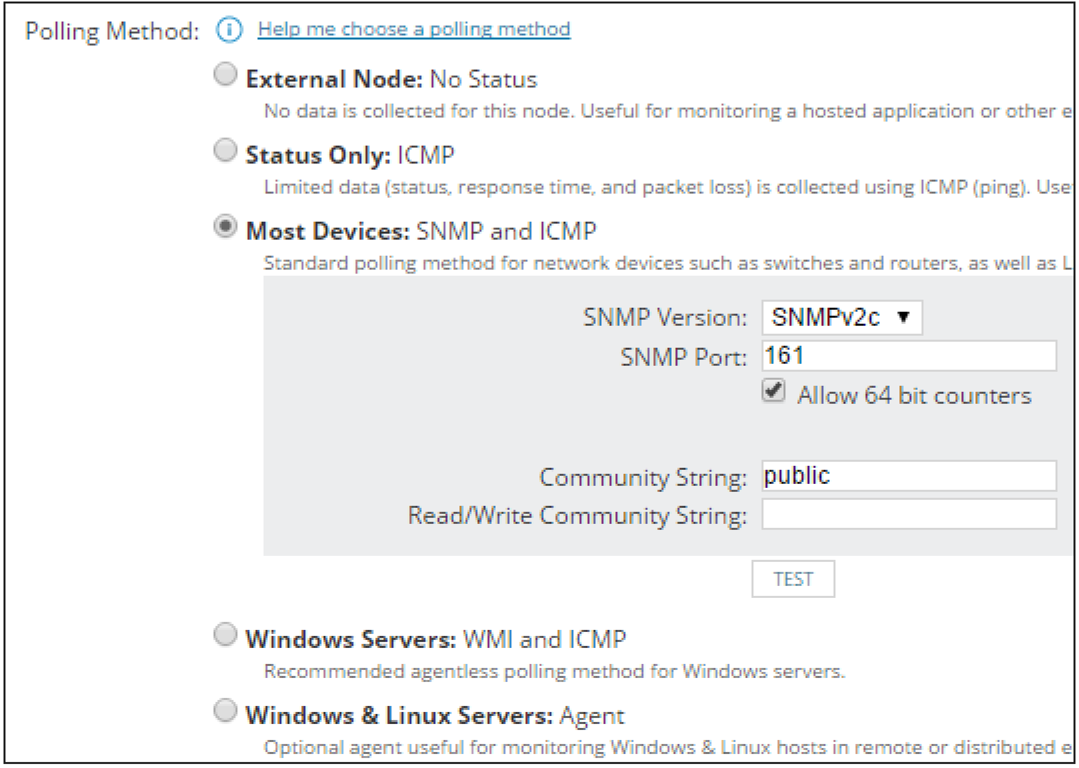
> Adding a single node offers more detail in monitoring and is the recommended approach when you have a node with high latency. Do not include nodes with high latency in a discovery job.

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.



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

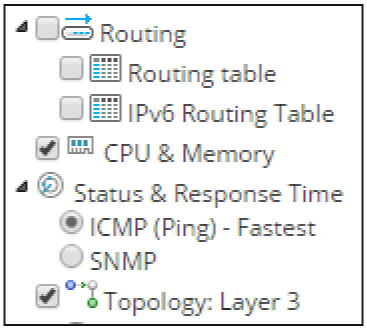
Community String: public
Read/Write Community String:

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

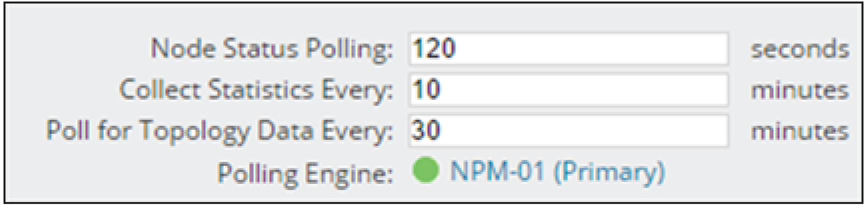
4. Select the statistics and resources to monitor on the node, and click Next.



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

5. If you 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.



Node Status Polling: 120 seconds

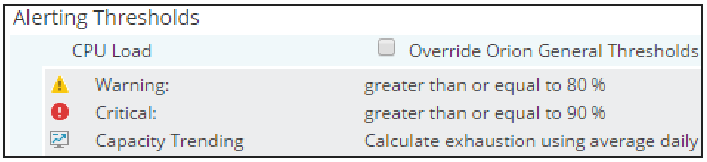
Collect Statistics Every: 10 minutes

Poll for Topology Data Every: 30 minutes

Polling Engine: ● NPM-01 (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 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.



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.

Advanced discovery

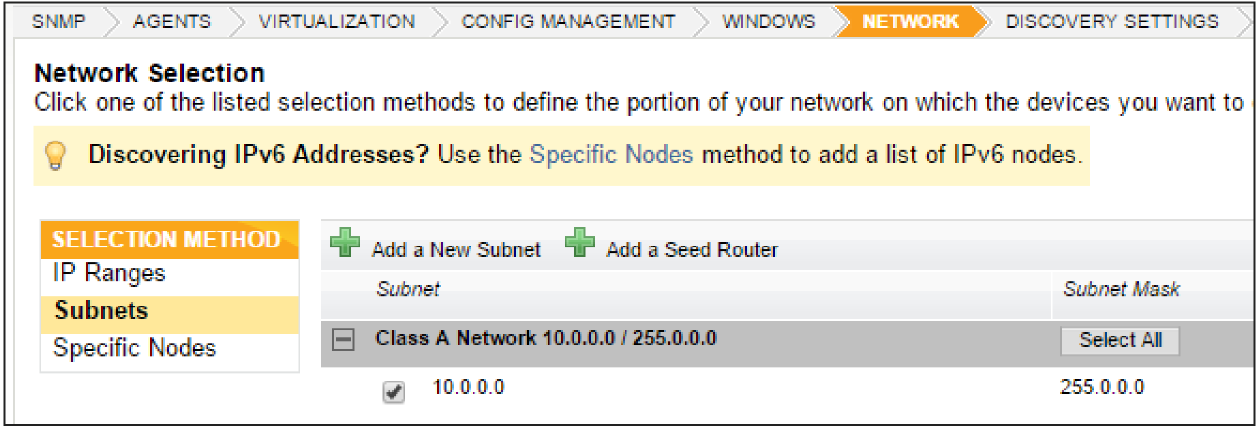
[Check out this video on managing discovery jobs and performance.]

At this point you have completed an initial discovery. Now you can add discoveries to include other segments of your IT environment.

> ⓘ Discovery jobs do not impact polling. Polling is prioritized first.

- **Multiple jobs.** SolarWinds recommends building as many discovery jobs as needed to scan your network. Initially, run the jobs immediately so you can see everything on your network, and then schedule the jobs to run periodically. Dividing the discovery into multiple jobs makes it easier to be selective about what to monitor, and decreases the amount of time each job runs. When you have a large environment, consider dividing discovery jobs by:
    - Credentials - the more credentials you have, the longer it takes for the discovery job to complete. Place the most common credentials at the top of the list.
    - IP address range - use a range that consists of fewer than 2,000 IP addresses. In a range, unresponsive IP addresses slow down discovery.
    - Latency - run discoveries for remote offices separately so that you can adjust the timeout threshold.
    - Polling engine - if you have multiple polling engines, configure a discovery for a specific polling engine.

- **Discovery ranges.** Although you can discover specific nodes, SolarWinds recommends using a range of IP addresses or subnets for a more complete picture of your network. None of the discovered elements count toward your license total or affect system performance until you begin monitoring. You can add multiple IP ranges or subnets to the same scan, but you cannot include IP ranges and subnets in the same scan.



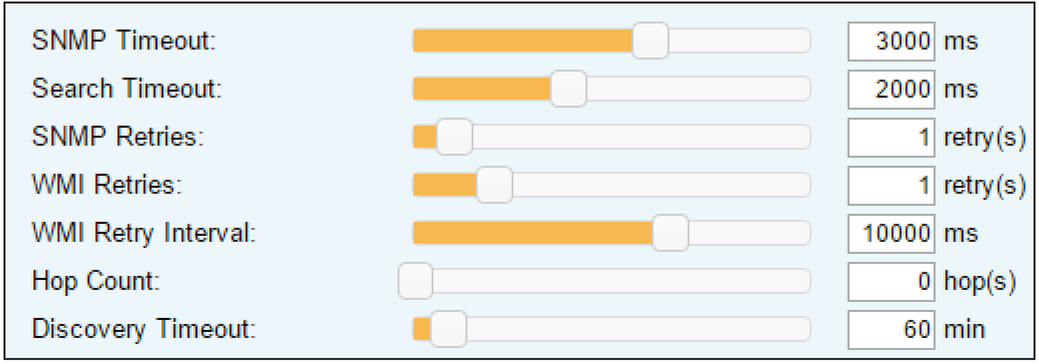
Network Selection

Click one of the listed selection methods to define the portion of your network on which the devices you want to

Discovering IPv6 Addresses? Use the Specific Nodes method to add a list of IPv6 nodes.

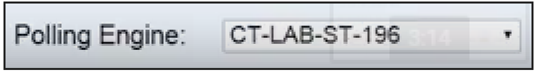
Subnet	Subnet Mask
Class A Network 10.0.0.0 / 255.0.0.0	
☑ 10.0.0.0	255.0.0.0

- **Discovery thresholds.** If you run a discovery and nodes you expect to see are not found, you may need to adjust the timeout and retry thresholds. In an environment with high latency, the default values may not be high enough. Only adjust these values after an initial scan. The higher the threshold value, the longer the discovery job takes to complete.



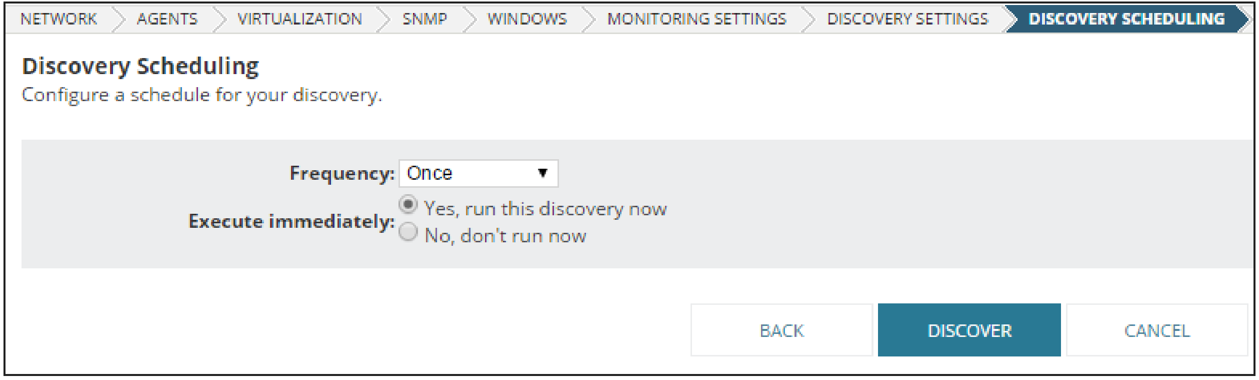
SNMP Timeout: 3000 ms
Search Timeout: 2000 ms
SNMP Retries: 1 retry(s)
WMI Retries: 1 retry(s)
WMI Retry Interval: 10000 ms
Hop Count: 0 hop(s)
Discovery Timeout: 60 min

- **Polling engine.** If you have multiple polling engines, you will see an option to select a polling engine. The polling engine you select runs the discovery job and monitors your network. SolarWinds recommends that you limit a poller to 12,000 elements, so be careful not to overload one polling engine. If you have a large environment with significant differences in latency, position the polling engine close to the monitored objects.



Polling Engine: CT-LAB-ST-196

- **Schedule intervals.** Schedule your discovery jobs to run periodically to identify new devices that were added to your network. Unless you work in a dynamic environment where new devices are frequently added to your network, SolarWinds recommends scheduling discovery daily. You can also select Advanced from the Frequency drop-down menu to create a custom frequency. The schedule interval you choose depends on how often you want to scan for changes to the network and the size and performance of your deployment.



Discovery Scheduling

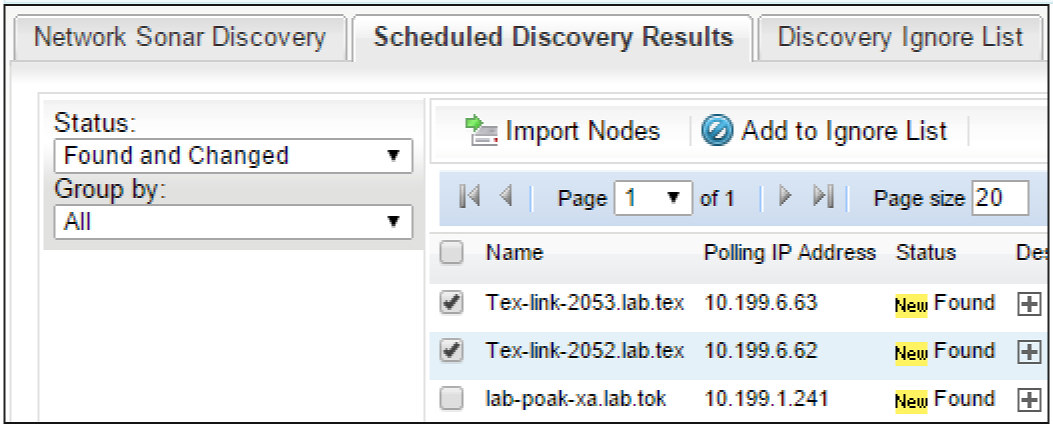
Configure a schedule for your discovery.

Frequency: Once

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

- **Scheduled results.** A manual, scheduled discovery only finds network elements, but does not automatically start monitoring. You must select what you want the system to monitor. If the scheduled job locates nodes that you do not want to monitor, select those nodes and click Add to Ignore List. Ignoring hides elements from the results list the next time the discovery job runs.

ⓘ Scheduled discovery profiles should not use IP address ranges that include nodes using DHCP.



Status: Found and Changed

Group by: All

Page 1 of 1 Page size 20

□	Name	Polling IP Address	Status	Des
☑	Tex-link-2053.lab.tex	10.199.6.63	New Found	⊞
☑	Tex-link-2052.lab.tex	10.199.6.62	New Found	⊞
□	lab-poak-xa.lab.tok	10.199.1.241	New Found	⊞

Monitor

This section includes instructions on how to explore and troubleshoot network problems:

- Navigate SolarWinds NPM
- Identify and troubleshoot a node that has a problem
- Identify and troubleshoot an interface that has a problem
- Monitor your network paths
- Plan to scale monitoring

Navigate SolarWinds NPM

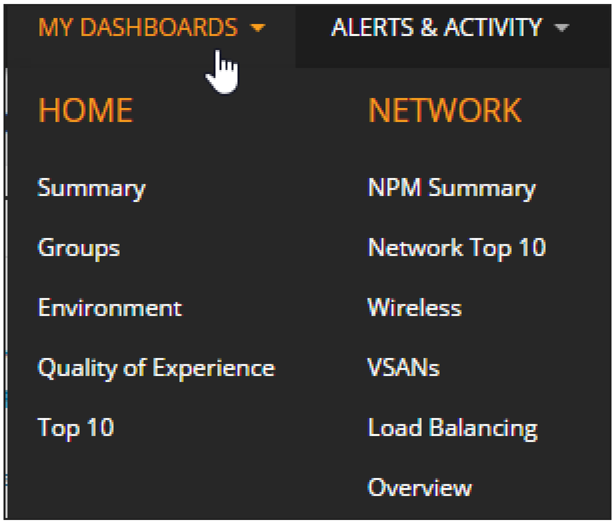
Check out this video on navigating the Web Console.

After you have installed and configured SolarWinds NPM, you can log in to the Web Console.

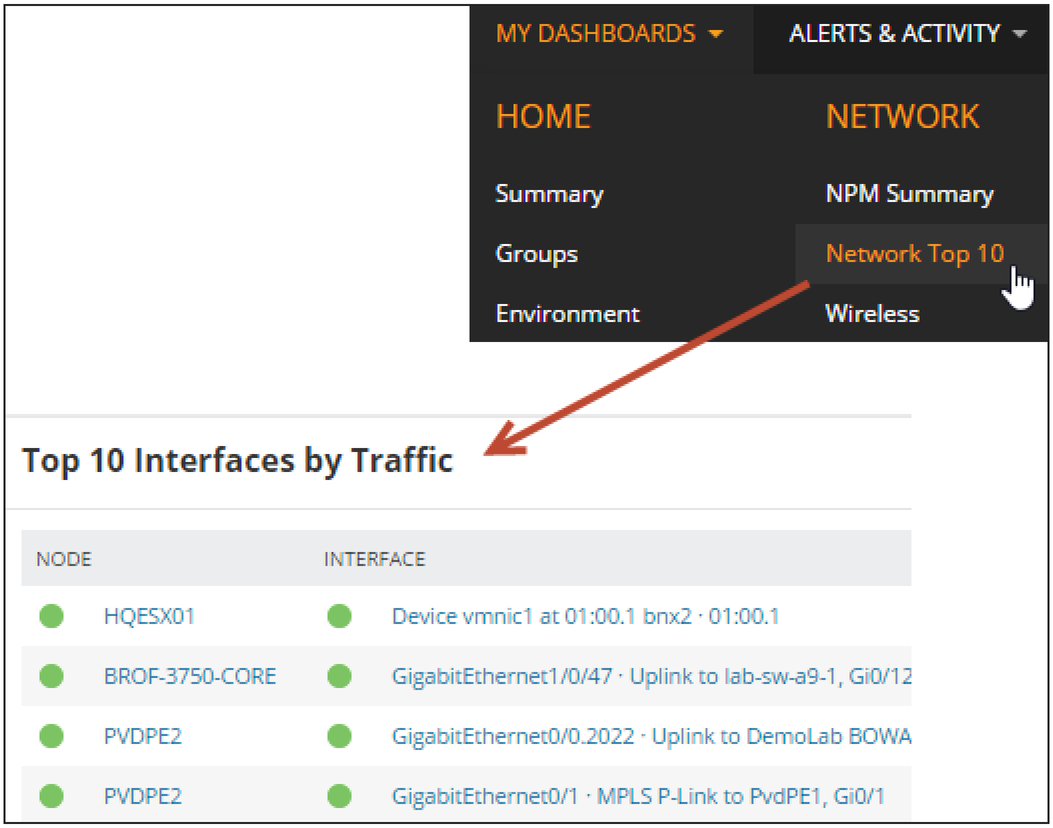
The following terms will help as you explore SolarWinds NPM:

- **Orion Platform:** The common backend platform used by the SolarWinds Orion 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 Orion monitoring tools.
- **Orion Web Console:** The web interface you see when you log on to Orion that is used to view, configure, and manage all of your monitored objects. You can access the Orion Web Console from any computer connected to the internet.
- **View:** An individual page in the web console.
- **Resource:** The widgets or informational blocks that make up a view.
- **Element:** Anything that can be monitored by Orion.

When you first log in, tabs appear at the top of the web console. Other than Home, each application tab corresponds to an Orion module. If you have installed only SolarWinds NPM, then you will see a Home tab and a Network tab.



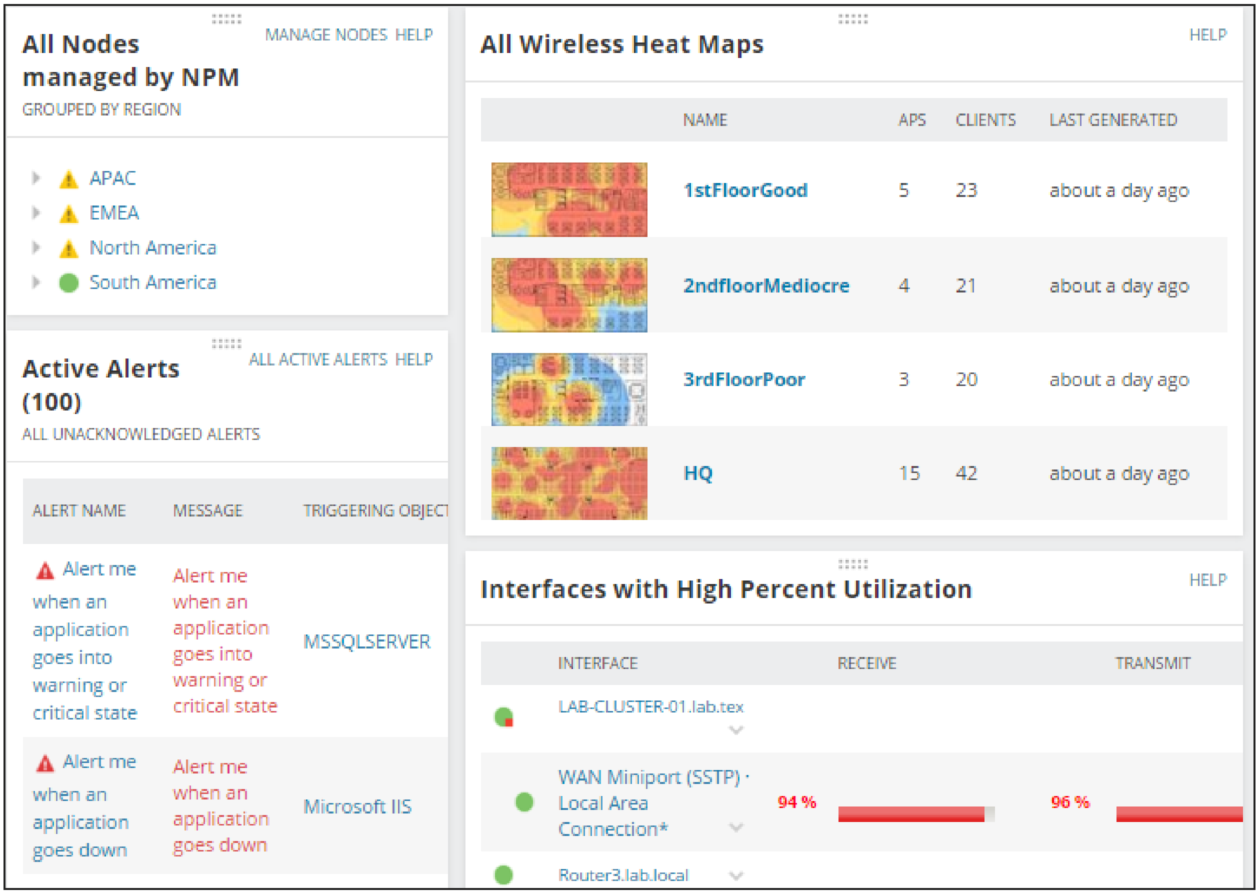
Tabs contain views, which are pages within the Orion Web Console. The Home tab contains views that are common among all Orion modules. The Network tab contains views specific to SolarWinds NPM, for example, Network Top 10.



Top 10 Interfaces by Traffic

NODE		INTERFACE
●	HQESX01	● Device vmnic1 at 01:00.1 bnx2 · 01:00.1
●	BROF-3750-CORE	● GigabitEthernet1/0/47 · Uplink to lab-sw-a9-1, Gi0/12
●	PVDPE2	● GigabitEthernet0/0.2022 · Uplink to DemoLab BOWA
●	PVDPE2	● GigabitEthernet0/1 · MPLS P-Link to PvdPE1, Gi0/1

Views contain resources, which show you the details and statistics of whatever you are monitoring. Views can be customized to include any resources you want. You have hundreds of resources from which to choose.



All Nodes managed by NPM

MANAGE NODES HELP

GROUPED BY REGION

- ⚠ APAC
- ⚠ EMEA
- ⚠ North America
- ● South America

Active Alerts (100)

ALL ACTIVE ALERTS HELP

ALL UNACKNOWLEDGED ALERTS

ALERT NAME	MESSAGE	TRIGGERING OBJECT
⚠ Alert me when an application goes into warning or critical state	Alert me when an application goes into warning or critical state	MSSQLSERVER
⚠ Alert me when an application goes down	Alert me when an application goes down	Microsoft IIS

All Wireless Heat Maps

HELP

	NAME	APS	CLIENTS	LAST GENERATED
	1stFloorGood	5	23	about a day ago
	2ndfloorMediocre	4	21	about a day ago
	3rdFloorPoor	3	20	about a day ago
	HQ	15	42	about a day ago

Interfaces with High Percent Utilization

HELP

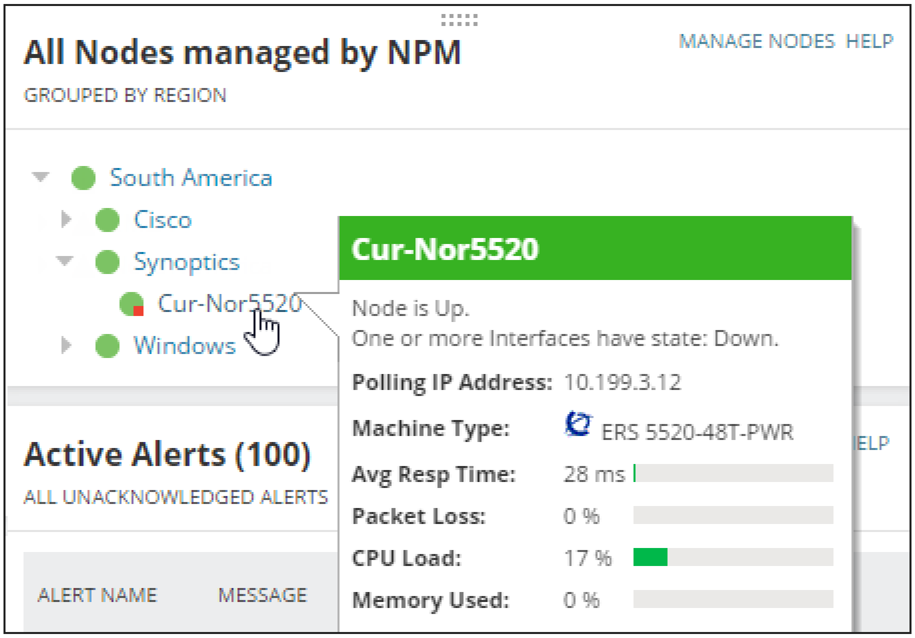
	INTERFACE	RECEIVE	TRANSMIT
●	LAB-CLUSTER-01.lab.tex		
●	WAN Miniport (SSTP) · Local Area Connection*	94 %	96 %
●	Router3.lab.local		

Overview of an element

Within a view, elements that appear in green are up and running, and working as expected. Elements 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 that appears next to the node name. The red square indicates that the system is monitoring a child of that node, for example, an interface.

You can explore a node by placing your cursor over a monitored element to see its details. In this example, one or more interfaces are down.

Check out this video on viewing your devices.



All Nodes managed by NPM

MANAGE NODES HELP

GROUPED BY REGION

- South America
  - Cisco
  - Synoptics
    - Cur-Nor5520
  - Windows

Cur-Nor5520

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

Polling IP Address:	10.199.3.12
Machine Type:	ERS 5520-48T-PWR
Avg Resp Time:	28 ms
Packet Loss:	0 %
CPU Load:	17 %
Memory Used:	0 %

Active Alerts (100)

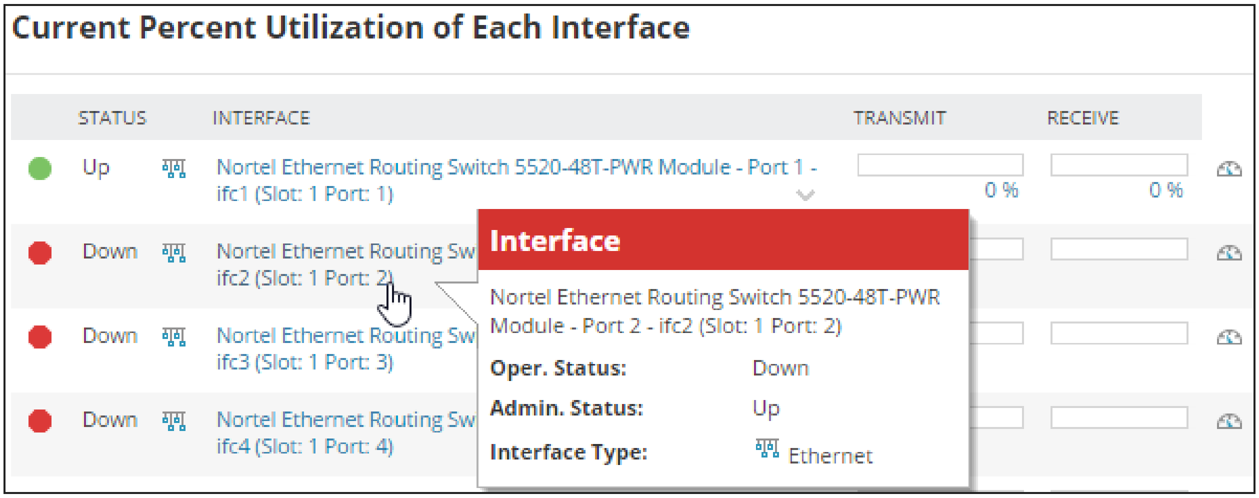
ALL UNACKNOWLEDGED ALERTS

ELP

ALERT NAME	MESSAGE

Details of an element

Elements within a view are dynamically linked so you can drill down and view the details of the element. In this example, the Cur-Nor5520 node was selected on the NPM Summary view, and the Node Details page opens. The Current Percent Utilization of Each Interface resource provides more information about interfaces.



Current Percent Utilization of Each Interface

STATUS	INTERFACE	TRANSMIT	RECEIVE
● Up	Nortel Ethernet Routing Switch 5520-48T-PWR Module - Port 1 - ifc1 (Slot: 1 Port: 1)	0 %	0 %
● Down	Nortel Ethernet Routing Sw ifc2 (Slot: 1 Port: 2)		
● Down	Nortel Ethernet Routing Sw ifc3 (Slot: 1 Port: 3)		
● Down	Nortel Ethernet Routing Sw ifc4 (Slot: 1 Port: 4)		

Interface

Nortel Ethernet Routing Switch 5520-48T-PWR Module - Port 2 - ifc2 (Slot: 1 Port: 2)

Oper. Status:	Down
Admin. Status:	Up
Interface Type:	Ethernet

Identify and troubleshoot a node that has a problem

Before you begin:

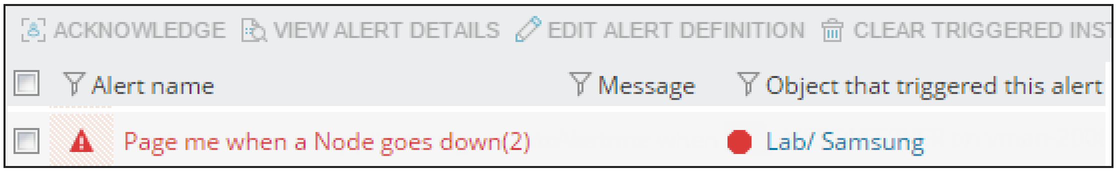
- Add discovered devices to SolarWinds Orion
- Allow SolarWinds NPM to monitor the devices long enough to collect data.

> ⓘ 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

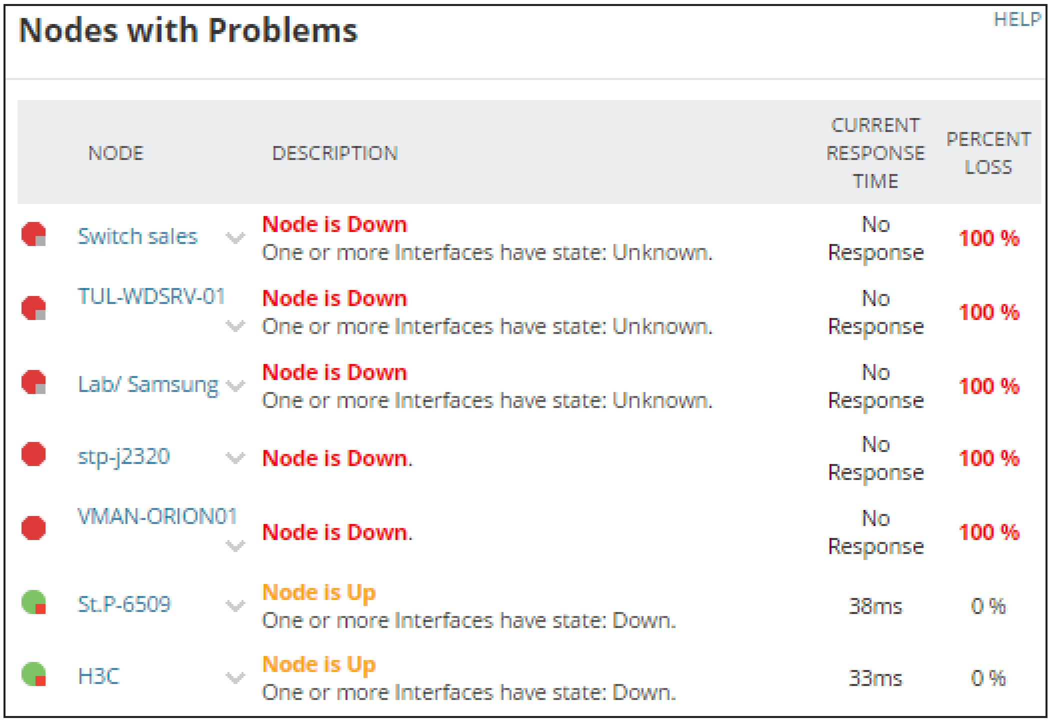
The easiest way to identify a problem is to have an alert notify you. Some alerts are enabled by default. You can enable additional alerts described later in this guide.

The Node down alert is enabled by default. Therefore, if a node goes down (that is, it does not respond to a ping), you will see it immediately in the Active Alerts resource 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 resources as red (down) or yellow (warning).

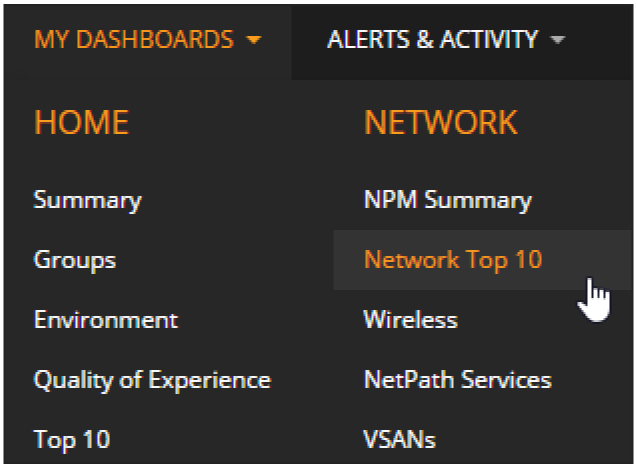


Nodes with Problems

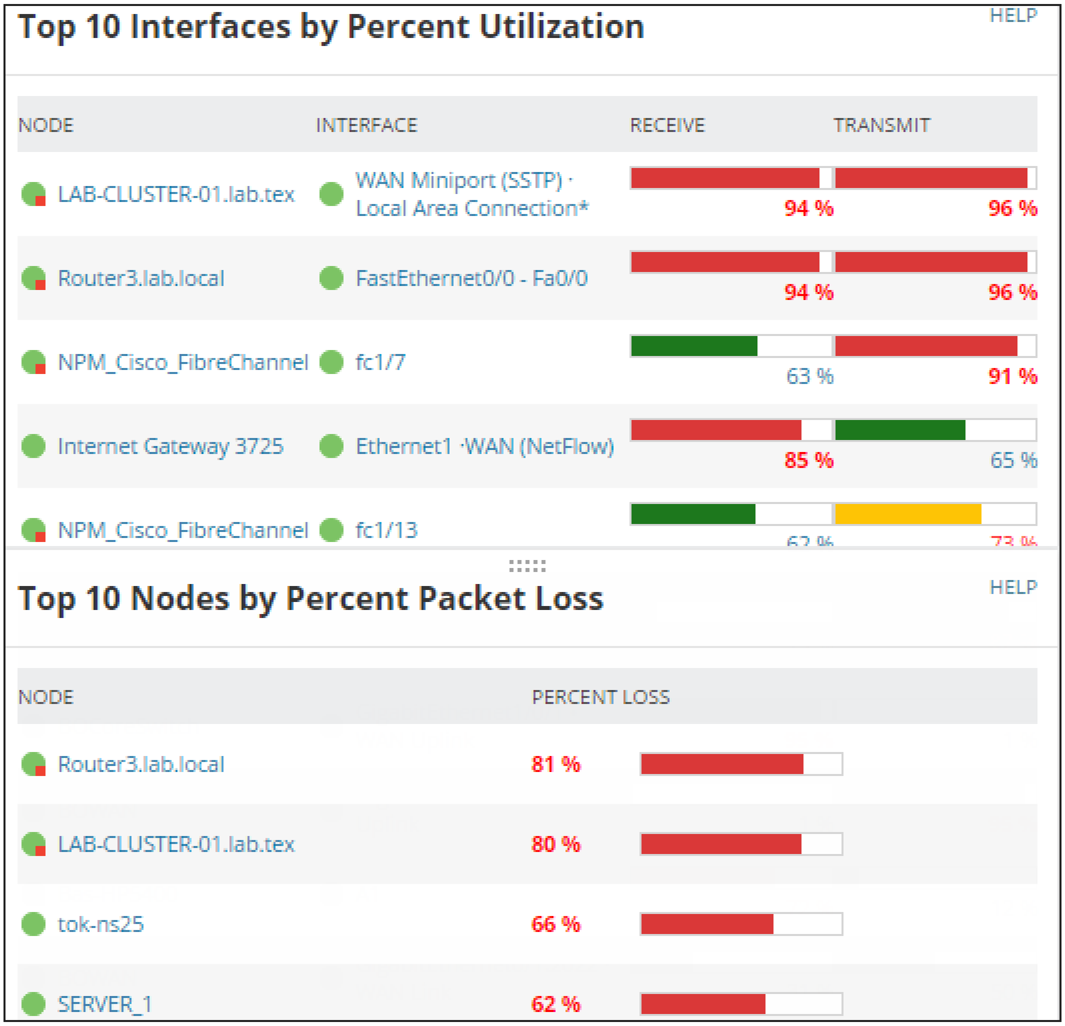
	NODE	DESCRIPTION	CURRENT RESPONSE TIME	PERCENT LOSS
●	Switch sales	Node is Down One or more Interfaces have state: Unknown.	No Response	100 %
●	TUL-WDSRV-01	Node is Down One or more Interfaces have state: Unknown.	No Response	100 %
●	Lab/ Samsung	Node is Down One or more Interfaces have state: Unknown.	No Response	100 %
●	stp-j2320	Node is Down.	No Response	100 %
●	VMAN-ORION01	Node is Down.	No Response	100 %
●	St.P-6509	Node is Up One or more Interfaces have state: Down.	38ms	0 %
●	H3C	Node is Up One or more Interfaces have state: Down.	33ms	0 %

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

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



The resources 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
LAB-CLUSTER-01.lab.tex	WAN Miniport (SSTP) · Local Area Connection*	94 %	96 %
Router3.lab.local	FastEthernet0/0 - Fa0/0	94 %	96 %
NPM_Cisco_FibreChannel	fc1/7	63 %	91 %
Internet Gateway 3725	Ethernet1 ·WAN (NetFlow)	85 %	65 %
NPM_Cisco_FibreChannel	fc1/13	62 %	73 %

Top 10 Nodes by Percent Packet Loss

HELP

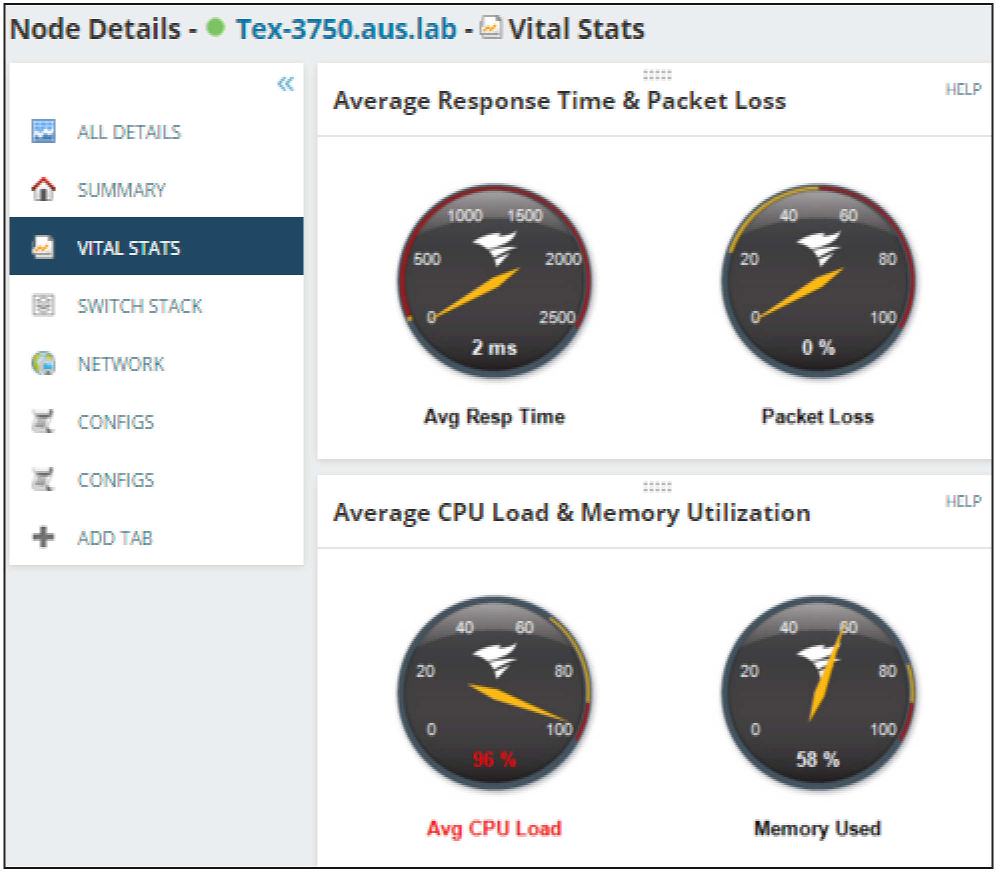
NODE	PERCENT LOSS
Router3.lab.local	81 %
LAB-CLUSTER-01.lab.tex	80 %
tok-ns25	66 %
SERVER_1	62 %

Step 2: Get more details about the node

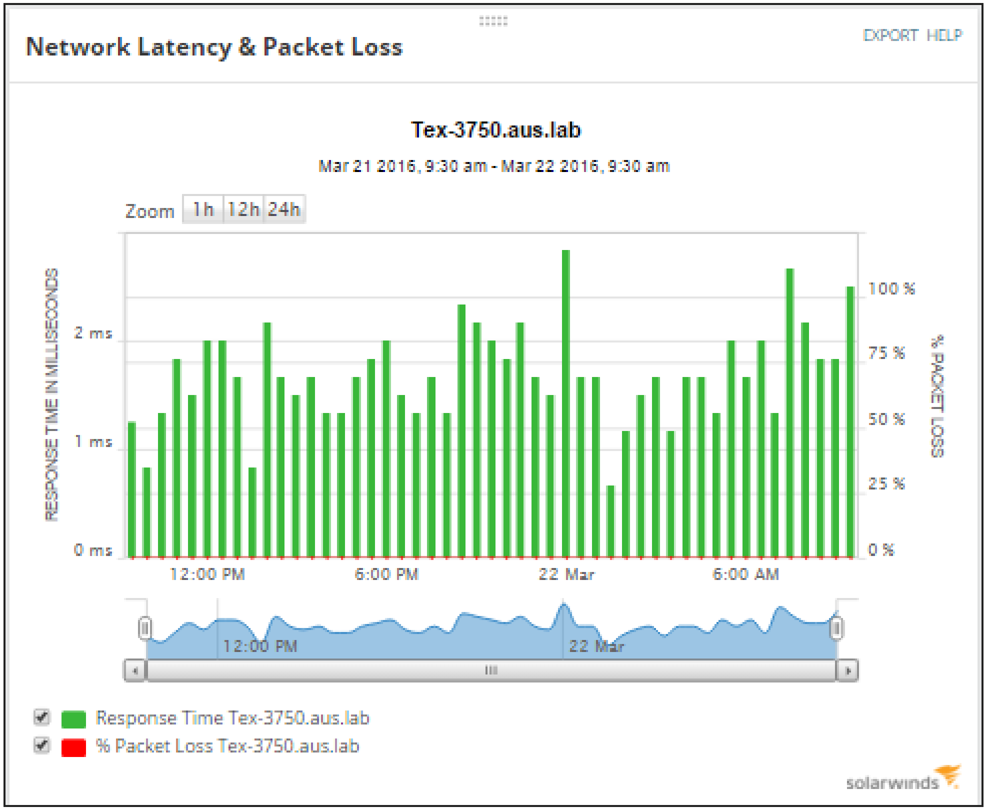
When you find a node with a problem, click the node name in any resource to open the Node Details page.

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

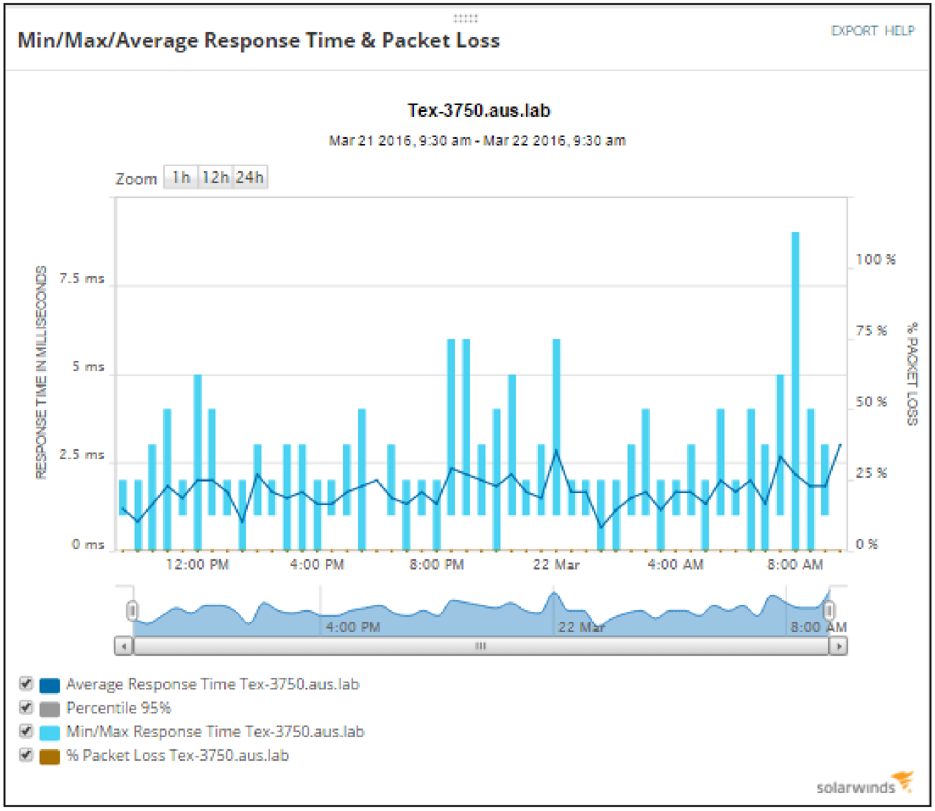
1. Check the power. Is it plugged in?
2. Check the LAN link light. Is it connected to the network?
3. Log in to the device and begin troubleshooting it.
   If a node responds to a ping but shows signs of health or performance issues, use the information on the Node Details page to help troubleshoot.
   - Check the Response Time, Packet Loss, CPU load, and Memory Utilization. Usually, those statistics are the first indicators of a problem. In our example, the CPU load on this node is high.



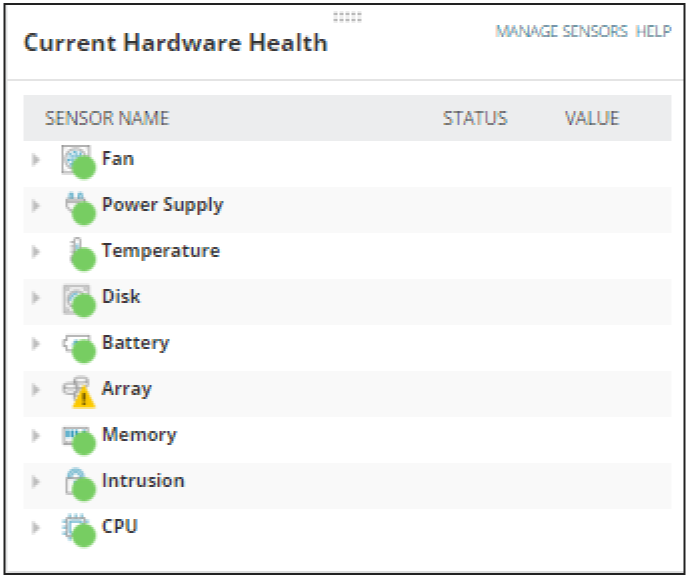
- Use the Network Latency & Packet Loss, as well as the Min/Max/Average Response Time resources to see if this is a momentary problem or a continuing issue.


Network Latency & Packet Loss
EXPORT HELP
Tex-3750.aus.lab
Mar 21 2016, 9:30 am - Mar 22 2016, 9:30 am
Zoom 1h 12h 24h
RESPONSE TIME IN MILLISECONDS
2 ms
1 ms
0 ms
100 %
75 %
50 %
25 %
0 %
% PACKET LOSS
12:00 PM
6:00 PM
22 Mar
6:00 AM
12:00 PM
22 Mar
☑ 🟩 Response Time Tex-3750.aus.lab
☑ 🟥 % Packet Loss Tex-3750.aus.lab
solarwinds

Min/Max/Average Response Time & Packet Loss


Min/Max/Average Response Time & Packet Loss
EXPORT HELP
Tex-3750.aus.lab
Mar 21 2016, 9:30 am - Mar 22 2016, 9:30 am
Zoom 1h 12h 24h
RESPONSE TIME IN MILLISECONDS
7.5 ms
5 ms
2.5 ms
0 ms
100 %
75 %
50 %
25 %
0 %
% PACKET LOSS
12:00 PM
4:00 PM
8:00 PM
22 Mar
4:00 AM
8:00 AM
4:00 PM
22 Mar
8:00 AM
☑ Average Response Time Tex-3750.aus.lab
☑ Percentile 95%
☑ Min/Max Response Time Tex-3750.aus.lab
☑ % Packet Loss Tex-3750.aus.lab
solarwinds

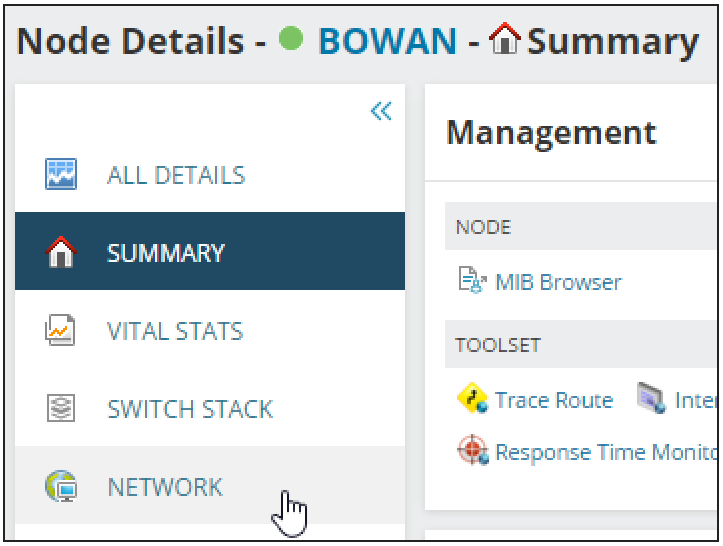
- Depending on what type of node you are monitoring, you may see additional resources specific to that type of device. For example:
  Hardware health: Reports on physical elements of the hardware for Cisco, Dell, F5, HP, and Juniper.



Current Hardware Health

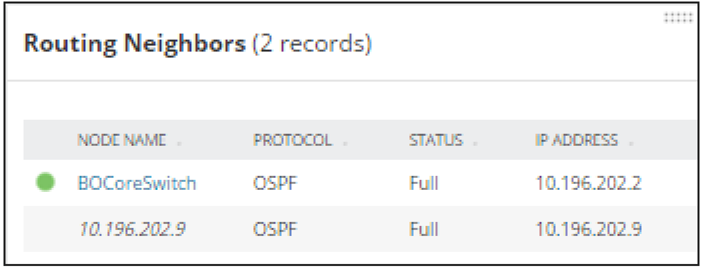
SENSOR NAME	STATUS	VALUE
Fan		
Power Supply		
Temperature		
Disk		
Battery		
Array		
Memory		
Intrusion		
CPU		

Routing table information: For routers and switches, multiple resources show a variety of route-related information. Look under the Network subview for these resources.



Node Details - ● BOWAN - Summary

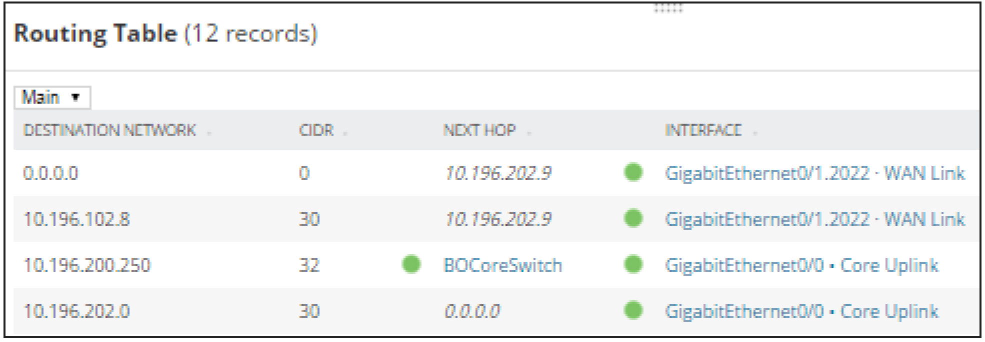
Routing Neighbors



Routing Neighbors (2 records)

	NODE NAME	PROTOCOL	STATUS	IP ADDRESS
●	BOCoreSwitch	OSPF	Full	10.196.202.2
	10.196.202.9	OSPF	Full	10.196.202.9

Routing Table

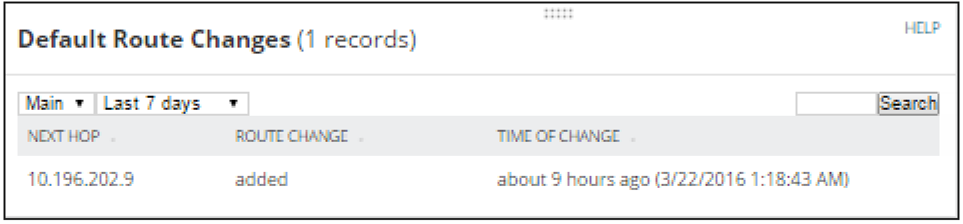


Routing Table (12 records)

Main ▾

DESTINATION NETWORK	CIDR	NEXT HOP	INTERFACE
0.0.0.0	0	*10.196.202.9*	● GigabitEthernet0/1.2022 · WAN Link
10.196.102.8	30	*10.196.202.9*	● GigabitEthernet0/1.2022 · WAN Link
10.196.200.250	32	● BOCoreSwitch	● GigabitEthernet0/0 • Core Uplink
10.196.202.0	30	*0.0.0.0*	● GigabitEthernet0/0 • Core Uplink

Default Route Changes

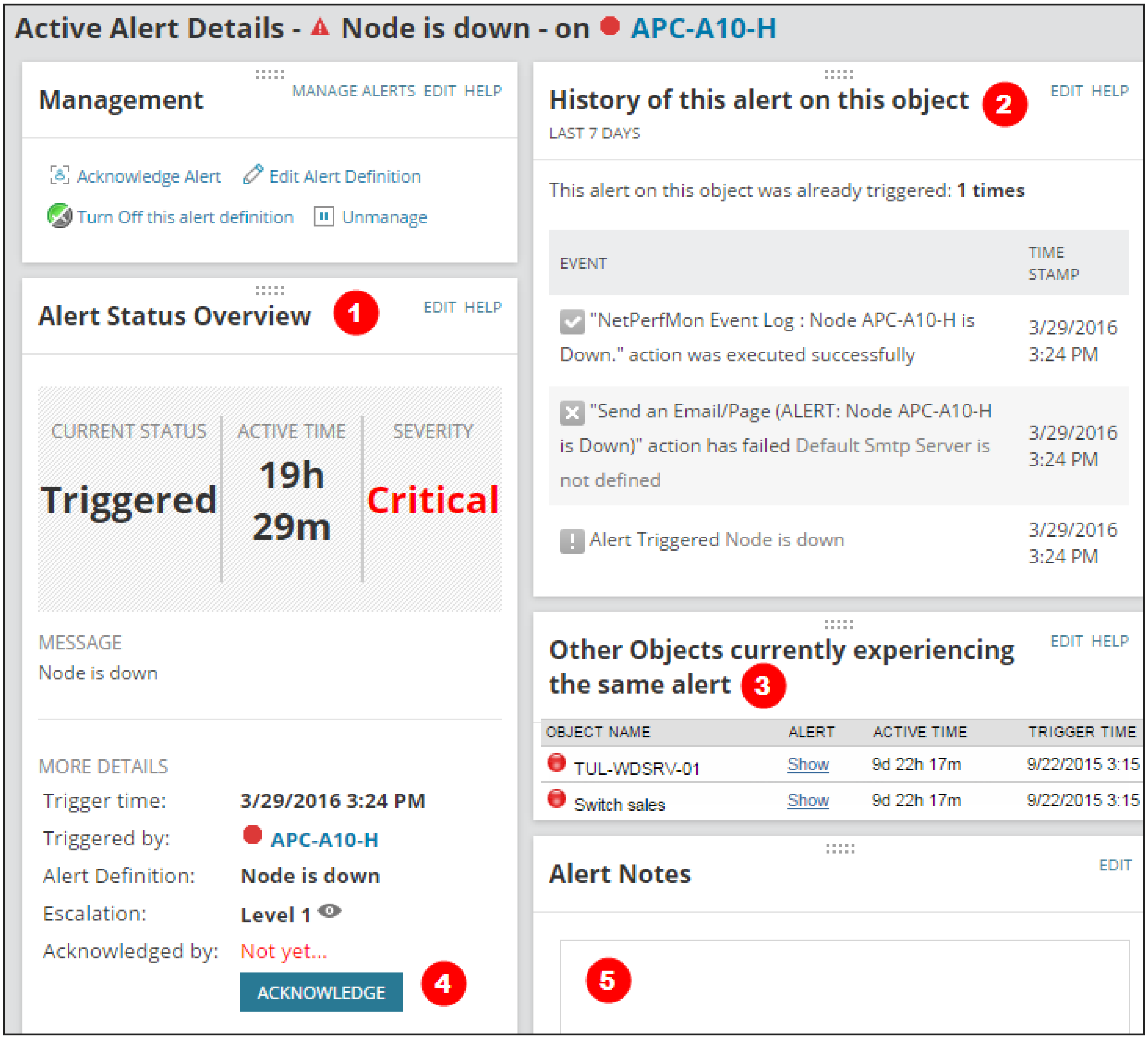


Default Route Changes (1 records)

NEXT HOP	ROUTE CHANGE	TIME OF CHANGE
10.196.202.9	added	about 9 hours ago (3/22/2016 1:18:43 AM)

Step 3: Get more details about the alert

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



Active Alert Details - ⚠ Node is down - on ● APC-A10-H

Management MANAGE ALERTS EDIT HELP

Acknowledge Alert · Edit Alert Definition · Turn Off this alert definition · Unmanage

Alert Status Overview 1 EDIT HELP

CURRENT STATUS	ACTIVE TIME	SEVERITY
Triggered	19h 29m	Critical

MESSAGE
Node is down

MORE DETAILS

Trigger time:	3/29/2016 3:24 PM
Triggered by:	● APC-A10-H
Alert Definition:	Node is down
Escalation:	Level 1
Acknowledged by:	Not yet...

ACKNOWLEDGE 4

History of this alert on this object 2 EDIT HELP
LAST 7 DAYS

This alert on this object was already triggered: **1 times**

EVENT	TIME STAMP
✓ "NetPerfMon Event Log : Node APC-A10-H is Down." action was executed successfully	3/29/2016 3:24 PM
☒ "Send an Email/Page (ALERT: Node APC-A10-H is Down)" action has failed Default Smtp Server is not defined	3/29/2016 3:24 PM
! Alert Triggered Node is down	3/29/2016 3:24 PM

Other Objects currently experiencing the same alert 3 EDIT HELP

OBJECT NAME	ALERT	ACTIVE TIME	TRIGGER TIME
● TUL-WDSRV-01	Show	9d 22h 17m	9/22/2015 3:15
● Switch sales	Show	9d 22h 17m	9/22/2015 3:15

Alert Notes EDIT

5

1	**Alert Status Overview**: Tells you when the alert happened, its importance, and whether or not it was acknowledged.
2	**History**: If the same alert is triggered repeatedly, there may be a systemic problem. For example, if a device frequently goes up and down, it may be a sign of a flapping route.
3	**Other Objects**: Sometimes the same alerts occur on multiple nodes because of a single trigger. For example, if an edge device is having problems, any devices that are dependent on the edge device might also report problems.

4	**Acknowledge**: Acknowledging an alert indicates that you are aware of the issue and the problem is being investigated.
5	**Alert Notes**: Each person troubleshooting an issue can enter notes about their activities and any discoveries. The Acknowledge and Notes features are helpful when multiple people are troubleshooting a problem.

Identify and troubleshoot an interface that has a problem

Before you begin:

- Add discovered devices to SolarWinds Orion
- Monitor one or more interfaces on at least one device. Allow SolarWinds NPM to monitor the devices long enough to collect data.

> ⓘ 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.

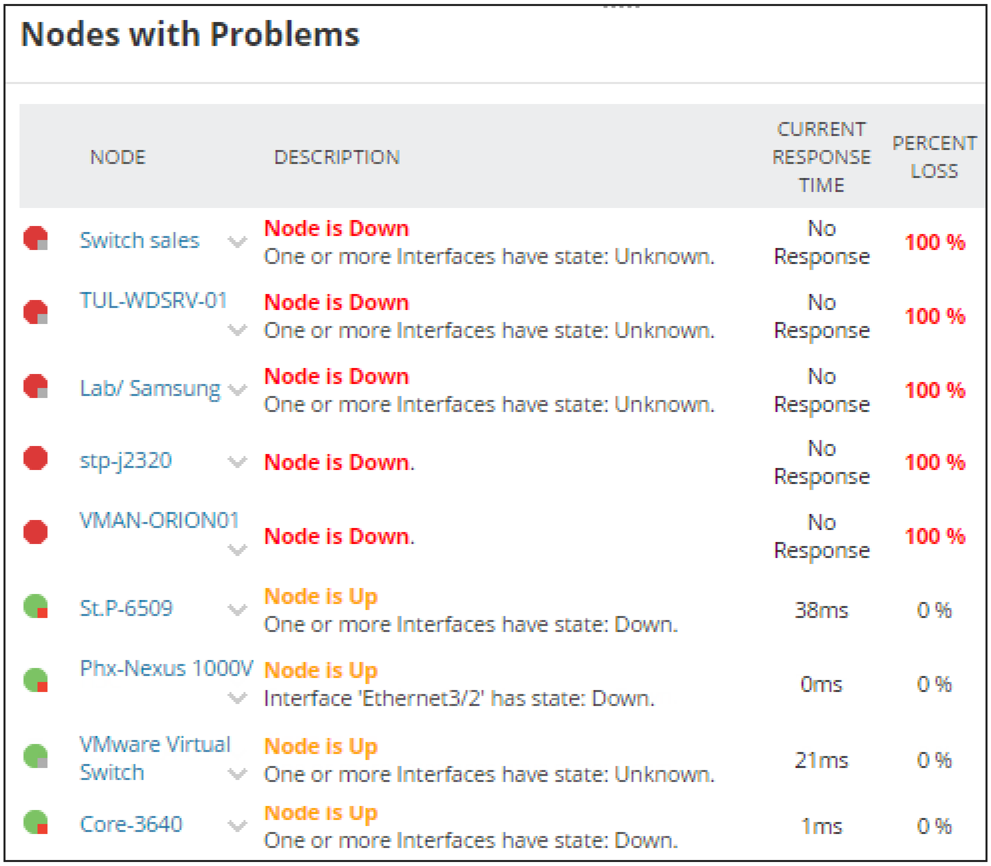
Step 1: Determine there is a problem

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 resource 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

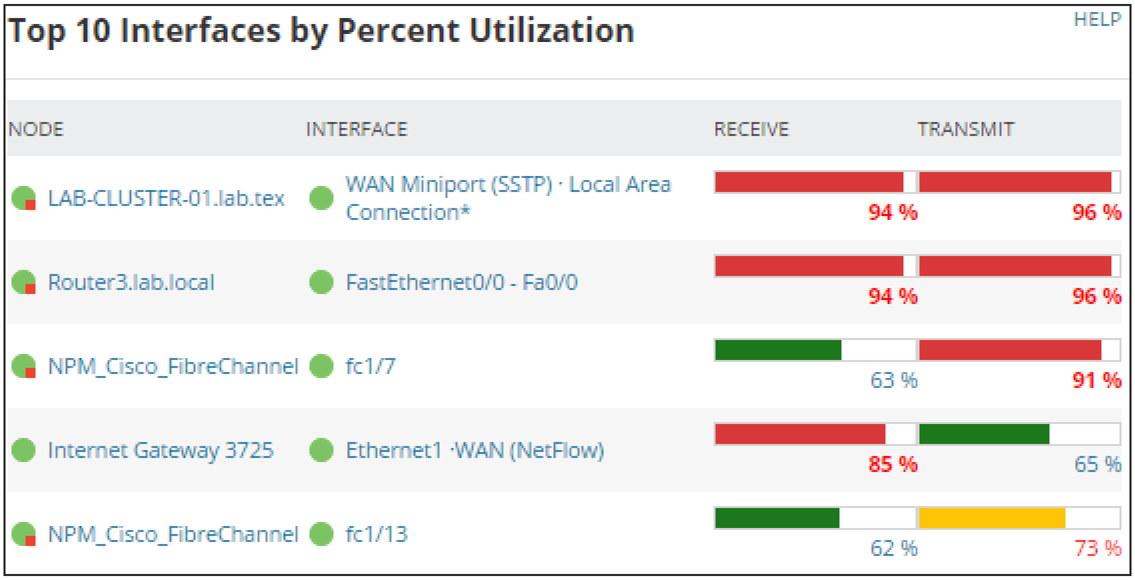
	NODE	DESCRIPTION	CURRENT RESPONSE TIME	PERCENT LOSS
●	Switch sales	Node is Down One or more Interfaces have state: Unknown.	No Response	100 %
●	TUL-WDSRV-01	Node is Down One or more Interfaces have state: Unknown.	No Response	100 %
●	Lab/ Samsung	Node is Down One or more Interfaces have state: Unknown.	No Response	100 %
●	stp-j2320	Node is Down.	No Response	100 %
●	VMAN-ORION01	Node is Down.	No Response	100 %
●	St.P-6509	Node is Up One or more Interfaces have state: Down.	38ms	0 %
●	Phx-Nexus 1000V	Node is Up Interface 'Ethernet3/2' has state: Down.	0ms	0 %
●	VMware Virtual Switch	Node is Up One or more Interfaces have state: Unknown.	21ms	0 %
●	Core-3640	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 resources on this page.

Top 10 Interfaces by Percent Utilization

This resource 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.



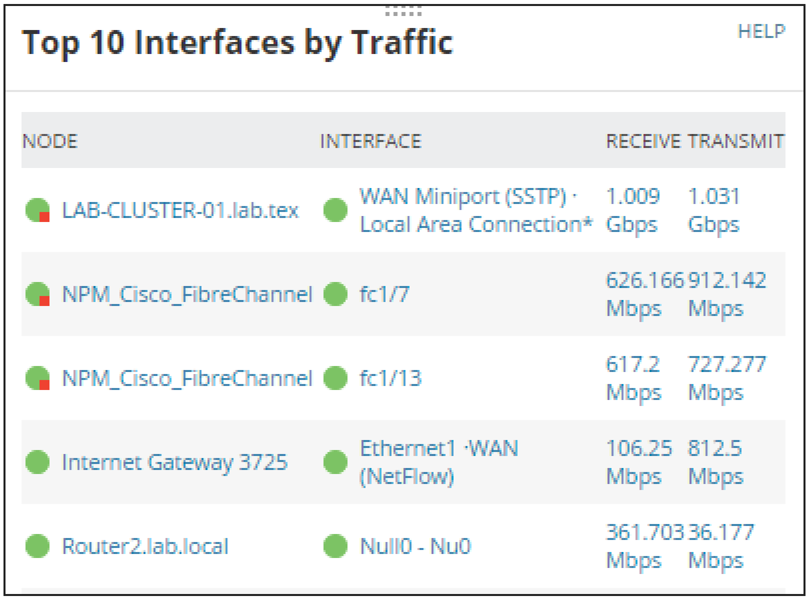
Top 10 Interfaces by Percent Utilization

HELP

NODE	INTERFACE	RECEIVE	TRANSMIT
LAB-CLUSTER-01.lab.tex	WAN Miniport (SSTP) · Local Area Connection*	94 %	96 %
Router3.lab.local	FastEthernet0/0 - Fa0/0	94 %	96 %
NPM_Cisco_FibreChannel	fc1/7	63 %	91 %
Internet Gateway 3725	Ethernet1 ·WAN (NetFlow)	85 %	65 %
NPM_Cisco_FibreChannel	fc1/13	62 %	73 %

Top 10 Interfaces by Traffic

This resource 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

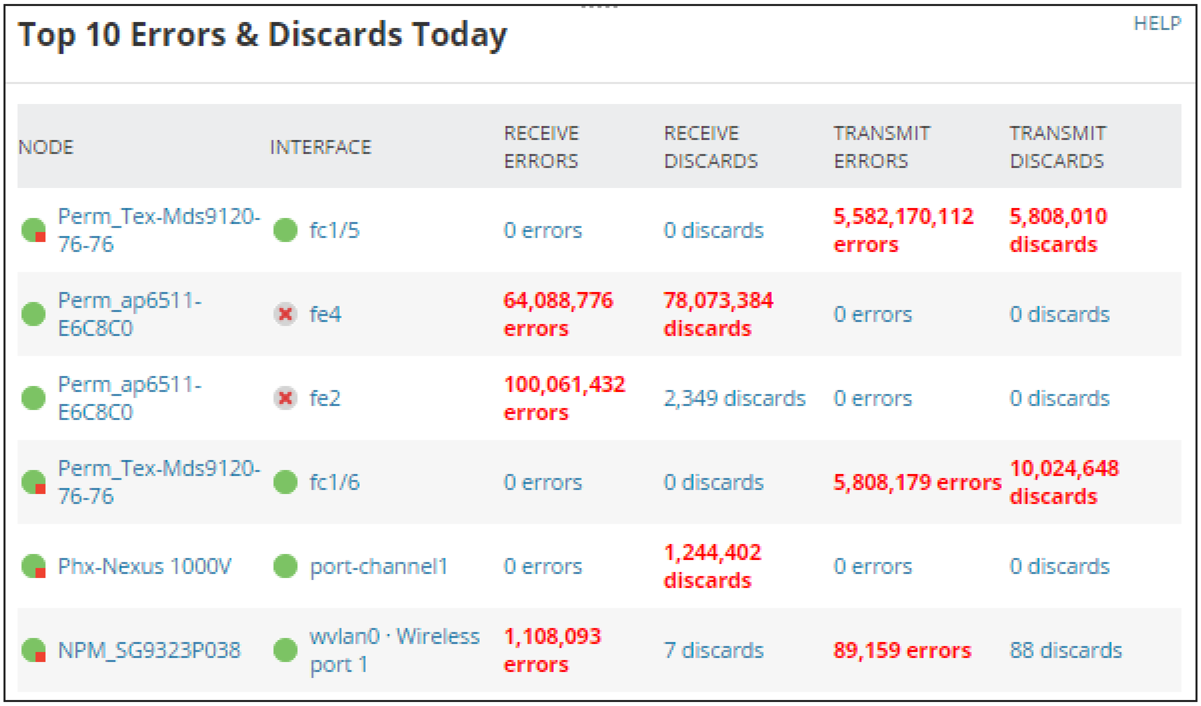
HELP

NODE	INTERFACE	RECEIVE	TRANSMIT
LAB-CLUSTER-01.lab.tex	WAN Miniport (SSTP) · Local Area Connection*	1.009 Gbps	1.031 Gbps
NPM_Cisco_FibreChannel	fc1/7	626.166 Mbps	912.142 Mbps
NPM_Cisco_FibreChannel	fc1/13	617.2 Mbps	727.277 Mbps
Internet Gateway 3725	Ethernet1 ·WAN (NetFlow)	106.25 Mbps	812.5 Mbps
Router2.lab.local	Null0 - Nu0	361.703 Mbps	36.177 Mbps

Top 10 Errors & Discards Today

This resource 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

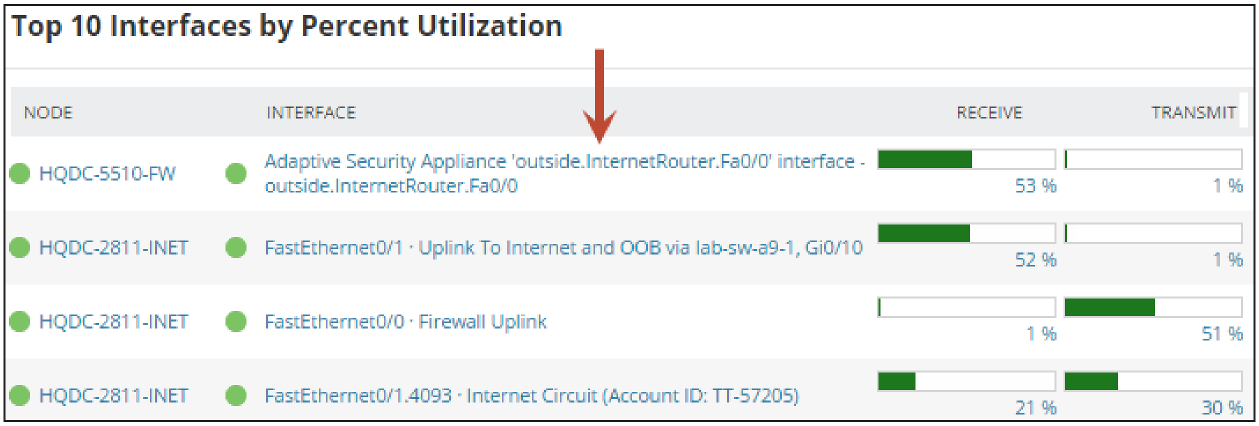
NODE	INTERFACE	RECEIVE ERRORS	RECEIVE DISCARDS	TRANSMIT ERRORS	TRANSMIT DISCARDS
● Perm_Tex-Mds9120-76-76	● fc1/5	0 errors	0 discards	5,582,170,112 errors	5,808,010 discards
● Perm_ap6511-E6C8C0	✖ fe4	64,088,776 errors	78,073,384 discards	0 errors	0 discards
● Perm_ap6511-E6C8C0	✖ fe2	100,061,432 errors	2,349 discards	0 errors	0 discards
● Perm_Tex-Mds9120-76-76	● fc1/6	0 errors	0 discards	5,808,179 errors	10,024,648 discards
● Phx-Nexus 1000V	● port-channel1	0 errors	1,244,402 discards	0 errors	0 discards
● NPM_SG9323P038	● 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.

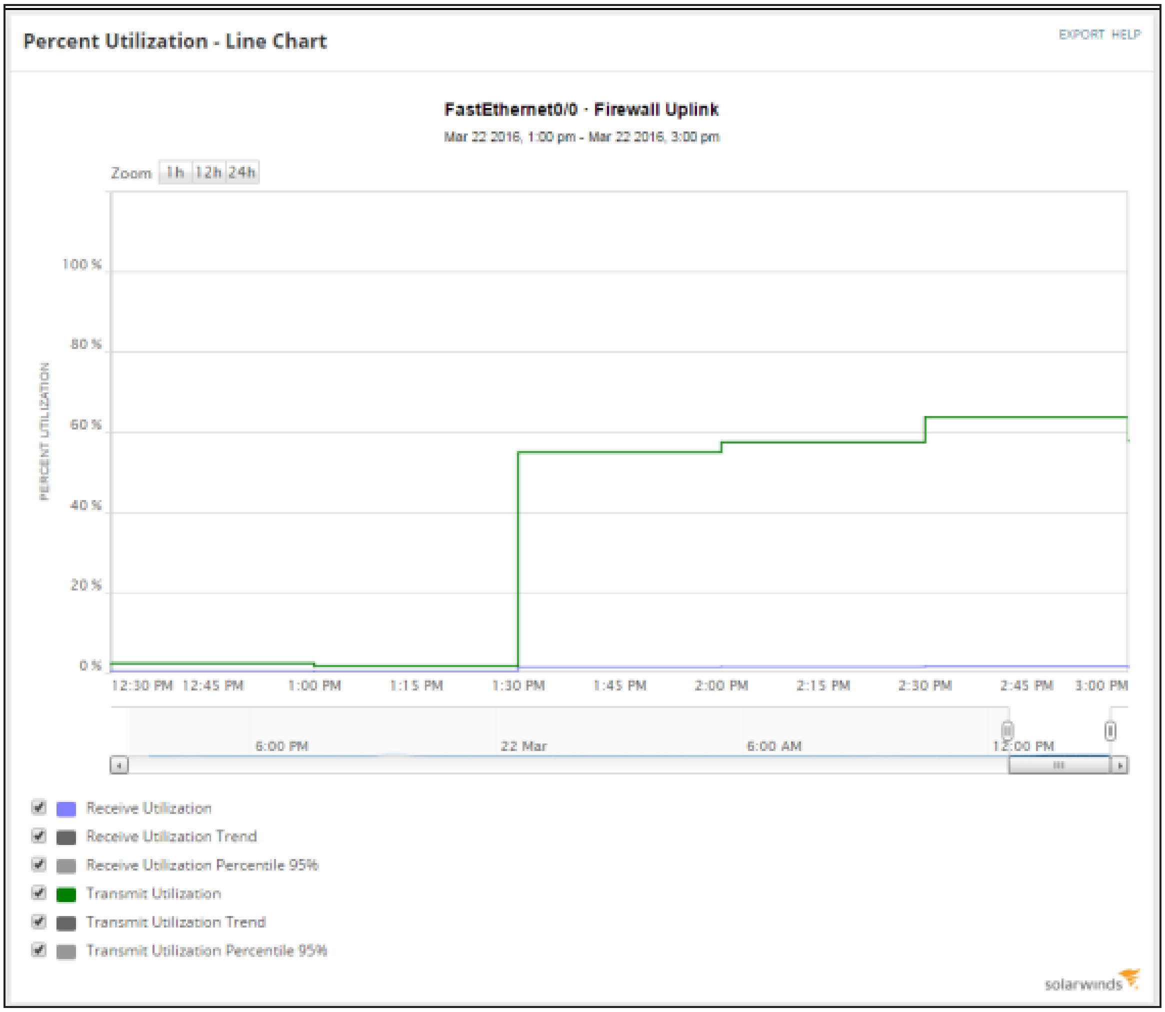
Once you have found an interface with a problem (or, if all your interfaces are healthy, an interface with high utilization, errors, or discards), click the interface name in any resource. The Interface Details page opens.



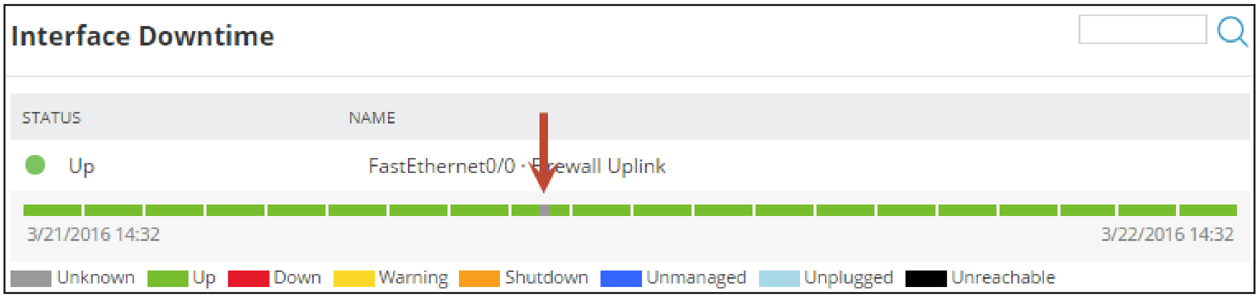
Top 10 Interfaces by Percent Utilization

NODE	INTERFACE	RECEIVE	TRANSMIT
● HQDC-5510-FW	● Adaptive Security Appliance 'outside.InternetRouter.Fa0/0' interface - outside.InternetRouter.Fa0/0	53 %	1 %
● HQDC-2811-INET	● FastEthernet0/1 · Uplink To Internet and OOB via lab-sw-a9-1, Gi0/10	52 %	1 %
● HQDC-2811-INET	● FastEthernet0/0 · Firewall Uplink	1 %	51 %
● HQDC-2811-INET	● FastEthernet0/1.4093 · Internet Circuit (Account ID: TT-57205)	21 %	30 %

- Check the Percent Utilization resource 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 resource displays the interface status for the last 24 hours. If the interface status changed, you can see it in this resource. In the following example, the resource shows that the interface had one period when its status was unknown during the last 24 hours, but it is currently up.



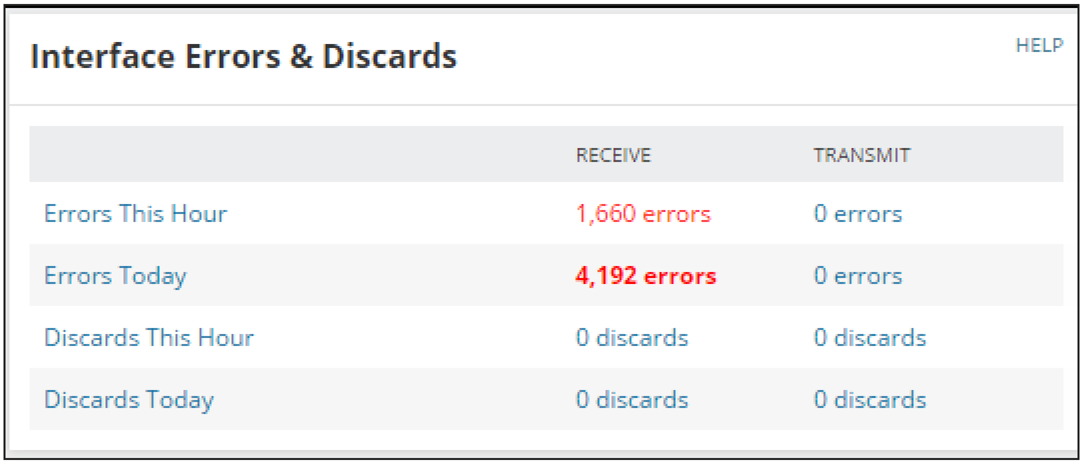
Interface Downtime

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 resource 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.

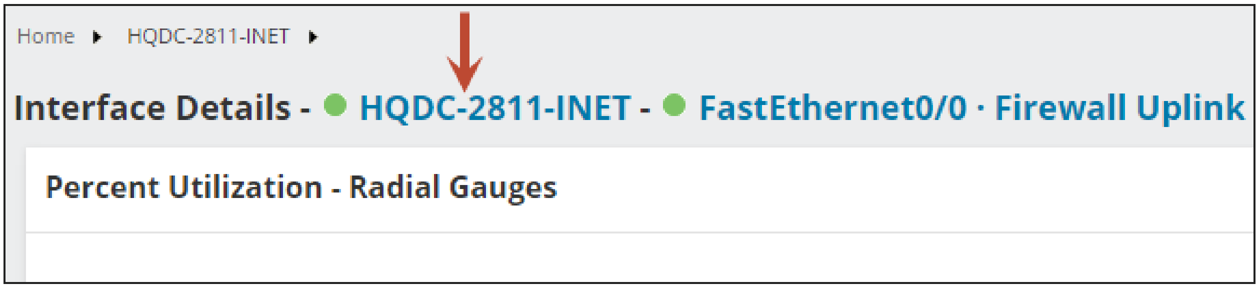


Interface Errors & Discards HELP

	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.



Home ▸ HQDC-2811-INET ▸

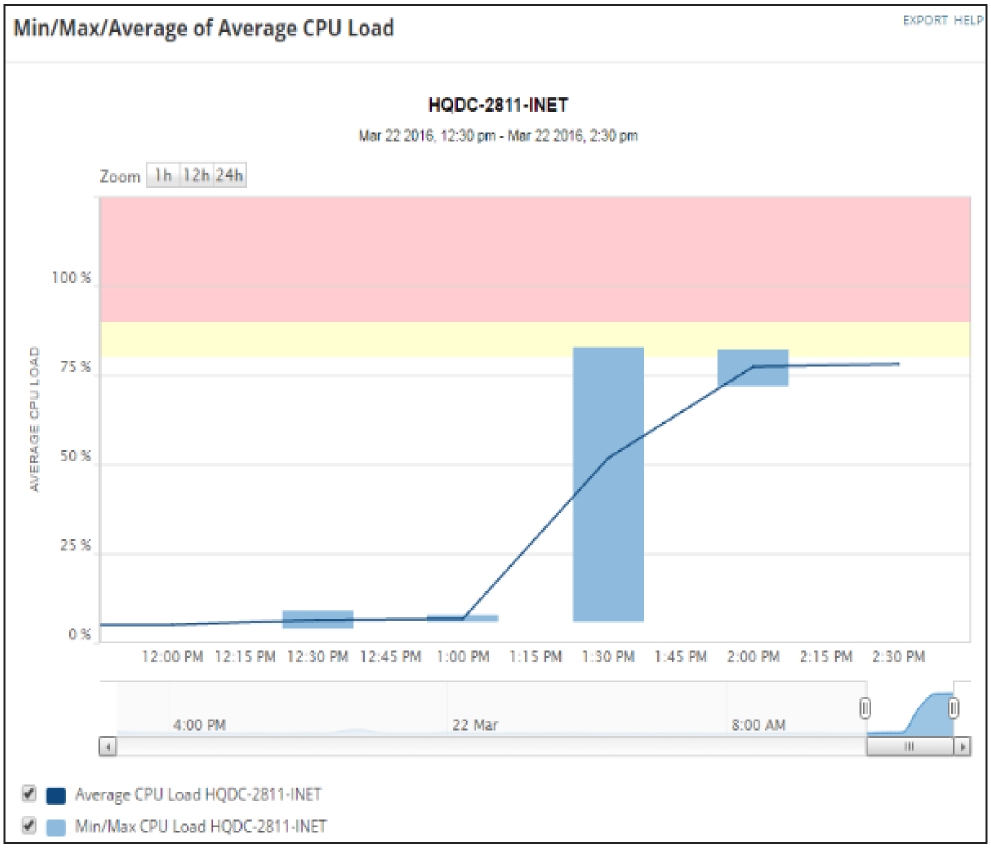
Interface Details - ● HQDC-2811-INET - ● FastEthernet0/0 · Firewall Uplink

Percent Utilization - Radial Gauges

Examine the following resources on this page.

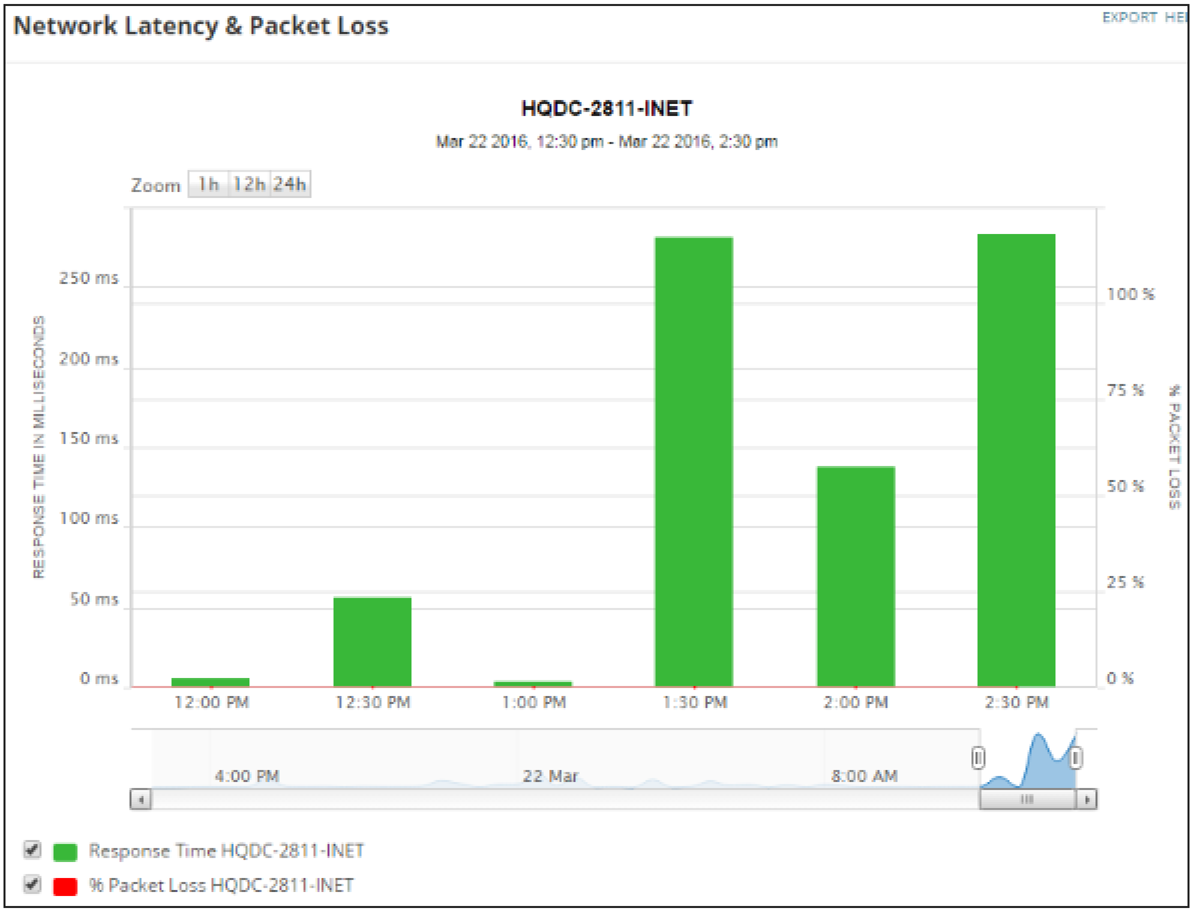
Min/Max/Average Response Time & Packet Loss

This resource 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 resource 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 resources indicate an unknown increase in traffic that occurred at approximately 1:30 PM, leading to higher interface utilization, CPU load, and dropped packets. Since values are not yet critical and no alerts have been triggered, 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 Network Traffic Analyzer), explore the cause of the traffic spike.

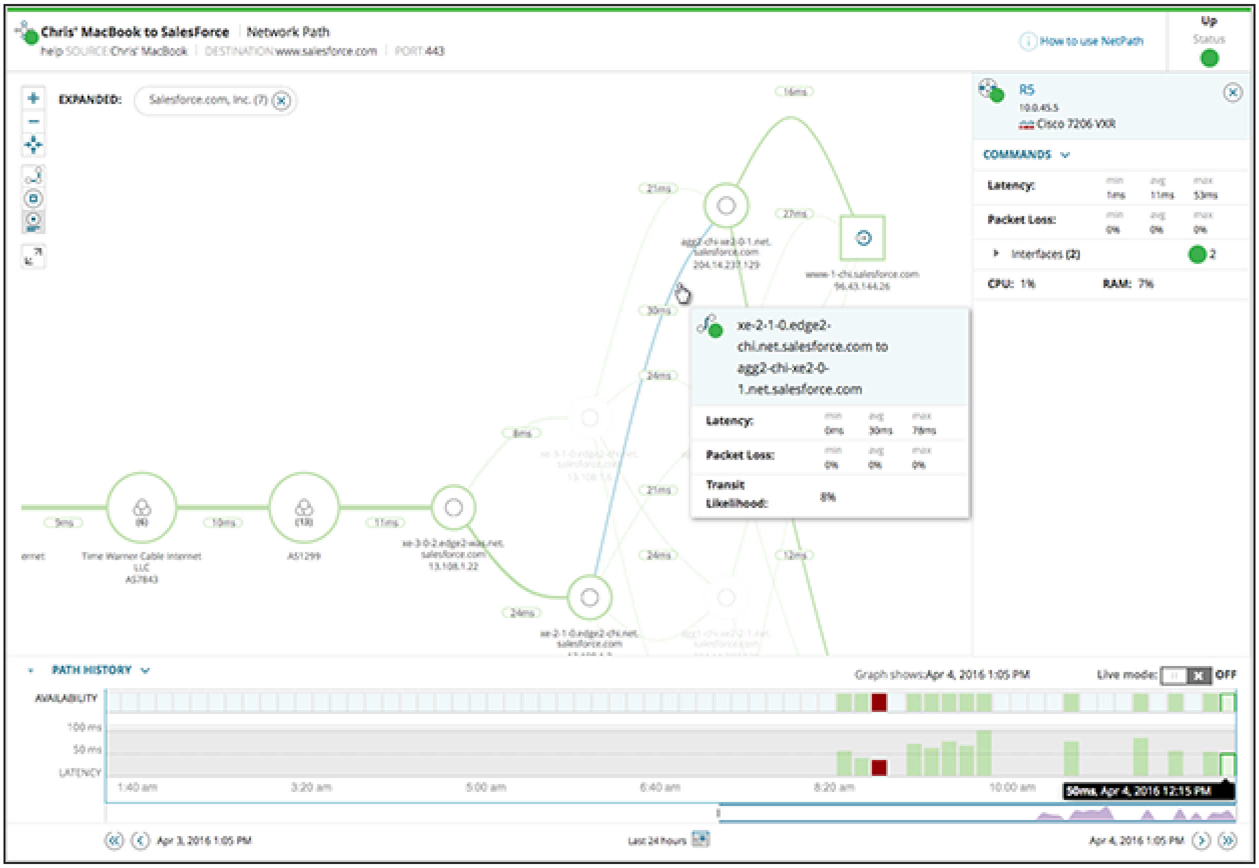
Monitor your network paths

Check out this video on using NetPath™.

Use NetPath™ to discover and troubleshoot network paths node-by-node – not only the part of the network that you manage, but also nodes and links of your providers.

NetPath™:

- Creates a detailed (potentially multi-path) map between a Windows node and a destination you specify.
- Overlays the path with performance metrics and device details of the nodes, interfaces, and connectors it finds.
- Quickly identifies problem areas. Hover over objects to see more details using the Object Inspector, or drill down on managed nodes.


Chris' MacBook to SalesForce
Network Path
help SOURCE Chris' MacBook
DESTINATION www.salesforce.com
PORT 443
How to use NetPath
Up
Status
EXPANDED:
Salesforce.com, Inc. (7)
9ms
10ms
11ms
8ms
16ms
21ms
27ms
30ms
24ms
21ms
24ms
12ms
24ms
ernet
(6)
Time Warner Cable Internet LLC AS7843
(13)
AS1299
xe-3-0-2.edge2-was.net.salesforce.com 13.108.1.22
xe-2-1-0.edge2-chi.net.salesforce.com
agg2-chi-xe2-0-1.net.salesforce.com 204.14.237.129
www-1-chi.salesforce.com 96.43.144.26
xe-3-1-0.edge2-chi.net.salesforce.com 13.108.1.6
agg1-chi-xe2-2-1.net.salesforce.com
PATH HISTORY
Graph shows:Apr 4, 2016 1:05 PM
Live mode: OFF
AVAILABILITY
100 ms
50 ms
LATENCY
1:40 am
3:20 am
5:00 am
6:40 am
8:20 am
10:00 am
50ms, Apr 4, 2016 12:15 PM
Apr 3, 2016 1:05 PM
Last 24 hours
Apr 4, 2016 1:05 PM

R5
10.0.45.5
Cisco 7206 VXR

COMMANDS

	min	avg	max
Latency:	1ms	11ms	53ms
Packet Loss:	0%	0%	0%

Interfaces (2) ● 2

CPU: 1% RAM: 7%

xe-2-1-0.edge2-chi.net.salesforce.com to agg2-chi-xe2-0-1.net.salesforce.com

	min	avg	max
Latency:	0ms	30ms	78ms
Packet Loss:	0%	0%	0%
Transit Likelihood:	8%		

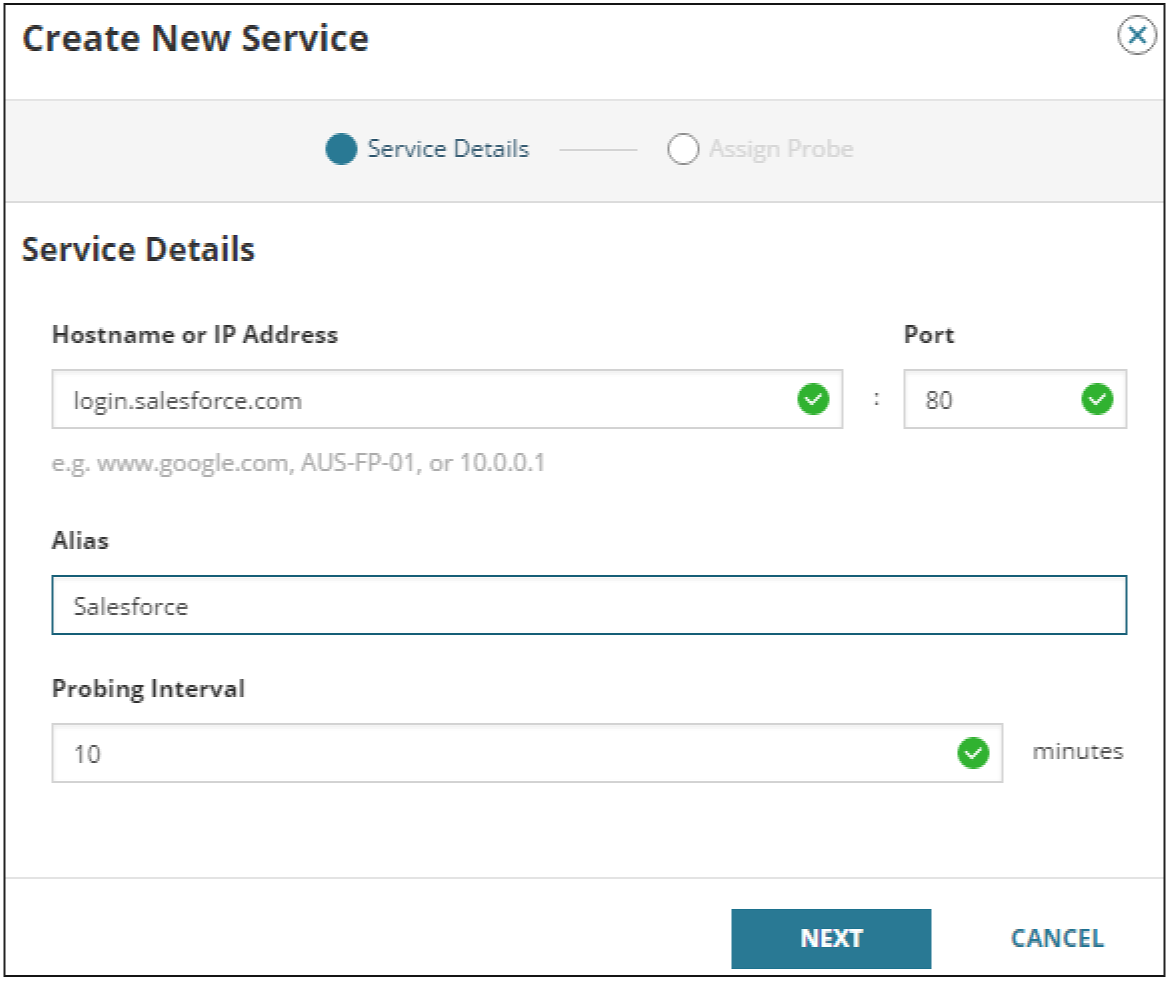
Notes:

- You must open certain ports on your firewall for network connectivity used by NetPath™. For more information, see the "NetPath™ Requirements" section in the SolarWinds Network Performance Monitor Administrator Guide.
- NTA 4.2 and NCM 7.4.1 are the minimum required versions to use the Orion integration features with NetPath™.

Create a NetPath™ service

In this scenario, Salesforce has been slow, and you want to analyze the path to find out where the problem is.

1. Click My Dashboards > Network > NetPath Services.
2. If this is your first time using NetPath™, you'll see an introductory wizard that shows how NetPath™ works. Otherwise, click Create New Service.
3. In the Hostname field, enter `login.salesforce.com`, and in the Port field, enter `80`.
4. Enter `Salesforce` as the alias.
5. Set the Probing Interval to 10 minutes, and click Next.
   Probing frequency determines how often Orion discovers the path and measures the path's performance.



Create New Service

Service Details

Hostname or IP Address: login.salesforce.com

Port: 80

Alias: Salesforce

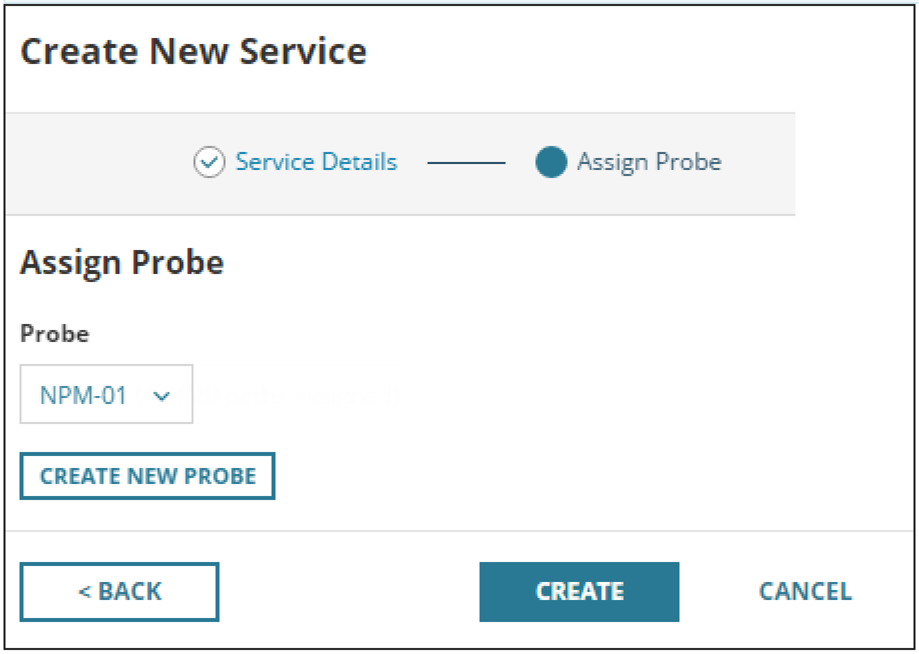
Probing Interval: 10 minutes

6. Assign a probe to the path.
   The Orion main poller includes a probe you can use, or you can add a probe to a Windows device.

7. Click Create.

   It takes the system at least the time specified as the probing interval to map the path.

   > ⓘ For more information on NetPath™, or if you are unable to get NetPath™ working, see the "Discover your network paths" chapter in the SolarWinds Network Performance Monitor 12.0 Administrator Guide.



Create New Service

✓ Service Details —— ● Assign Probe

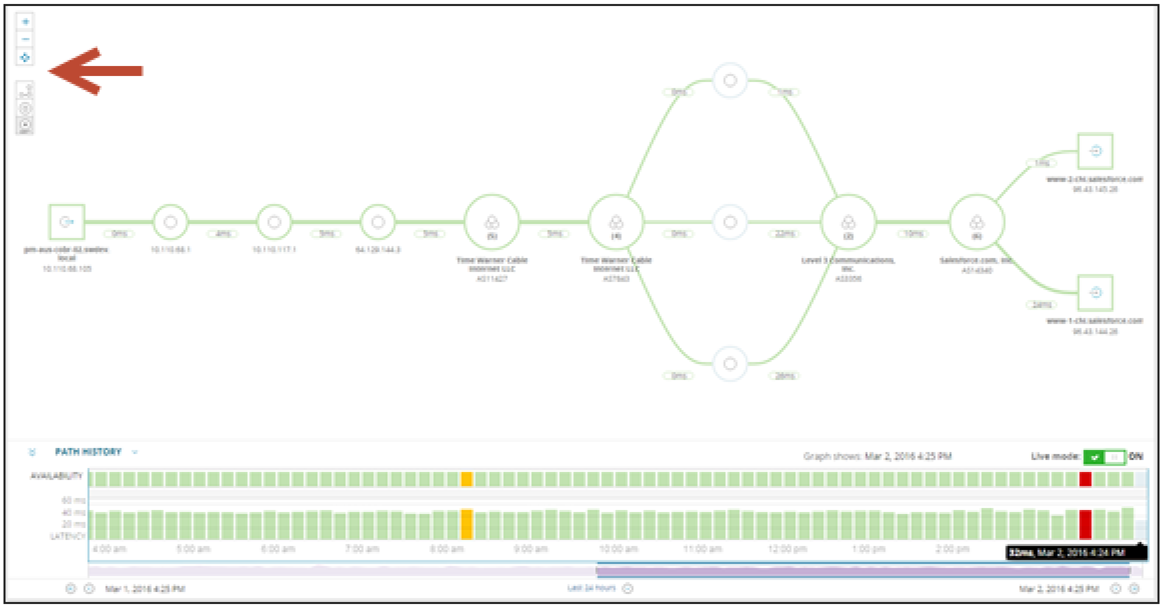
Assign Probe

Probe: NPM-01

Troubleshoot with NetPath™

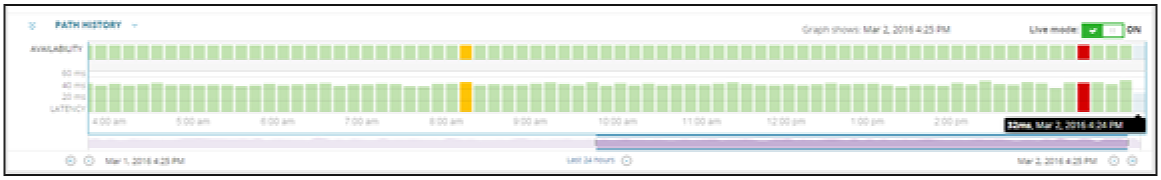
After NetPath™ maps the path, you can see your internal network, traversed segments of ISP networks, and the destination network, plus the details and statuses of the objects on the route.

You can use the controls in the top left of the page to zoom in and out, and to control the level of detail shown. The path between SolarWinds' Austin HQ and Salesforce shows the maximum level of detail.

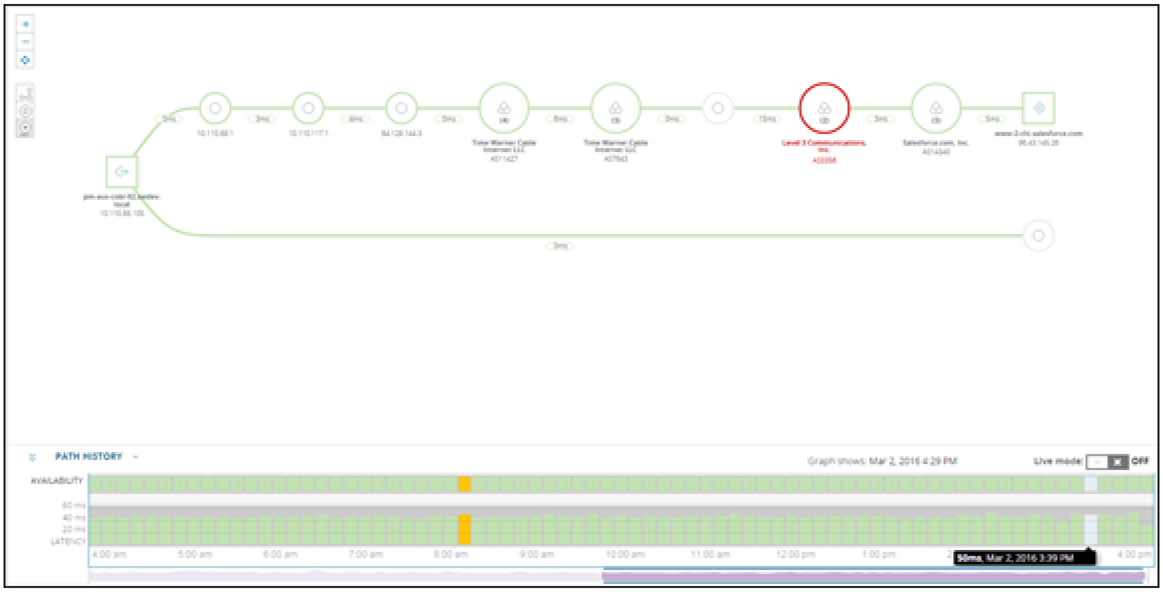


NetPath™ monitors paths at regular intervals (the probing interval) and keeps historical data, which is shown in the Path History section at the bottom of the page. You can see in this example that the path is fine now, but was red a few intervals ago.

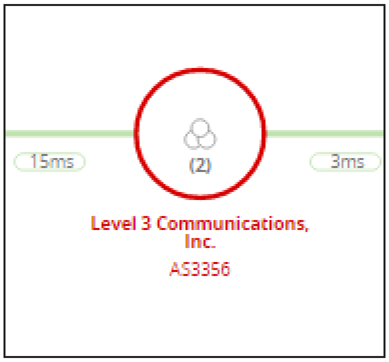
Click the red bar to see the path at that time.



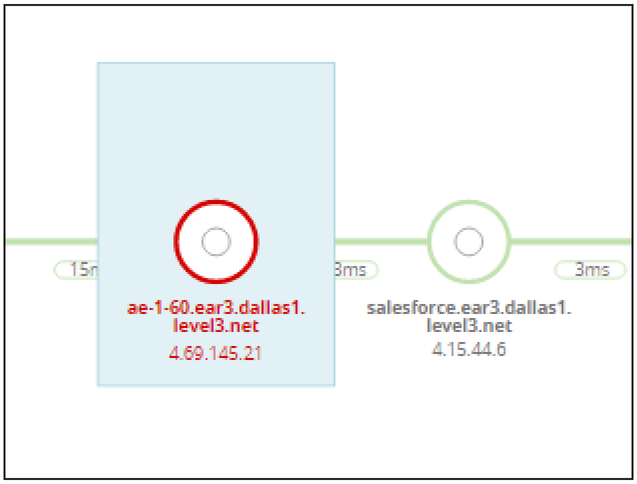
Notice that the path is different during this time period than the current time. That's normal. Paths can and do change over time.



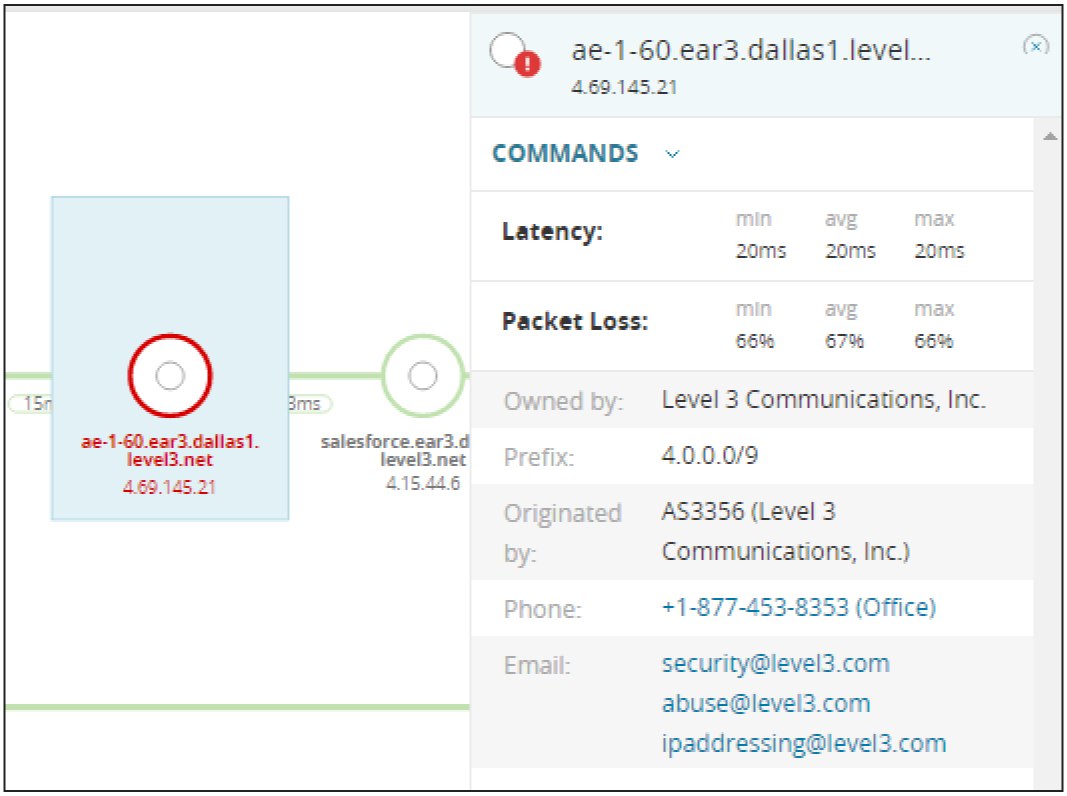
If you look closely at the red object, you can see that it's actually two objects.



Double-click the object to expand it.



If you single-click the individual device that's causing the problem, the Object Inspector opens.



ae-1-60.ear3.dallas1.level...
4.69.145.21

	min	avg	max
Latency:	20ms	20ms	20ms
Packet Loss:	66%	67%	66%

Owned by:	Level 3 Communications, Inc.
Prefix:	4.0.0.0/9
Originated by:	AS3356 (Level 3 Communications, Inc.)
Phone:	+1-877-453-8353 (Office)
Email:	security@level3.com abuse@level3.com ipaddressing@level3.com

It looks like this device had high packet loss during this 10 minute time period, but the problem seems to be resolved. If you had caught this while it was happening, you could use the information in the Object Inspector to contact the device's owner and report the problem. And because NetPath™ keeps a history of each path, you can identify trends over time, and troubleshoot intermittent problems.

Plan to scale monitoring

You installed and configured your Orion product, discovered part of your IT environment, and have monitoring statistics displayed in Orion 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.

Alerts and reports

This section includes information on working with preconfigured alerts and reports:

- How alerts work
- Work with preconfigured alerts
- How reports work
- Run a preconfigured report

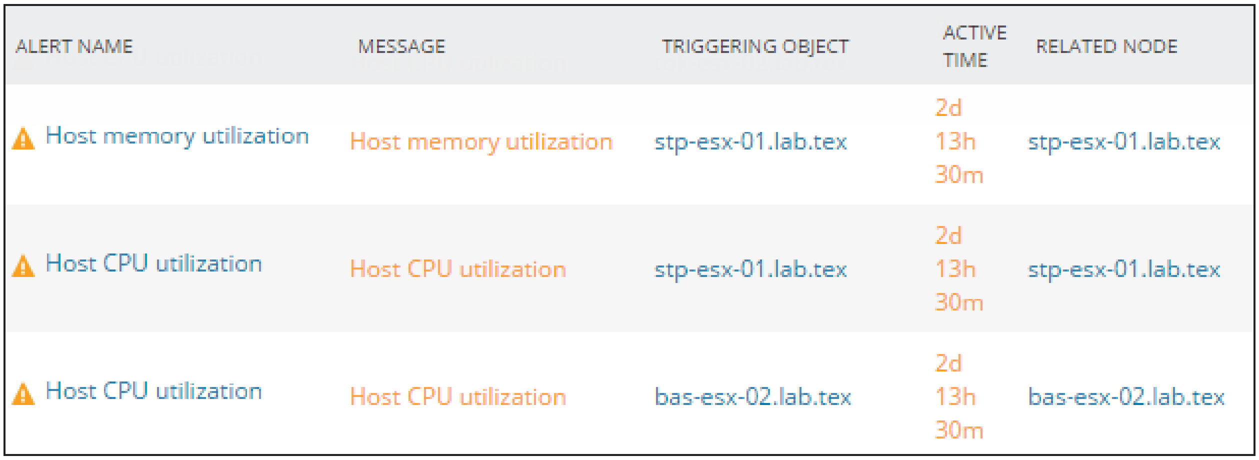
How alerts work

An alert is notification that there is a problem with a monitored element. Orion comes with hundreds of predefined alerts for common problems such as a node or application going down, high interface utilization or packet loss, and many other problems.

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 to SolarWinds Orion.

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

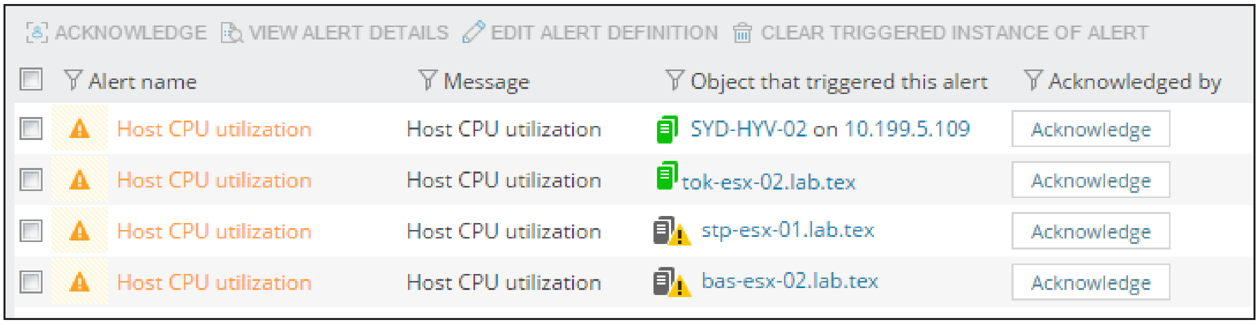
By default, alerts appear in the Active Alerts resource on the Orion Home page.



ALERT NAME	MESSAGE	TRIGGERING OBJECT	ACTIVE TIME	RELATED NODE
⚠ Host memory utilization	Host memory utilization	stp-esx-01.lab.tex	2d 13h 30m	stp-esx-01.lab.tex
⚠ Host CPU utilization	Host CPU utilization	stp-esx-01.lab.tex	2d 13h 30m	stp-esx-01.lab.tex
⚠ Host CPU utilization	Host CPU utilization	bas-esx-02.lab.tex	2d 13h 30m	bas-esx-02.lab.tex

To see all alerts, you can click the All Active Alerts button in the Active Alerts resource, or you can go to Home > 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	SYD-HYV-02 on 10.199.5.109	Acknowledge
☐	⚠	Host CPU utilization	Host CPU utilization	tok-esx-02.lab.tex	Acknowledge
☐	⚠	Host CPU utilization	Host CPU utilization	stp-esx-01.lab.tex	Acknowledge
☐	⚠	Host CPU utilization	Host CPU utilization	bas-esx-02.lab.tex	Acknowledge

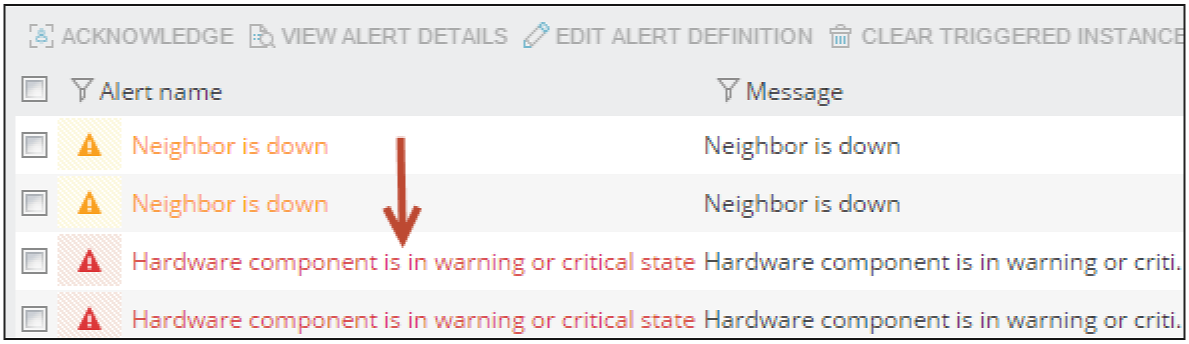
You can create your own alerts, either by modifying a predefined alert, or by creating a custom alert. Alerting is very powerful and can be complex, with multiple trigger conditions, reset conditions, and actions. The trigger condition defines the event that must occur to activate an alert. Trigger conditions are built using child conditions, which are evaluated in order.

Work with preconfigured alerts

Check out this video on managing existing alerts.

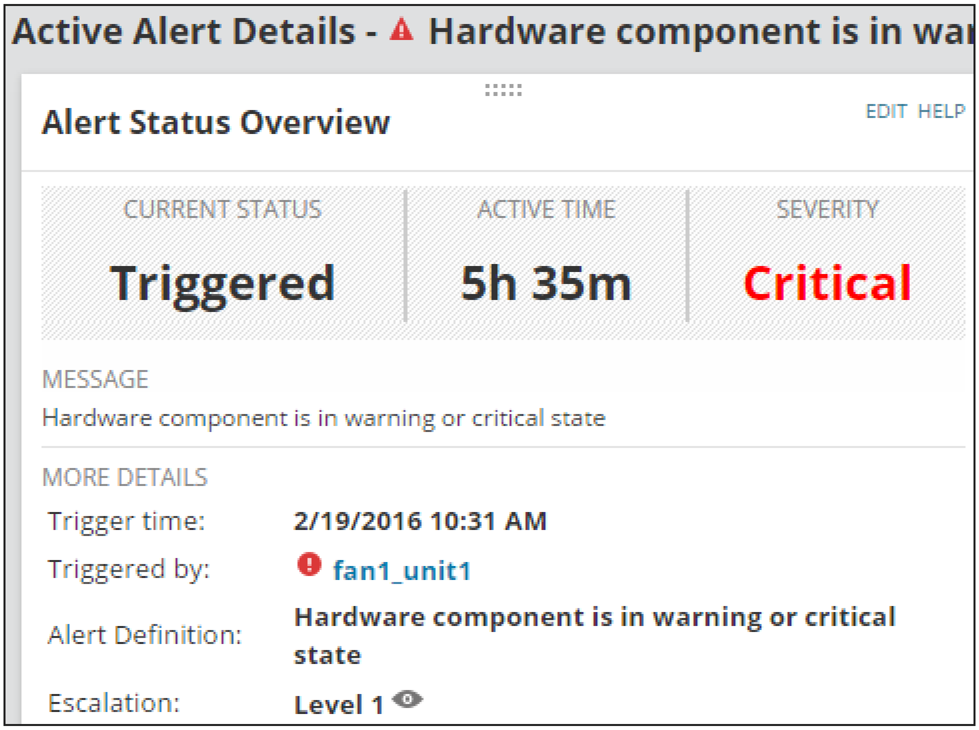
When an alert triggers, any associated alert actions also trigger, and the alert appears on the All Active Alerts page. In the all Active Alerts page you can view the details of alert, view the details of the monitored element that triggered the alert, and acknowledge the alert.

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 wai

Alert Status Overview

CURRENT STATUS	ACTIVE TIME	SEVERITY
Triggered	5h 35m	Critical

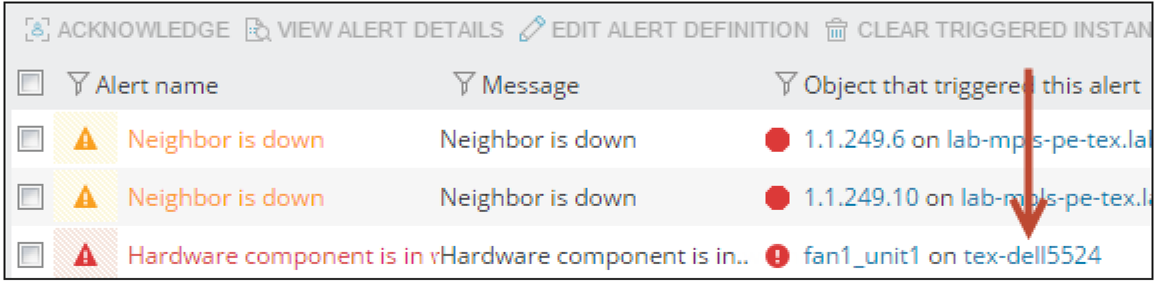
MESSAGE

Hardware component is in warning or critical state

MORE DETAILS

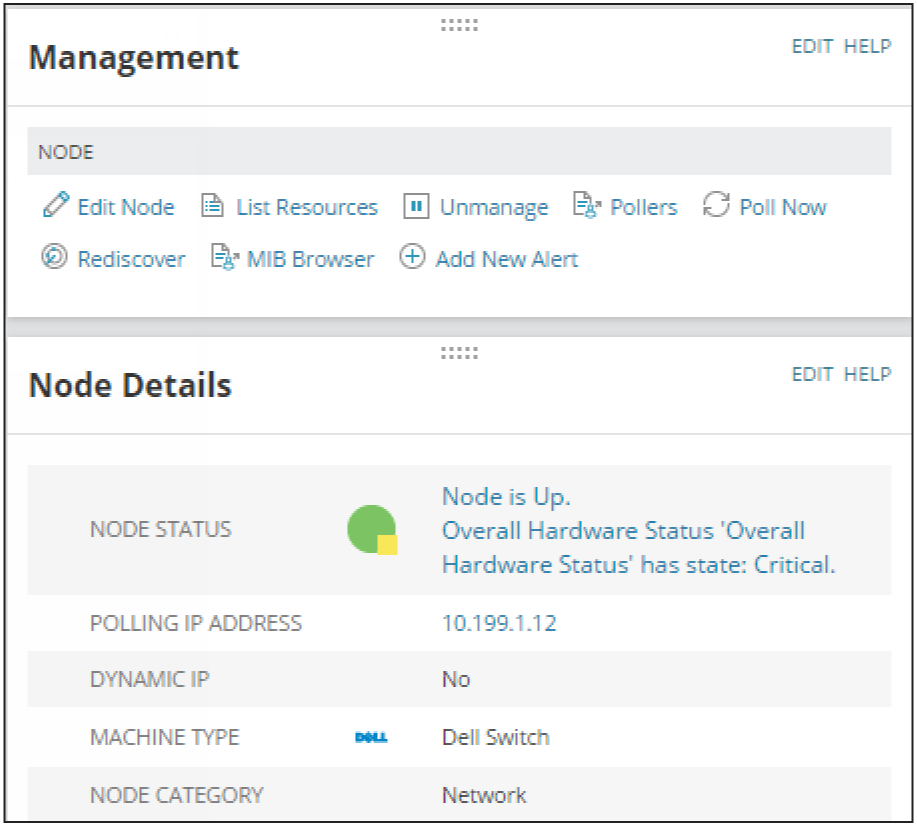
Trigger time:	2/19/2016 10:31 AM
Triggered by:	fan1_unit1
Alert Definition:	Hardware component is in warning or critical state
Escalation:	Level 1

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



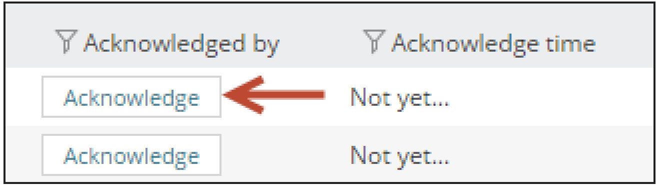
□		Alert name	Message	Object that triggered this alert
□	⚠	Neighbor is down	Neighbor is down	● 1.1.249.6 on lab-mpls-pe-tex.la
□	⚠	Neighbor is down	Neighbor is down	● 1.1.249.10 on lab-mpls-pe-tex.l
□	⚠	Hardware component is in v	Hardware component is in..	● fan1_unit1 on tex-dell5524

The details page of the selected object appears.



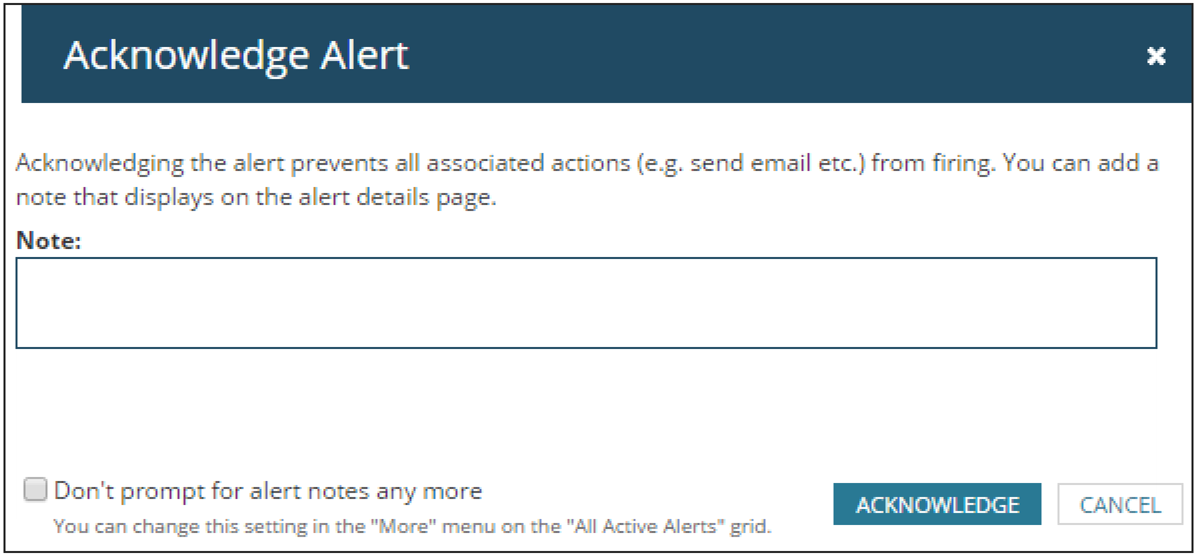
NODE STATUS	Node is Up. Overall Hardware Status 'Overall Hardware Status' has state: Critical.
POLLING IP ADDRESS	10.199.1.12
DYNAMIC IP	No
MACHINE TYPE	Dell Switch
NODE CATEGORY	Network

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.
   When acknowledged, the alert will not trigger again.



Acknowledge Alert

Acknowledging the alert prevents all associated actions (e.g. send email etc.) from firing. You can add a note that displays on the alert details page.

Note:

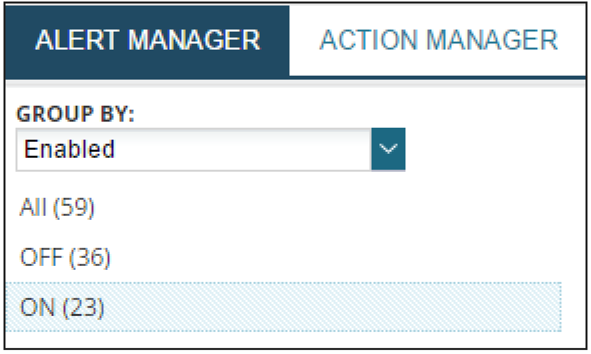
□ Don't prompt for alert notes any more

You can change this setting in the "More" menu on the "All Active Alerts" grid.

List preconfigured, enabled alerts

SolarWinds NPM ships with preconfigured, enabled alerts, and a number of disabled 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.



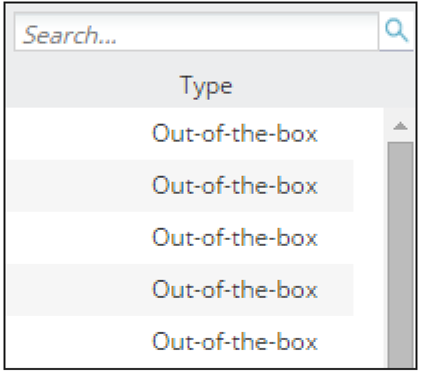
GROUP BY: Enabled

All (59)

OFF (36)

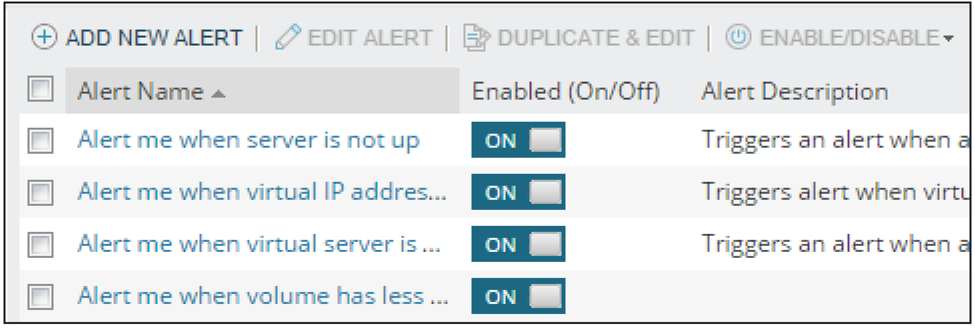
ON (23)

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



Type
Out-of-the-box
Out-of-the-box
Out-of-the-box
Out-of-the-box
Out-of-the-box

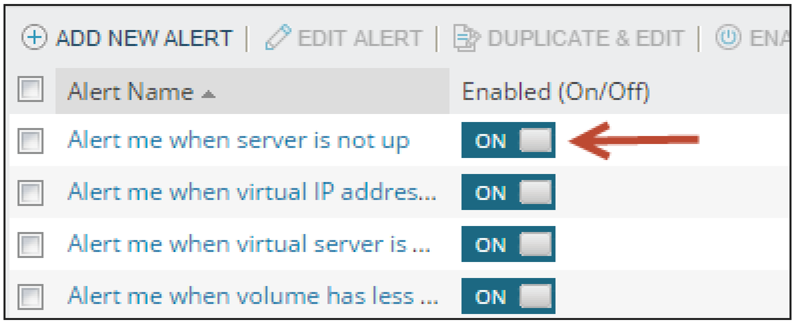
5. Review the list of preconfigured, enabled alerts.



□	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.



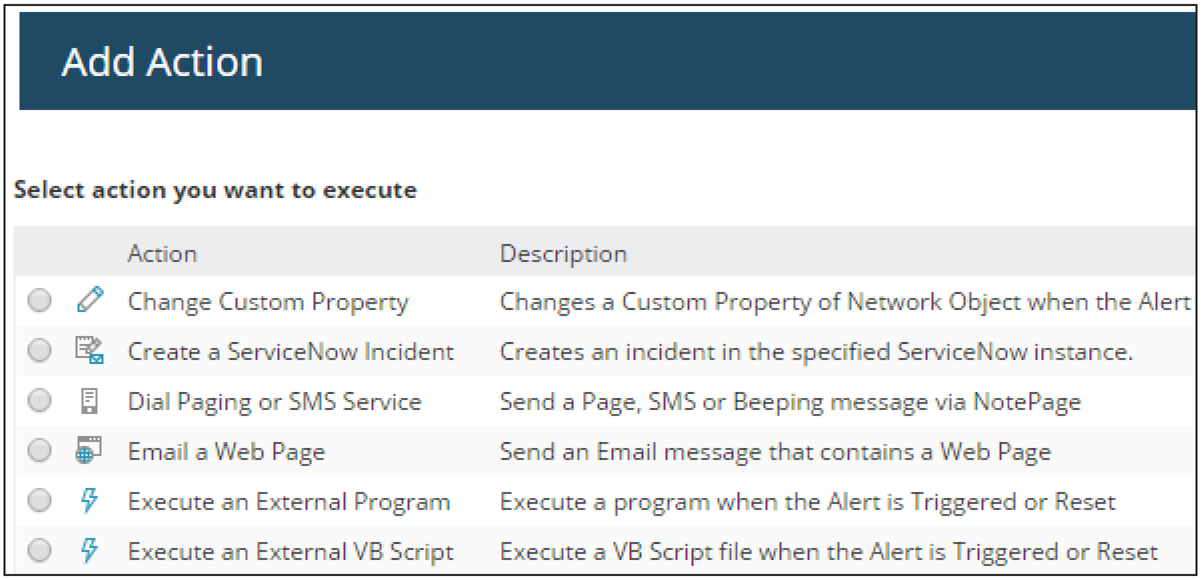
□	Alert Name ▲	Enabled (On/Off)
□	Alert me when server is not up	ON
□	Alert me when virtual IP addres...	ON
□	Alert me when virtual server is ...	ON
□	Alert me when volume has less ...	ON

Action types

You can configure an alert to trigger one or more actions, such as:

- Send an email
- Send a page
- Manage a virtual machine (for example, power on/off)
- Log the alert to 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.



Add Action

Select action you want to execute

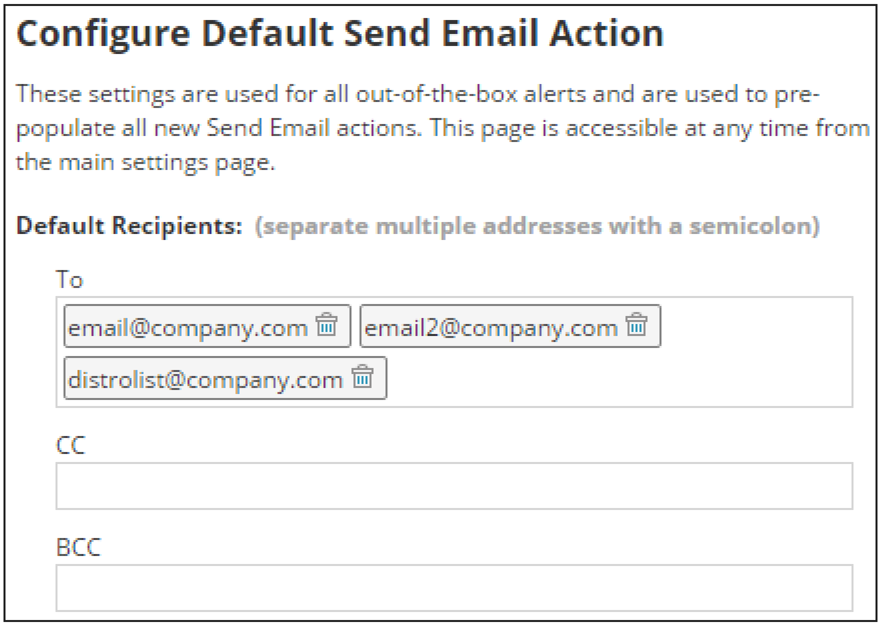
	Action	Description
○	Change Custom Property	Changes a Custom Property of Network Object when the Alert
○	Create a ServiceNow Incident	Creates an incident in the specified ServiceNow instance.
○	Dial Paging or SMS Service	Send a Page, SMS or Beeping message via NotePage
○	Email a Web Page	Send an Email message that contains a Web Page
○	Execute an External Program	Execute a program when the Alert is Triggered or Reset
○	Execute an External VB Script	Execute a VB Script file when the Alert is Triggered or Reset

Configure the default email action

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

SolarWinds Orion 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

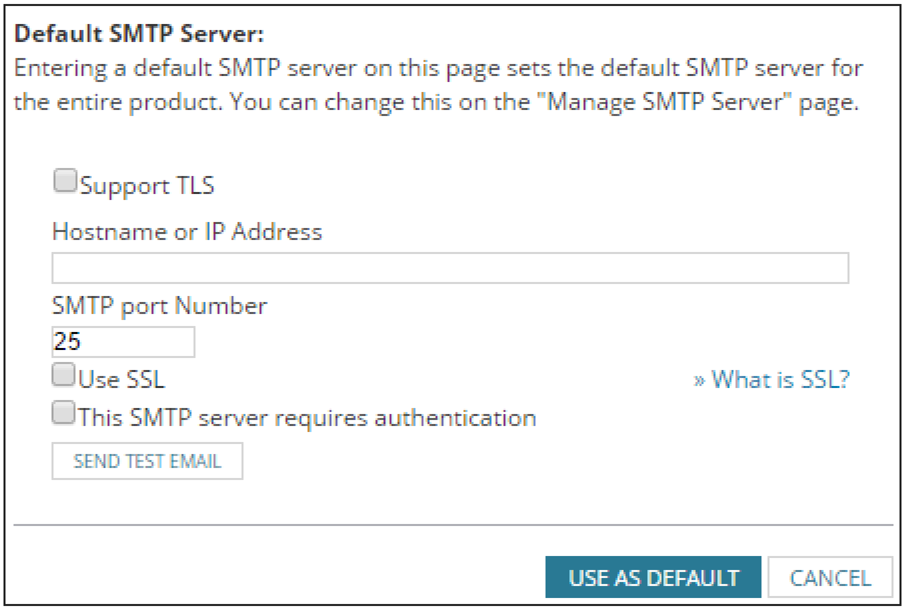
email@company.com email2@company.com distrolist@company.com

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.

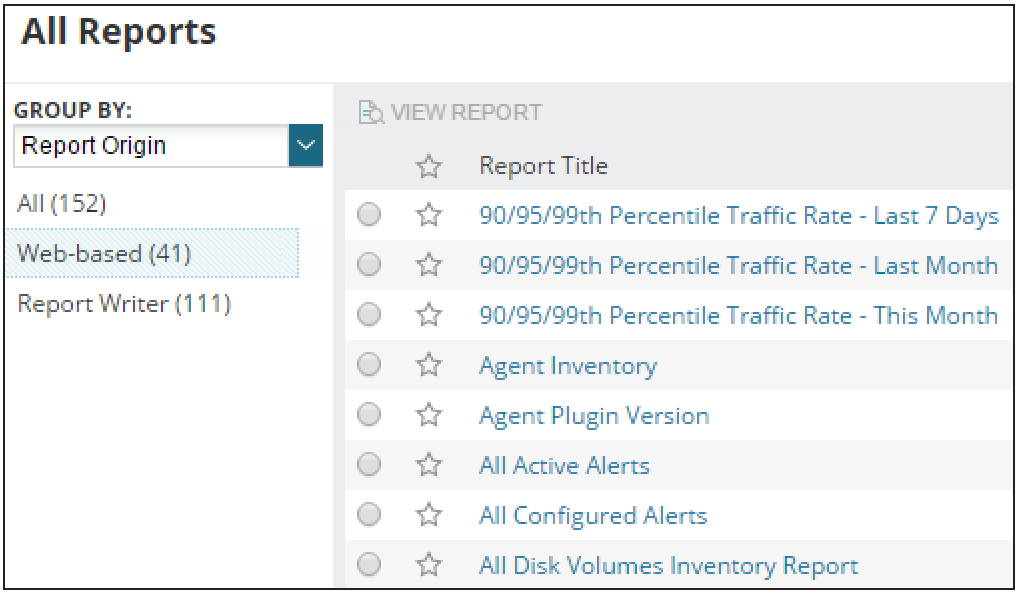
You can run an ad-hoc report, or schedule reports to be sent to you automatically, as a PDF, a web page, or email. For example, use a schedule when you want to receive the bandwidth usage from the last 7 days report every Monday morning.

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

Reports populate when:

- You Discover your network and Add discovered devices to SolarWinds Orion
- There is enough data to include in the report. Depending on the polling interval and data type, some reports do not populate immediately. For example, it takes two weeks for baseline reports to populate.

SolarWinds provides predefined reports for each Orion module. Click Home > Reports to see the available predefined reports.



All Reports

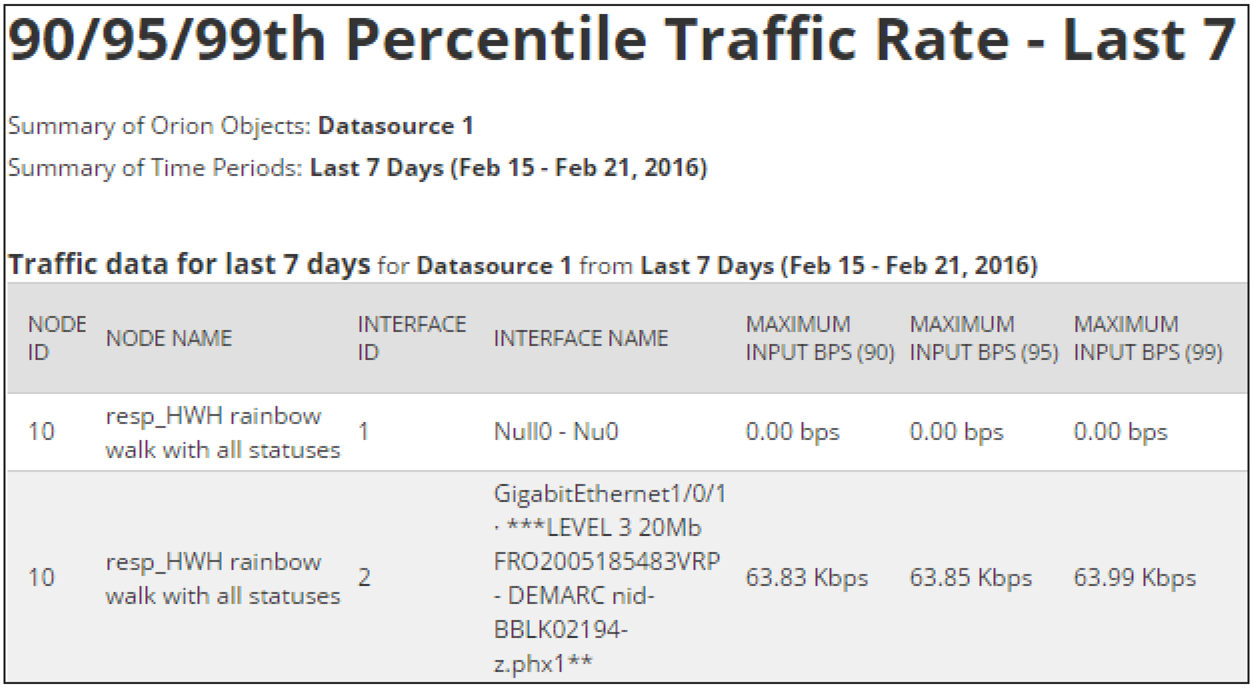
GROUP BY: Report Origin

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

VIEW REPORT

	☆	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

On the All Reports page, you can select any report and click View Report to run it immediately.



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	resp_HWH rainbow walk with all statuses	1	Null0 - Nu0	0.00 bps	0.00 bps	0.00 bps
10	resp_HWH rainbow walk with all statuses	2	GigabitEthernet1/0/1 · ***LEVEL 3 20Mb FRO2005185483VRP - DEMARC nid-BBLK02194-z.phx1**	63.83 Kbps	63.85 Kbps	63.99 Kbps

You can create your own custom reports by either editing an existing report or creating a report from scratch. Reports can combine any number or type of Orion resources, including charts, tables, and gauges. You can customize the size of the report, the layout, and add a logo and a footer.

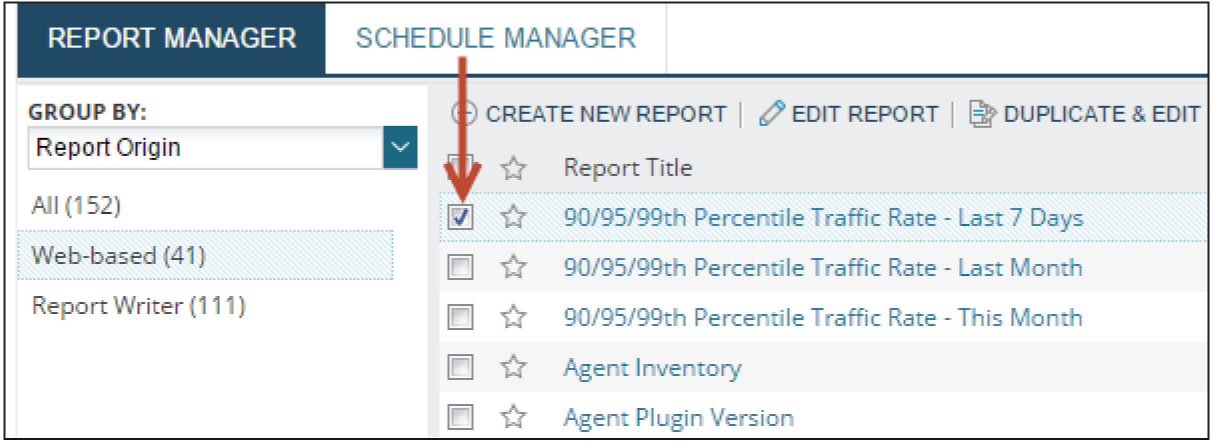
Run a preconfigured report

The following steps show you how to run and schedule the 95th Percentile Traffic Rate report.

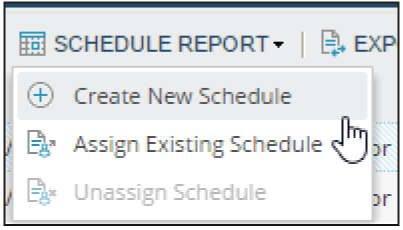
This report populates with data when:

- You Discover your network and Add discovered devices to SolarWinds Orion
- At least seven days has past since you deployed SolarWinds NPM

1. Click Reports > All Reports.
2. On the All Reports panel, locate the 95th Percentile Traffic Rate - Last 7 Days report.
3. Click the report title.

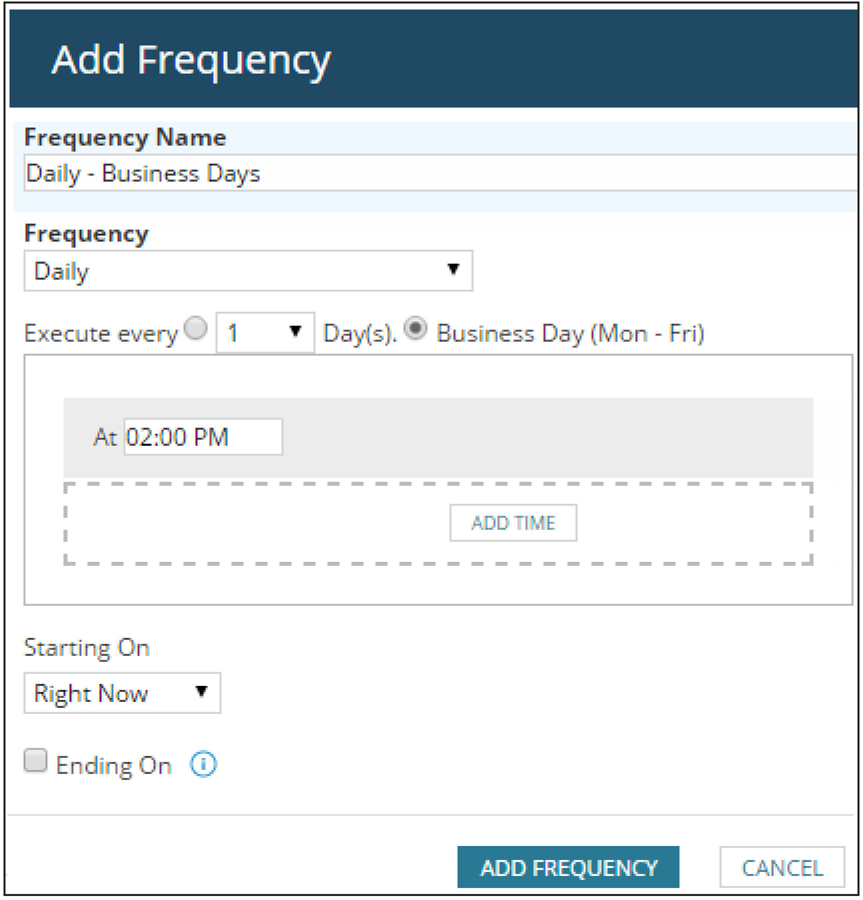


4. On the report panel, click Schedule Report > Create New Schedule.



5. On the Schedule Properties panel, type a name and description and click Next.
6. On the Schedule Frequency panel, click Add Frequency.
7. On the Add Frequency dialog box, type a name and select a time interval.
8. Select the days when you want to execute the report.

9. 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

10. On the Schedule Frequency panel, click Next.
11. On the Actions to Execute panel, click Next.
12. On the Schedule Configuration Summary panel, review the schedule and click Create Schedule.

Schedule a web-based report

1. Click Settings > All Settings > Manage Reports.
2. Select a web-based report, and click Schedule Report > Create New Schedule.
3. Continue with the previous procedure, starting with Step 5.

User accounts

This section provides information on working with user accounts:

- How user accounts work
- Create a user
- Use Active Directory credentials for Orion Platform users
- Change account passwords

How user accounts work

Check out this video on account permissions and limitations.

User accounts consist of three types of permissions:

- Basic account permissions
- View assignments
- Application specific settings

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.

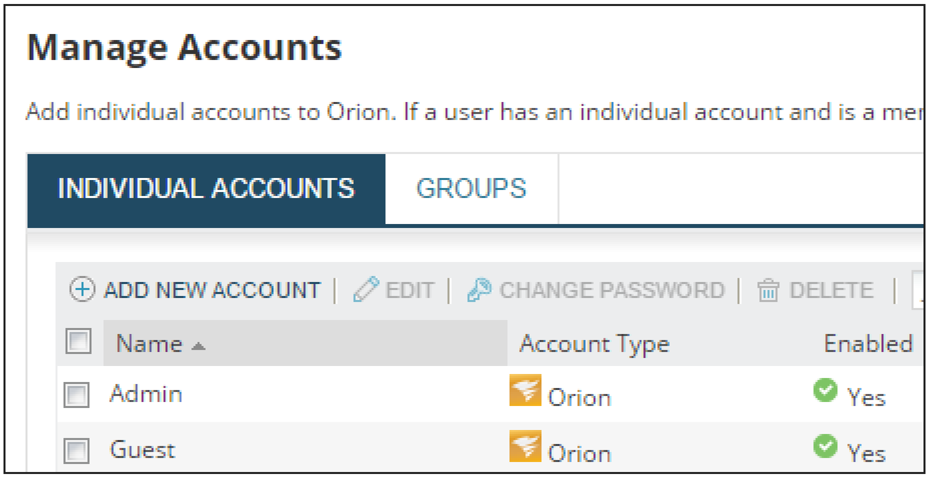
TASK	ACCESS (SELECT YES FOR THIS OPTION OR DO AS INSTRUCTED)
Add and edit user accounts and reset passwords. SolarWinds recommends that you do not allow users to change their own Orion Web Console account passwords.	Allow Administrator Rights
Add, edit, and delete nodes.	Allow Node Management Rights
Enable/disable monitoring elements.	Allow Account to Unmanage Objects
Add, edit, schedule, and delete reports.	Allow Report Management Rights

Task	Access (Select Yes for this option or do as instructed)
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. SolarWinds does not recommend enabling Alert Management Rights when a user account is set to expire. When the account expires, any alert the account created will behave erratically.
Customize views.	Allow Account to Customize Views
Access only a set of devices (type, location, department, and so on).	Click Add Limitation and define the limitation.

Create a user

Check out this video on creating users.

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.

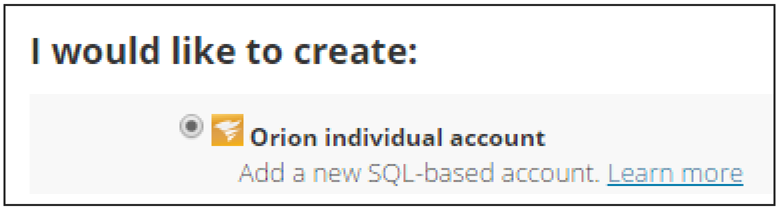


Manage Accounts

Add individual accounts to Orion. If a user has an individual account and is a mer

□	Name ▲	Account Type	Enabled
□	Admin	Orion	✓ Yes
□	Guest	Orion	✓ Yes

3. Select Orion individual account, and click Next.



I would like to create:

● Orion individual account
Add a new SQL-based account. Learn more

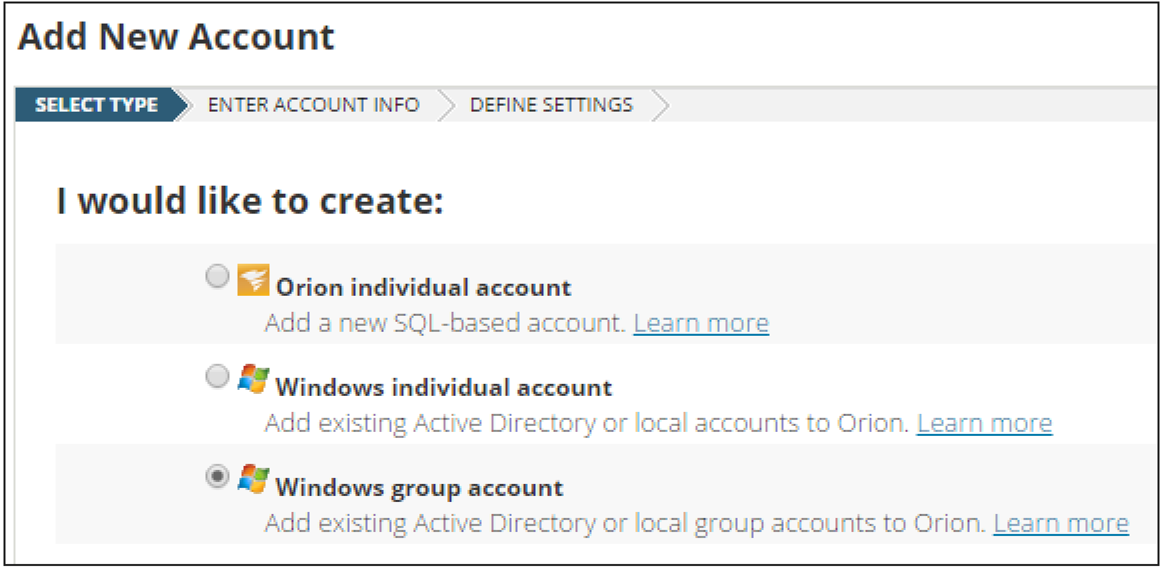
4. Provide the account credentials, and click Next.
5. On Define Settings, provide rights so that the user can perform assigned tasks, select default views and menu bars, and then click Submit.

Use Active Directory credentials for Orion Platform users

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

I would like to create:

○ Orion individual account
Add a new SQL-based account. Learn more

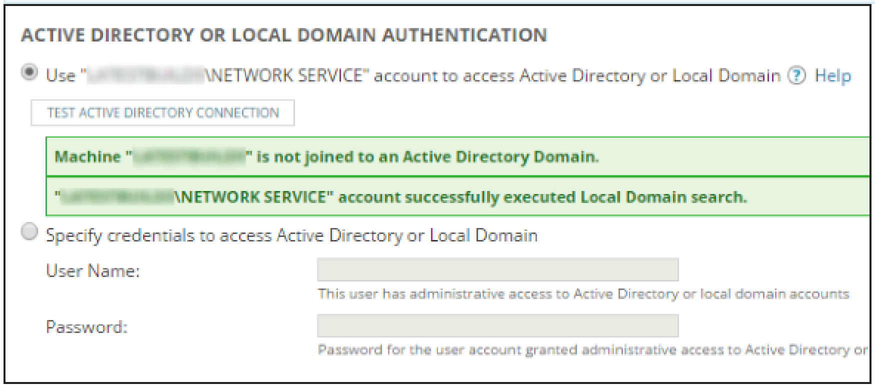
○ Windows individual account
Add existing Active Directory or local accounts to Orion. Learn more

● 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.
   - This option is not available when LDAP is enabled. You must specify credentials manually.



ACTIVE DIRECTORY OR LOCAL DOMAIN AUTHENTICATION

● Use "[redacted]\NETWORK SERVICE" account to access Active Directory or Local Domain ? Help

TEST ACTIVE DIRECTORY CONNECTION

Machine "[redacted]" is not joined to an Active Directory Domain.

"[redacted]\NETWORK SERVICE" account successfully executed Local Domain search.

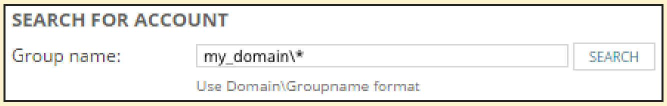
○ Specify credentials to access Active Directory or Local Domain

User Name: This user has administrative access to Active Directory or local domain accounts

Password: Password for the user account granted administrative access to Active Directory or

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: my_domain* SEARCH

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.

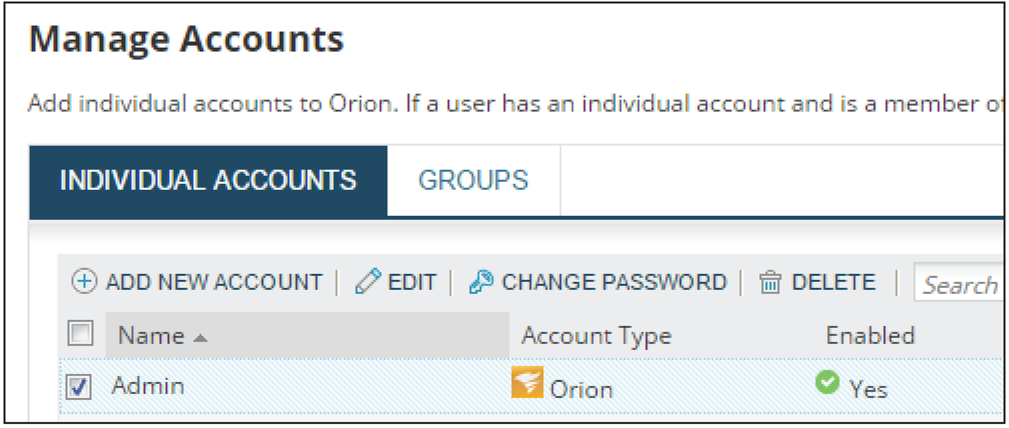
Users can now log in to the Orion Web Console using their local domain or Active Directory credentials.

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.



Manage Accounts

Add individual accounts to Orion. If a user has an individual account and is a member of

□	Name ▲	Account Type	Enabled
☑	Admin	Orion	✓ Yes

4. Enter and confirm the new password, and click Change Password.

Get connected

This section contains information on accessing the SolarWinds Customer Portal and engaging with THWACK, the SolarWinds community of IT pros:

- Access the Customer Portal
- Set up additional Customer Portal user accounts
- Engage with the SolarWinds community

Access the Customer Portal

The SolarWinds Customer Portal provides access to license and maintenance information, support cases, and product downloads, as well as live and instructor-led virtual classroom training.

Create your user profile

To create a user profile, you must know the SolarWinds customer ID (SWID) issued to your company. If you are a SolarWinds customer but do not have a SWID, contact SolarWinds Customer Support.

> ⓘ Users with multiple SWIDs require only one user profile. Your user profile can be linked to multiple SWIDs.

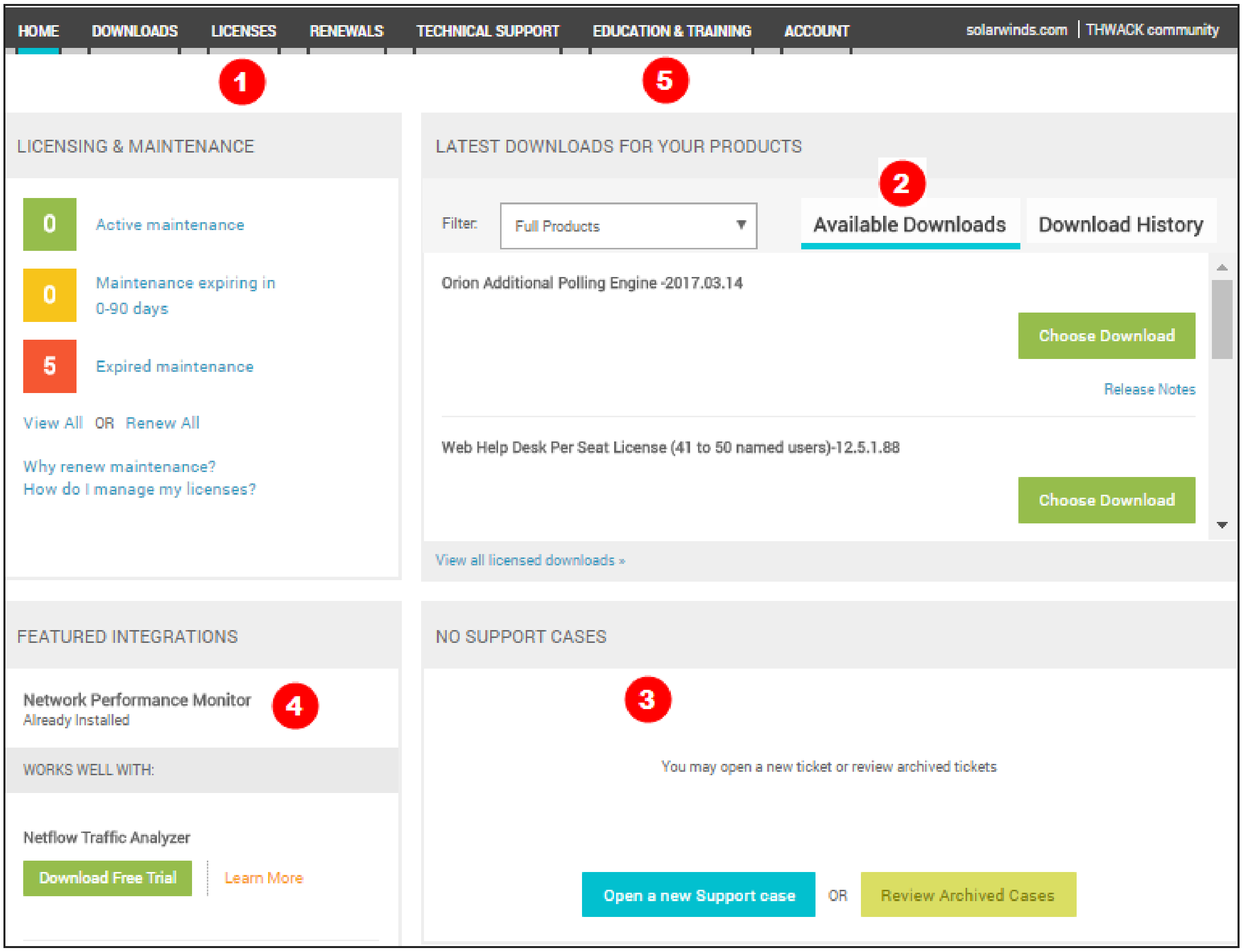
1. Go to customerportal.solarwinds.com.
2. Click the Register tab.
3. Enter your organization's SWID and your email address.

   > ⓘ If you have multiple SWIDs, enter any SWID to create your profile. Later, use the User Profile menu to link the other SWIDs to your profile.

   The account administrator will review the request, and you will receive an email when it is approved.

For more information about creating an account, see this FAQ page.

Explore the Customer Portal



LICENSING & MAINTENANCE

0	Active maintenance
0	Maintenance expiring in 0-90 days
5	Expired maintenance

View All OR Renew All

Why renew maintenance?
How do I manage my licenses?

LATEST DOWNLOADS FOR YOUR PRODUCTS

Orion Additional Polling Engine -2017.03.14

Web Help Desk Per Seat License (41 to 50 named users)-12.5.1.88

View all licensed downloads »

FEATURED INTEGRATIONS

Network Performance Monitor
Already Installed

WORKS WELL WITH:

Netflow Traffic Analyzer

NO SUPPORT CASES

You may open a new ticket or review archived tickets

1	Manage licenses and access license keys.
2	Download purchased products.
3	Open a new support case and monitor existing cases.
4	Download free trials of integrated products.
5	Sign up for training.

Set up additional Customer Portal user accounts

If you are an account administrator for the SolarWinds Customer Portal, you can add additional user accounts and define each user's access level. Set up additional accounts to allow other users to view information in the portal, create a support case, access information about existing support cases, or sign up for training.

ⓘ For more information about user account types and permissions, see this FAQ page.

1. Log in to the SolarWinds Customer Portal using an account with Account Administrator level access.
2. In the user account drop-down menu in the upper-right corner, click Company Account Settings.
3. Click the Add User button.
4. Enter the user's email address.
5. Specify the user's access level and click Create.
    - Account Administrator: can access all areas of the Customer Portal. Can also add and remove users, edit user profile information, and assign roles and contact types to users.
    - Standard Access: can access all areas of the Customer Portal.
    - No Access: cannot access the Customer Portal, but is listed as a contact on the account.

   The system sends a user profile creation email to the user. The user account is listed as Pending in the Admin portal until the user activates their account through the user profile creation email.

Engage with the SolarWinds community

Use the SolarWinds THWACK community website to learn more about SolarWinds products, participate in discussions, and get help resolving issues.

Create a THWACK account

You can read content on THWACK without an account. However, having an account allows you to take full advantage of the site by submitting feature requests, liking or following posts, and contributing content. When you create a THWACK account, SolarWinds will not send you unsolicited emails or add you to marketing lists.

1. Go to thwack.solarwinds.com.
2. Click Register in the top right.
3. Enter the required information and accept the license agreement.
4. Click Create Account.

ⓘ After you create a THWACK account, you will be asked if you want to link your THWACK account with your Customer Portal account. If you link the accounts, you will see more relevant content and messages in the Customer Portal.

Explore the THWACK site

After you create an account, complete the onboarding mission to begin exploring THWACK. Participating in the THWACK community earns points, which you can use to purchase items in the THWACK store.

As a member of the THWACK community, you can:

- Participate in community discussions and get answers to your questions.
  In the product forums, you can post questions and view responses to other users' questions. Advice, resolutions, and troubleshooting tips are provided by community members and by SolarWinds employees.
- Extend product capabilities with custom templates, reports, and scripts.
  The THWACK product forums include thousands of downloadable templates, reports, and scripts you can use to customize or extend your SolarWinds products. This content is contributed by SolarWinds employees and by other community members.
- View product roadmaps, which list the features currently being developed for future product releases.
- Be notified of User Experience sessions where you can share your experiences, and help make SolarWinds products better.
- Influence the direction of a product by submitting feature requests and voting for other users' feature requests.
- Read blogs about SolarWinds products and about general IT topics.