Network Performance Monitor

Version 12.5
Part 1 of 2: Get Started
© 2019 SolarWinds Worldwide, LLC. All rights reserved.

This document may not be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the prior written consent of SolarWinds. All right, title, and interest in and to the software, services, and documentation are and shall remain the exclusive property of SolarWinds, its affiliates, and/or its respective licensors.

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS, OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON THE DOCUMENTATION, INCLUDING WITHOUT LIMITATION NONINFRINGEMENT, ACCURACY, COMPLETENESS, OR USEFULNESS OF ANY INFORMATION CONTAINED HEREIN. IN NO EVENT SHALL SOLARWINDS, ITS SUPPLIERS, NOR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY, EVEN IF SOLARWINDS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

The SolarWinds, SolarWinds & Design, Orion, and THWACK trademarks are the exclusive property of SolarWinds Worldwide, LLC or its affiliates, are registered with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries. All other SolarWinds trademarks, service marks, and logos may be common law marks or are registered or pending registration. All other trademarks mentioned herein are used for identification purposes only and are trademarks of (and may be registered trademarks) of their respective companies.
# Table of Contents

Network Performance Monitor Getting Started Guide .......................................................... 5
What should I monitor with NPM? ......................................................................................... 6
  Discovery checklist .............................................................................................................. 6
Discover your network with NPM ......................................................................................... 8
Add discovered devices to NPM .......................................................................................... 13
Plan to scale NPM monitoring ............................................................................................. 16
Add a single node for monitoring to NPM .......................................................................... 17
Navigate SolarWinds NPM .................................................................................................. 19
  Overview of an entity ......................................................................................................... 19
Identify and troubleshoot a node that has a problem with NPM ........................................ 21
  Step 1: Determine there is a problem ................................................................................ 21
  Step 2: Get more details about the node ........................................................................ 23
  Step 3: Get more details about the alert ........................................................................... 25
Identify and troubleshoot an interface that has a problem with NPM ................................. 26
  Step 1: Determine there is a problem ................................................................................ 26
    Top 10 Interfaces by Percent Utilization ...................................................................... 27
    Top 10 Interfaces by Traffic ......................................................................................... 28
    Top 10 Errors & Discards Today .................................................................................... 28
  Step 2: Get more details about the interface .................................................................... 29
  Step 3: Get more details about the problem ................................................................... 31
    Min/Max/Average Response Time & Packet Loss ......................................................... 32
    Network Latency & Packet Loss .................................................................................... 33
How alerts work in NPM ....................................................................................................... 34
  Work with preconfigured alerts in NPM ......................................................................... 35
    List preconfigured, enabled alerts ............................................................................... 37
  Enable and disable alerts .................................................................................................. 38
  Action types ...................................................................................................................... 39
  Configure the default email action .................................................................................. 39
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>How reports work in NPM</td>
<td>41</td>
</tr>
<tr>
<td>Run a report</td>
<td>41</td>
</tr>
<tr>
<td>Schedule a web-based report</td>
<td>42</td>
</tr>
<tr>
<td><strong>Beyond Getting Started with NPM</strong></td>
<td>44</td>
</tr>
<tr>
<td>Orion Platform Administrator Guide</td>
<td>44</td>
</tr>
<tr>
<td>NPM Administrator Guide</td>
<td>44</td>
</tr>
</tbody>
</table>
Network Performance Monitor Getting Started Guide


To learn how to start monitoring your environment with NPM, complete the following tasks:

- **Install NPM.**
  
  See the [SolarWinds Orion Installer](https://www.solarwinds.com/orion/products/installer) for system requirements, planning checklists, and installation instructions. The Getting Started Guide expects that you have already installed NPM.

- **Discover the devices** on your network and select devices to monitor.
  
  - [What should you monitor?](#)
  
  - How to discover the network, add discovered devices or a single node for monitoring.

- **Investigate** devices with issues:
  
  - Meet the NPM user interface - the [Orion Web Console](https://www.solarwinds.com/orion/products/console).
  
  - [Troubleshoot a node](https://www.solarwinds.com/orion/products/troubleshoot) that has a problem.
  
  - [Troubleshoot an interface](https://www.solarwinds.com/orion/products/troubleshoot) that has a problem.

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

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

When you have finished this guide, see [Getting Started with NPM: Customize](https://www.solarwinds.com/orion/products/customize) to get familiar with basic customization procedures and [Beyond Getting Started with NPM](https://www.solarwinds.com/orion/products/beyond) for information about other NPM functionality.

**Existing customers:** Access your licensed software from the [SolarWinds Customer Portal](https://www.solarwinds.com/customer-portal). If you need any implementation help, contact our [Support Reps](https://www.solarwinds.com/support).

**Evaluators:** Download your free 30-day evaluation from [www.solarwinds.com](https://www.solarwinds.com). If you need assistance with your evaluation, contact [sales@solarwinds.com](mailto:sales@solarwinds.com).
What should I monitor with NPM?

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

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

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

Discovery checklist

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

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

- **SNMP**: primarily used to monitor network devices, for example, routers, firewalls, and switches. To enable SNMP, consult the device documentation.

  **SNMP requirements**
  - For correct device identification, monitored devices must allow access to the SysObjectID.
  - Unix-based devices should use the version of Net-SNMP (5.5 or later) specific to the Unix-based operating system in use.
  - 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, 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.

- **WMI**: usually enabled on Windows devices by default. If the polling engine and device are separated by a firewall, SolarWinds recommends that you deploy an optional agent to securely monitor Windows servers and applications by WMI.

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

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

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

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

- Determine SNMP v1/2 community strings and SNMP v3 community strings and credentials of the devices to monitor.

- Determine log in credentials for each monitored device.

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

- Determine Windows credentials: domain or local admin.
Discover your network with NPM

Watch this video on discovering your network.

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

Log in to the Orion Web Console

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

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

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

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

1. If the Discovery Wizard does not start automatically after configuration, click Settings > Network Discovery.
2. Click Add New Discovery, and then click Start.
3. On the Network panel, if this is your first discovery, add a limited number of IP addresses.

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

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Ranges</td>
<td>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.</td>
</tr>
<tr>
<td>Subnets</td>
<td>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.</td>
</tr>
<tr>
<td>IP Addresses</td>
<td>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.</td>
</tr>
<tr>
<td>Active Directory</td>
<td>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.</td>
</tr>
</tbody>
</table>
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.
6. On the SNMP panel:
   a. If all devices on your network require only the default SNMPv1 and SNMPv2 public and private community strings, click Next.
   b. If any device on your network uses a community string other than public or private, or if you want to use an SNMPv3 credential, click Add Credential and provide the required information.

![Add New Credential](image)

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](image)

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.


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

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

Check out this video on adding devices to SolarWinds NPM.

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

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

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

1. Ensure that only the device types you want to monitor are selected, and click Next.

   **Network Sonar Results Wizard**

<table>
<thead>
<tr>
<th>Device Types to Import</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select the device types to monitor.</td>
</tr>
<tr>
<td>Count</td>
</tr>
<tr>
<td>-------</td>
</tr>
<tr>
<td>☑️</td>
</tr>
<tr>
<td>☑️</td>
</tr>
<tr>
<td>☑️</td>
</tr>
<tr>
<td>☑️</td>
</tr>
</tbody>
</table>

   ![Network Sonar Results Wizard](image)

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

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

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

   ![List of Interfaces](image)

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

<table>
<thead>
<tr>
<th>Count</th>
<th>Volume Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>RAM</td>
</tr>
<tr>
<td>12</td>
<td>Virtual Memory</td>
</tr>
<tr>
<td>3</td>
<td>Other</td>
</tr>
<tr>
<td>19</td>
<td>Fixed Disk</td>
</tr>
<tr>
<td>4</td>
<td>RAM Disk</td>
</tr>
</tbody>
</table>

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 removed from future network discovery, manual or scheduled. If you wish to ignore items, do so before importing.

<table>
<thead>
<tr>
<th>Polling IP Address</th>
<th>Name</th>
<th>Machine Type</th>
<th>Volumes</th>
<th>Polling Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.196.100.250</td>
<td>HQDC-3750-CORE.demo.lab</td>
<td>Catalyst 37xx Stack</td>
<td></td>
<td>SNMP</td>
</tr>
<tr>
<td>10.196.200.250</td>
<td>BROF-3750-CORE.demo.lab</td>
<td>Catalyst 37xx Stack</td>
<td></td>
<td>SNMP</td>
</tr>
<tr>
<td>10.196.202.1</td>
<td>BROF-2821-WAN.demo.lab</td>
<td>Cisco 2821</td>
<td></td>
<td>SNMP</td>
</tr>
<tr>
<td>10.196.204.11</td>
<td>BOHYV01</td>
<td>Hyper-V Server</td>
<td>RAM, Virtual Memory, Fixed Disk</td>
<td>SNMP</td>
</tr>
<tr>
<td>10.196.204.12</td>
<td>BOESX01.demo.lab</td>
<td>VMware ESX Server</td>
<td>RAM Disk (4), Fixed Disk</td>
<td>SNMP</td>
</tr>
</tbody>
</table>

5. When the import completes, click Finish.
6. Click the Home tab to begin exploring your network.
If the status of a node is Unknown after discovery, you may need to check a few settings in SolarWinds NPM. See Troubleshoot Unknown Nodes for more information.

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

You installed and configured your NPM, 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.
Add a single node for monitoring to NPM

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

Adding a single node offers more detail in monitoring and is recommended for nodes with high latency. Do not include nodes with high latency in a discovery job.

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

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

To add a single node for monitoring:

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

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

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

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

   c. Enter values for custom properties for the node.

   The Custom Properties area is empty if you have not defined any custom properties for the monitored nodes. See "Add custom properties to nodes" in the SolarWinds Getting Started Guide - Customize.

   d. To adjust when the status of the node changes to Warning or Critical, edit alerting thresholds for the metric. Select the Override box and set thresholds specific for the node.

7. Click OK, Add Node.

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

Check out this video on navigating the Web Console.

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

In the meantime, see the following terms that might be helpful when 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 in to the Orion Platform. It 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.

- **Widget**: The informational blocks that make up a view.

- **Entity**: Anything that can be monitored by the Orion Platform.

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

**Overview of an entity**

Within a view, entities that appear in green are up and working as expected. Entities that appear red or partially red need attention. In this example, all nodes are up, but node Cur-Nor5520 has an issue as indicated by the red square next to the node name. The red square indicates that the system is monitoring a child of that node, for example, an interface.
To explore a node, place your cursor over the entity to see more details. In this example, one or more interfaces are down. Click the node to drill down to the node details page.

Check out this video on viewing your devices.
Identify and troubleshoot a node that has a problem with NPM

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

Step 1: Determine there is a problem

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

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

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

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

If you have configured your alerts to send email, you get an email when a node goes down.
If you do not see any alerts, click My Dashboards > Network > Network Top 10.

The widgets on this page help identify nodes that respond to a ping but have other health problems.
Step 2: Get more details about the node

When you find a node with a problem, click the node name in any widget to open the Node Details page. If a node is down (red), this means it does not respond to a ping. To resolve an issue of this severity:

1. Check the power. Is it plugged in?
2. Check the LAN link light. Is it connected to the network?
3. Log in to the device and begin troubleshooting it.

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

- Check the Response Time, Packet Loss, CPU load, and Memory Utilization widgets. Usually, those statistics are the first indicators of a problem. In our example, the CPU load on this node is high.
- Use the Network Latency & Packet Loss, as well as the Min/Max/Average Response Time charts, to see if this is a momentary problem or a continuing issue.

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

  **Hardware health**: Reports on physical elements of the hardware for Cisco, Dell, F5, HP, and Juniper.
Routing table information: For routers and switches, multiple widgets show a variety of route-related information. Look under the Network subview for routing widgets, such as Routing Neighbors, Routing Table, or Default Route Changes.

Step 3: Get more details about the alert

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

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 with NPM**, alerts are triggered when a node goes down. Alerts can also be triggered when an interface has a problem, such as high utilization or the interface going down.

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

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

### Nodes with Problems

<table>
<thead>
<tr>
<th>NODE</th>
<th>DESCRIPTION</th>
<th>CURRENT RESPONSE TIME</th>
<th>PERCENT LOSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch sales</td>
<td>Node is Down</td>
<td>No Response</td>
<td>100 %</td>
</tr>
<tr>
<td></td>
<td>One or more Interfaces have state: Unknown.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TUL-WDSRV-01</td>
<td>Node is Down</td>
<td>No Response</td>
<td>100 %</td>
</tr>
<tr>
<td></td>
<td>One or more Interfaces have state: Unknown.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lab/ Samsung</td>
<td>Node is Down</td>
<td>No Response</td>
<td>100 %</td>
</tr>
<tr>
<td></td>
<td>One or more Interfaces have state: Unknown.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>stp-j2320</td>
<td>Node is Down</td>
<td>No Response</td>
<td>100 %</td>
</tr>
<tr>
<td>VMAN-ORION01</td>
<td>Node is Down</td>
<td>No Response</td>
<td>100 %</td>
</tr>
<tr>
<td></td>
<td>One or more Interfaces have state: Down.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>St.P-6509</td>
<td>Node is Up</td>
<td>38ms</td>
<td>0 %</td>
</tr>
<tr>
<td></td>
<td>One or more Interfaces have state: Down.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phx-Nexus 1000V</td>
<td>Node is Up</td>
<td>0ms</td>
<td>0 %</td>
</tr>
<tr>
<td></td>
<td>Interface 'Ethernet3/2' has state: Down.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VMware Virtual</td>
<td>Node is Up</td>
<td>21ms</td>
<td>0 %</td>
</tr>
<tr>
<td>Switch</td>
<td>One or more Interfaces have state: Unknown.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Core-3640</td>
<td>Node is Up</td>
<td>1ms</td>
<td>0 %</td>
</tr>
<tr>
<td></td>
<td>One or more Interfaces have state: Down.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
In your environment, you might not have any down interfaces. To find an interface with issues that need to be investigated, click My Dashboards > Network > Network Top 10 to open the Network Top 10 view. Review the following widgets on this page.

**Top 10 Interfaces by Percent Utilization**

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

Any interface with high utilization deserves more investigation.

<table>
<thead>
<tr>
<th>NODE</th>
<th>INTERFACE</th>
<th>RECEIVE</th>
<th>TRANSMIT</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAB-CLUSTER-01.lab.tex</td>
<td>WAN Miniport (SSTP) - Local Area Connection*</td>
<td>94 %</td>
<td>96 %</td>
</tr>
<tr>
<td>Router3.lab.local</td>
<td>FastEthernet0/0 - Fa0/0</td>
<td>94 %</td>
<td>96 %</td>
</tr>
<tr>
<td>NFM_Cisco_FibreChannel</td>
<td>fc1/7</td>
<td>63 %</td>
<td>91 %</td>
</tr>
<tr>
<td>Internet Gateway 3725</td>
<td>Ethernet1 - WAN (NetFlow)</td>
<td>85 %</td>
<td>65 %</td>
</tr>
<tr>
<td>NFM_Cisco_FibreChannel</td>
<td>fc1/13</td>
<td>62 %</td>
<td>73 %</td>
</tr>
</tbody>
</table>
Top 10 Interfaces by Traffic

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

<table>
<thead>
<tr>
<th>NODE</th>
<th>INTERFACE</th>
<th>RECEIVE</th>
<th>TRANSMIT</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAB-CLUSTER-01.lab.tex</td>
<td>WAN Miniport (SSTP) Local Area Connection*</td>
<td>1.009 Gbps</td>
<td>1.031 Gbps</td>
</tr>
<tr>
<td>NPM_Cisco_FibreChannel</td>
<td>fc:1/7</td>
<td>626.166 Mbps 912.142 Mbps</td>
<td></td>
</tr>
<tr>
<td>NPM_Cisco_FibreChannel</td>
<td>fc:1/13</td>
<td>617.2 Mbps 727.277 Mbps</td>
<td></td>
</tr>
<tr>
<td>Internet Gateway 3725</td>
<td>Ethernet1 - WAN (NetFlow)</td>
<td>106.25 Mbps 812.5 Mbps</td>
<td></td>
</tr>
<tr>
<td>Router2.lab.local</td>
<td>Null0 - Nu0</td>
<td>361.703 Mbps 36.177 Mbps</td>
<td></td>
</tr>
</tbody>
</table>

Top 10 Errors & Discards Today

This widget shows:

- Errors: A packet that was received but could not be processed because there was a problem with the packet.
Discards: A packet that was received without errors but was dropped, usually because interface utilization is near 100%.

### Top 10 Errors & Discards Today

<table>
<thead>
<tr>
<th>NODE</th>
<th>INTERFACE</th>
<th>RECEIVE ERRORS</th>
<th>RECEIVE DISCARDS</th>
<th>TRANSIT ERRORS</th>
<th>TRANSIT DISCARDS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perm_Tex-Mds9120-75-76</td>
<td>fc1/5</td>
<td>0 errors</td>
<td>0 discards</td>
<td>5,582,170,112 errors</td>
<td>5,808,010 discards</td>
</tr>
<tr>
<td>Perm_ap5611-E6C8C0</td>
<td>fe4</td>
<td>64,088,776 errors</td>
<td>78,073,384 discards</td>
<td>0 errors</td>
<td>0 discards</td>
</tr>
<tr>
<td>Perm_ap5611-E6C8C0</td>
<td>fe2</td>
<td>100,061,432 errors</td>
<td>2,349 discards</td>
<td>0 errors</td>
<td>0 discards</td>
</tr>
<tr>
<td>Perm_Tex-Mds9120-75-76</td>
<td>fc1/6</td>
<td>0 errors</td>
<td>0 discards</td>
<td>5,808,179 errors 10,024,648 discards</td>
<td></td>
</tr>
<tr>
<td>Phx-Nexus 1000V</td>
<td>port-channel1</td>
<td>0 errors</td>
<td>1,244,402 discards</td>
<td>0 errors</td>
<td>0 discards</td>
</tr>
<tr>
<td>NPM_SG9323P038</td>
<td>wvlan0 : Wireless port 1</td>
<td>1,108,093 errors 7 discards</td>
<td>89,159 errors 88 discards</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Step 2: Get more details about the interface

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

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

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

- Click the interface name in any widget. The Interface Details page opens.
- Check the Percent Utilization widget for the last-polled value of transmit and receive utilization. If those values are high, you can also check the Percent Utilization – Line Chart to see the duration of the problem.

- The Interface Downtime widget displays the interface status for the last 24 hours. If the interface status changed, you can see it in this widget. In the following example, the interface had one period when its status was unknown during the last 24 hours, but it is currently up.
- The Interface Errors & Discards widget can also indicate problems. Since this device has high discards, and high discards are generally caused by a full buffer, check the Node Details for this device and determine if the buffer is full.

<table>
<thead>
<tr>
<th>Interface Errors &amp; Discards</th>
<th>RECEIVE</th>
<th>TRANSMIT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Errors This Hour</td>
<td>1,660 errors</td>
<td>0 errors</td>
</tr>
<tr>
<td>Errors Today</td>
<td>4,192 errors</td>
<td>0 errors</td>
</tr>
<tr>
<td>Discards This Hour</td>
<td>0 discards</td>
<td>0 discards</td>
</tr>
<tr>
<td>Discards Today</td>
<td>0 discards</td>
<td>0 discards</td>
</tr>
</tbody>
</table>

### 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.

Examine the following widgets.
Min/Max/Average Response Time & Packet Loss

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

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

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

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

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

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

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

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

You can also integrate alerts with SolarWinds Help Desk.

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

<table>
<thead>
<tr>
<th>ALERT NAME</th>
<th>MESSAGE</th>
<th>TRIGGERING OBJECT</th>
<th>ACTIVE TIME</th>
<th>RELATED NODE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host memory utilization</td>
<td>Host memory utilization</td>
<td>stp-esx-01.lab.tex</td>
<td>2d 13h 30m</td>
<td>stp-esx-01.lab.tex</td>
</tr>
<tr>
<td>Host CPU utilization</td>
<td>Host CPU utilization</td>
<td>stp-esx-01.lab.tex</td>
<td>2d 13h 30m</td>
<td>stp-esx-01.lab.tex</td>
</tr>
<tr>
<td>Host CPU utilization</td>
<td>Host CPU utilization</td>
<td>bas-esx-02.lab.tex</td>
<td>2d 13h 30m</td>
<td>bas-esx-02.lab.tex</td>
</tr>
</tbody>
</table>
To see all alerts, click the All Active Alerts button in the Active Alerts widget, or go to Alerts & Activity > Alerts. On this page, you can:

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

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

**Work with preconfigured alerts in NPM**

Watch this video on managing existing alerts.

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

1. To view the alert details, click the alert.
The Active Alert Details page appears.

2. To view the details of the network object that triggered the alert, click an object.
The details page of the selected object appears.

3. To acknowledge an alert:
   a. Click Acknowledge.

   ![Acknowledgement screenshot]

   b. Enter a note and click Acknowledge.

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

List preconfigured, enabled alerts

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

1. Click Alerts & Activity > Alerts.
2. Click Manage Alerts.
3. In the Group by field, select Enabled.

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

5. Review the list of preconfigured, enabled alerts.

Enable and disable alerts

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

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

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

Configure the default email action

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

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

1. Click Settings > All Settings > Configure Default Send Email Action.

2. In the Default Recipients section, provide the email addresses of default recipients, separated by a semicolon.

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 configuration](image)

- Support TLS
- Hostname or IP Address
- SMTP port Number: 25
- Use SSL
- This SMTP server requires authentication

[SEND TEST EMAIL]

[USE AS DEFAULT] [CANCEL]
How reports work in NPM

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

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

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

Run a report

SolarWinds provides predefined reports for each Orion module.

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

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

<table>
<thead>
<tr>
<th>NODE ID</th>
<th>NODE NAME</th>
<th>INTERFACE ID</th>
<th>INTERFACE NAME</th>
<th>MAXIMUM INPUT BPS (90)</th>
<th>MAXIMUM INPUT BPS (55)</th>
<th>MAXIMUM INPUT BPS (99)</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>resp_HWH rainbow walk with all statuses</td>
<td>1</td>
<td>Null0 - Nu0</td>
<td>0.00 bps</td>
<td>0.00 bps</td>
<td>0.00 bps</td>
</tr>
<tr>
<td>10</td>
<td>resp_HWH rainbow walk with all statuses</td>
<td>2</td>
<td>GigabitEthernet1/0/1</td>
<td>63.83 Kbps</td>
<td>63.85 Kbps</td>
<td>63.99 Kbps</td>
</tr>
</tbody>
</table>

Schedule a web-based report

1. Click Settings > All Settings > Manage Reports.

> You can also access the view from Reports: Click Reports > All Reports, and then click Manage Reports in the top right corner of the view.


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

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

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

6. Select the days when you want to execute the report.
7. Enter a time and click Add Frequency.

8. On the Schedule Frequency panel, click Next.

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

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

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

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

Orion Platform Administrator Guide

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

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

NPM Administrator Guide

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

- Discover your network paths with NetPath™
- Monitor custom metrics on your devices
- Use Network Insight for F5 BIG-IP, Cisco Nexus devices, Cisco ASA, and Cisco ACI
- Forecast capacity

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