Copyright © 1995-2015 SolarWinds Worldwide, LLC. All rights reserved worldwide.

No part of this document may be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the written consent of SolarWinds. All right, title, and interest in and to the software and documentation are and shall remain the exclusive property of SolarWinds and its respective licensors.

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON SOFTWARE AND DOCUMENTATION FURNISHED HEREUNDER INCLUDING WITHOUT LIMITATION THE WARRANTIES OF DESIGN, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT. IN NO EVENT SHALL SOLARWINDS, ITS SUPPLIERS, NOR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY EVEN IF SOLARWINDS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

The SOLARWINDS and SOLARWINDS & Design marks are the exclusive property of SolarWinds Worldwide, LLC and 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, registered or pending registration in the United States or in other countries. All other trademarks mentioned herein are used for identification purposes only and may be or are trademarks or registered trademarks of their respective companies.

About SolarWinds

SolarWinds, Inc. develops and markets an array of IT management, monitoring, and discovery tools to meet the diverse requirements of today’s IT management and consulting professionals. SolarWinds products continue to set benchmarks for quality and performance and have positioned the company as the leader in IT management and discovery technology. The SolarWinds customer base includes over 85 percent of the Fortune 500 and customers from over 170 countries. Our global business partner distributor network exceeds 100 distributors and resellers.

Contacting SolarWinds

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

<table>
<thead>
<tr>
<th>Team</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sales</td>
<td><a href="mailto:sales@solarwinds.com">sales@solarwinds.com</a></td>
</tr>
<tr>
<td></td>
<td><a href="http://www.solarwinds.com">www.solarwinds.com</a></td>
</tr>
<tr>
<td></td>
<td>1.866.530.8100</td>
</tr>
<tr>
<td></td>
<td>+353.21.5002900</td>
</tr>
<tr>
<td>Technical Support</td>
<td><a href="http://www.solarwinds.com/support/">www.solarwinds.com/support/</a></td>
</tr>
<tr>
<td>User Forums</td>
<td><a href="http://www.thwack.com">www.thwack.com</a></td>
</tr>
</tbody>
</table>

Conventions

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

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

<table>
<thead>
<tr>
<th>Document</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator Guide</td>
<td>Provides detailed setup, configuration, and conceptual information.</td>
</tr>
<tr>
<td>Page Help</td>
<td>Provides help for every window in the user interface</td>
</tr>
<tr>
<td>Release Notes</td>
<td>Provides late-breaking information, known issues, and updates. The latest release notes can be found at <a href="http://www.solarwinds.com">www.solarwinds.com</a>.</td>
</tr>
</tbody>
</table>
# Table of Contents

**How SolarWinds Packet Analysis Sensors Work** ................................................. 2
  Network Packet Analysis Sensor (NPAS) .......................................................... 2
  Server Packet Analysis Sensor (SPAS) ............................................................ 3

**Limitations to Packet Analysis Sensors** ......................................................... 3

**System Requirements** ...................................................................................... 4
  Network Packet Analysis Sensors (NPAS) .......................................................... 4
  Server Packet Analysis Sensors (SPAS) ............................................................ 4
  Port Requirements ............................................................................................. 5
  Port Mirroring Requirements ............................................................................. 5

**Common Packet Analysis Sensor Deployment Scenarios** ............................... 6
  Aggregation per application ................................................................................ 7
  Aggregation with access to network (NPAS) ....................................................... 8
  Aggregation with access to application servers (SPAS) ....................................... 9
  Aggregation per site ............................................................................................ 10
  Aggregation per site with access to network (NPAS) .......................................... 10
  Aggregation per site with access to application servers (SPAS) .......................... 11
  Aggregation per computer .................................................................................. 12
  Aggregation per computer with access to network (NPAS) .................................. 13
  Aggregation per computer with access to application servers (SPAS) ............... 14

**Deploying Packet Analysis Sensors** ................................................................. 15
  Deploying a Server Sensor .................................................................................. 15
  Deploying a Network Sensor .............................................................................. 16

**Monitoring QoE Applications and Nodes** ...................................................... 17
  Manage Global QoE Settings ............................................................................ 17
  QoE Applications ............................................................................................... 17
  Nodes with QoE Traffic ..................................................................................... 18
  Monitoring QoE Applications ............................................................................ 19
The document guides you through deploying SolarWinds Packet Analysis Sensors to specific nodes that are discovered by your Orion-platform product. These sensors provide the data for the Quality of Experience dashboard in the Web Console.
How SolarWinds Packet Analysis Sensors Work

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

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

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

Network Packet Analysis Sensor (NPAS)

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

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

Packets that correspond to monitored applications are analyzed for Quality of Experience metrics, such as response times or traffic volume. Data are then sent to the Orion server using the SolarWinds communication agent.
Server Packet Analysis Sensor (SPAS)

A server sensor (SPAS) can monitor:

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

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

Limitations to Packet Analysis Sensors

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

Use the following table to review the sensor limitations.

<table>
<thead>
<tr>
<th>Sensor Limitations</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum throughput (NPAS and SPAS)</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>Maximum number of nodes per sensor (NPAS)</td>
<td>50 nodes</td>
</tr>
<tr>
<td>Maximum number of node/application pairs (NPAS and SPAS)</td>
<td>50,000 pairs</td>
</tr>
<tr>
<td>Maximum number of sensors deployed on your network</td>
<td>1,000 sensors</td>
</tr>
<tr>
<td>Maximum number of applications per node/sensor (NPAS and SPAS)</td>
<td>1,000 applications per node</td>
</tr>
</tbody>
</table>

The system requirements increase for every 100 Mbps of traffic.
System Requirements

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

You will need administrative privileges for each node or switch.

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

Network Packet Analysis Sensors (NPAS)

<table>
<thead>
<tr>
<th>Hardware/Software</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS</td>
<td>Windows 7 or later, 64-bit</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2008 or later, 64-bit</td>
</tr>
<tr>
<td></td>
<td>Note: 32-bit operating systems are not supported.</td>
</tr>
<tr>
<td>CPU Cores</td>
<td>2 CPU Cores + 1 CPU Core per 100 Mbps</td>
</tr>
<tr>
<td>Hard drive space</td>
<td>500 MB</td>
</tr>
<tr>
<td>RAM</td>
<td>1 GB + 1 GB per 100 Mbps</td>
</tr>
<tr>
<td></td>
<td>(2 GB + 1 GB per 100 Mbps recommended)</td>
</tr>
<tr>
<td>Network</td>
<td>1 Gbps maximum throughput</td>
</tr>
<tr>
<td>Other</td>
<td>SPAN, mirror port, or in-line tap on the monitored switch</td>
</tr>
</tbody>
</table>

Server Packet Analysis Sensors (SPAS)

<table>
<thead>
<tr>
<th>Hardware/Software</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS</td>
<td>Windows 7 or later, 64-bit</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2008 or later, 64-bit</td>
</tr>
<tr>
<td></td>
<td>Note: 32-bit operating systems are not supported.</td>
</tr>
</tbody>
</table>
System Requirements

<table>
<thead>
<tr>
<th>Hardware/Software</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Cores</td>
<td>2 CPU Cores + 1 CPU Core per 100 Mbps</td>
</tr>
<tr>
<td>Hard drive space</td>
<td>500 MB</td>
</tr>
<tr>
<td>RAM</td>
<td>256 MB + 500 MB per 100 Mbps</td>
</tr>
<tr>
<td></td>
<td>(256 MB recommended + 500 MB per 100 Mbps)</td>
</tr>
<tr>
<td>Network</td>
<td>1Gbps maximum throughput</td>
</tr>
</tbody>
</table>

Port Requirements

<table>
<thead>
<tr>
<th>Port #</th>
<th>Protocol</th>
<th>Direction</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>17778</td>
<td>TCP</td>
<td>Outgoing</td>
<td>Used to send information back to your SolarWinds server.</td>
</tr>
<tr>
<td>135</td>
<td>TCP</td>
<td>Incoming</td>
<td>Used by your SolarWinds server to deploy the sensors and to apply updates to the sensors.</td>
</tr>
</tbody>
</table>

Port Mirroring Requirements

When deploying a Network Packet Analysis Sensor, you must create a SPAN, mirror port, or in-line tap on the monitored switch. For virtual switches you may create promiscuous port groups or a vTap instead. This requires at least one extra network interface to collect data from the managed network interface, a server to monitor the copied traffic, and a network cable to connect the mirrored port to the physical server.

Please view your vendor specific documentation for instructions on how to set up port mirroring. You can create port mirrors for both physical switches and virtual switches.

For an example of how to create SPAN, see your switch’s documentation.
Common Packet Analysis Sensor Deployment Scenarios

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

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

<table>
<thead>
<tr>
<th>Aggregation level</th>
<th>Sensor Deployment</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>I have access to my network (NPAS)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Per application</td>
<td>Deploy an NPAS to a port mirror that monitors all traffic to and from the application</td>
<td>Automatic</td>
</tr>
<tr>
<td>Per site</td>
<td>Deploy an NPAS to a port mirror that monitors all traffic to and from the site</td>
<td>Add a sampling of endpoints to the NPAS as managed nodes</td>
</tr>
<tr>
<td>Per client</td>
<td>Deploy an NPAS to a port mirror that monitors all traffic to and from the site</td>
<td>Add all of the endpoints to the NPAS as managed nodes</td>
</tr>
<tr>
<td><strong>I have access to my application servers (SPAS)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Per application</td>
<td>Deploy the SPAS directly on the application server</td>
<td>Automatic</td>
</tr>
<tr>
<td>Per site</td>
<td>Deploy the SPAS to select endpoints</td>
<td>Automatic</td>
</tr>
<tr>
<td>Per client</td>
<td>Deploy the SPAS to all endpoints</td>
<td>Automatic</td>
</tr>
</tbody>
</table>
Common Packet Analysis Sensor Deployment Scenarios

Notes:

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

- All monitored nodes must be managed by your Orion Platform product before they can be monitored by sensors.

- If the node is managed by your SolarWinds Orion server, applications and nodes are detected by default. If packet data is not collected, go to Settings > QoE Settings > Global QoE Settings, and activate the auto-detect option. You can also manually monitor applications and managed nodes or ignore them. See Monitoring QoE Applications and Defining Nodes for a Network Sensor for more information.

Aggregation per application

This deployment scenario provides a broad indication of the overall response time between computers and the monitored application.
Aggregation with access to network (NPAS)

Notes:

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

To deploy the network sensor:

2. Select the Network option, and then click Add Nodes.
3. Choose the node with the port mirror, SPAN or network tap set up to monitor your network switch.
4. Assign and test the credentials for the selected node.
5. Click Add Node(s) and Deploy Agent(s) to deploy the network sensor to the node.

**Aggregation with access to application servers (SPAS)**

To deploy from your Web Console:

2. Select the Server option, and then click Add Nodes.
3. Choose the nodes with the application you want to monitor.
4. Assign and test the credentials for each node.
5. Click Add Node(s) and Deploy Agent(s) to deploy an agent on the node.
**Aggregation per site**

This deployment scenario provides an aggregated response time per monitored site or network to the application. For example, the response time from your Detroit office to your datacenter is 1 second, but the response time from Boston to your datacenter is 7 seconds. If you used the aggregation per application deployment method, the response time for the application is 4 seconds.

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

**Aggregation per site with access to network (NPAS)**

![Diagram showing network setup with NPAS](image)

**Notes:**

- Create a port mirror, SPAN, or network tap on the switch with all the network traffic to or from the site. See [System Requirements](#) for more information.
Common Packet Analysis Sensor Deployment Scenarios

- Identify a sample set of users whose computers are monitored by the NPAS
- You can monitor multiple applications using the same NPAS.

**To deploy the network sensor:**

1. Click **Settings > QoE Settings > Manage QoE Packet Analysis Sensors > Add Packet Analysis Sensor**.
2. Select the **Network** option, and then click **Add Nodes**.
3. Choose the node with the port mirror, SPAN or network tap set up to monitor your network switch.
4. Assign and test the credentials for the selected node.
5. Click **Add Node(s) and Deploy Agent(s)** to deploy the network sensor to the node.

**Aggregation per site with access to application servers (SPAS)**

**Note:** Identify a sample set of users whose computers are monitored by the SPAS
To deploy from your Web Console:

2. Select the Server option, and then click Add Nodes.
3. Select the sampled set of user computers to monitor.
4. Assign and test the credentials for each node.
5. Click Add Node(s) and Deploy Agent(s) to deploy an agent on the node.

**Aggregation per computer**

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

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

This method requires all workstations to be managed within your Orion Platform product.
Aggregation per computer with access to network (NPAS)

Notes:

- Create a port mirror, SPAN, or network tap on the switch with all the network traffic to or from the site. See System Requirements for more information.
- You can monitor multiple applications using the same NPAS.

To deploy the network sensor:

2. Select the Network option, and then click Add Nodes.
3. Choose the node with the port mirror, SPAN or network tap set up to monitor your network switch.
4. Assign and test the credentials for the selected node.
5. Click **Add Node(s) and Deploy Agent(s)** to deploy the network sensor to the node.

**Aggregation per computer with access to application servers (SPAS)**

To deploy from your Web Console:

1. Click **Settings > QoE Settings > Manage QoE Packet Analysis Sensors > Add Packet Analysis Sensor**.
2. Select the **Server** option, and then click **Add Nodes**.
3. Select the all user computers to monitor.
4. Assign and test the credentials for each node.
5. Click **Add Node(s) and Deploy Agent(s)** to deploy an agent on the node.
Deploying Packet Analysis Sensors

Deploying a Server Sensor

These sensors can only monitor the packet traffic of a single application. After you deploy a server sensor to the application node, the sensor captures packets to and from the node. It then identifies packets that are sent to or from the monitored application and analyzes them for Quality of Experience metrics, such as response time or traffic volume.

To deploy a server sensor:

1. Click **Settings > QoE Settings > Manage QoE Packet Analysis Sensors > Add Packet Analysis Sensor**.

2. Select the **Server** option, and then click **Add Nodes**.

3. Choose the Windows nodes to which you want to deploy your server sensors, and then click **Add Selected Node**.

4. Assign and test credentials for each node on which you want to deploy sensors.

5. Click **Add Node(s) and Deploy Agent(s)** to deploy agents.

**Notes:**

- Deployment may take some time and will run as a background process.
- QoE automatically chooses settings, including the interface to capture traffic data and limits to memory and CPU, during agent deployment. You can change these settings once deployment is complete by selecting the sensor and clicking **Edit**.
- When installation is complete, you will see a message in the notification bar.
- You can confirm the deployment status on the Manage QoE Packet Analysis Sensors page.
Deploying Packet Analysis Sensors

To specify manually which applications to monitor, see Monitoring QoE Applications. Applications are automatically detected and added by default.

**Deploying a Network Sensor**

Network sensors must be deployed on any server connected to a switched SPAN/mirror port or in-line tap.

**Notes:**

- If you deploy from the Additional Web Console, the node must be reachable from the main polling engine during deployment. Data from sensors are directed to the polling engine assigned to the node when the sensor was deployed.
- Network sensors can monitor up to 50 discrete applications through a single network interface, but they cannot monitor more than 1 GB throughput.

**To deploy a Network sensor:**

1. Click **Settings > QoE Settings > Manage QoE Packet Analysis Sensors > Add Packet Analysis Sensor**.
2. Select the **Network** option, and then click **Add Nodes**.
3. Move the node that monitors your switch to the Selected Nodes panel, and click **Add Selected Node**.
4. Assign and test the credentials for the selected node.
5. Click **Add Node(s) and Deploy Agent(s)** to deploy an agent on the node.
6. Expand the network sensor you added, and click **Add Nodes to Monitor**.
7. Choose which node’s traffic you want to monitor from the switch, and click **Next**.
8. Select the specific application to monitor, and click **Next**. QoE can automatically detect the first 50 applications, or you can add specific applications.

When sensor deployment is complete, the installation wizard displays a message.

To specify manually which nodes and applications to monitor, see Monitoring QoE Applications and Nodes. Nodes are automatically detected and added by default.
Monitoring QoE Applications and Nodes

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

See Global QoE Settings for more information on how you can change these settings.

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

For more information, refer to the following topics:

- Manage Global QoE Settings
- Monitoring QoE Applications
- Defining Nodes for a Network Sensor

Manage Global QoE Settings

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

QoE Applications

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

**Auto-detect QoE applications**

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

**Note:** If you automatically detect nodes, you should also automatically detect applications.
Monitoring QoE Applications and Nodes

HTTP application domain detection level
Choose how granularly QoE breaks up http traffic to monitor.

- **Top level (http://*)** - Monitor all http traffic.
- **Second level (http://hostname/*)** - Separate and monitor http traffic based on domains.
- **Third level (http://hostname/path1/*)** - Separate and monitor http traffic based on the domain and 1st level directory within each domain.

Add auto-detected applications that are
Further refine the applications that are monitored by choosing to monitor all application traffic sources, traffic destinations, or all application traffic. Packet sources and destinations are based on the source or destination IP address included in the packet.

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

For each node, include top X application that have at least Y% of total QoE traffic.
Filter the number of applications that are monitored to applications that generate a certain amount of network traffic.

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

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

**Note:** If you automatically detect nodes, you should also automatically detect applications.
Add auto-detected monitored nodes that are

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

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

## Monitoring QoE Applications

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

### Notes:

- Because of the hardware requirements needed to process large amounts of traffic, SolarWinds recommends that you preferentially monitor business-critical nodes and applications. For more information about recommended hardware specifications, see [System Requirements](#).

- You should not assign more than 50 applications to a single node due to potential performance issues. However, you can monitor up to 1000 applications.

### Monitoring Applications Automatically

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

**Note**: Only applications that meet the criteria selected in **QoE Applications** are monitored automatically.
Monitoring QoE Applications and Nodes

To monitor application traffic automatically:

1. Click Settings > QoE Settings > Manage Global QoE Settings.
2. Select Active in Auto-detect QoE applications.
3. Change other settings to refine the number of applications you automatically monitor. See Global QoE Settings for more information on the settings.
4. Click Submit.

Monitoring Applications Manually

You may choose to add monitored applications manually to QoE.

To select specific applications for monitoring:

1. Click Settings > QoE Settings > Manage QoE Applications.

   **Notes:**
   - Applications are only listed if there are monitored nodes. You must first add a Network or Server Sensor before you can enable any applications. For more information, see Common Packet Analysis Sensor Deployment Scenarios.
   - Applications listed with the Enabled/Disabled toggle "ON" are currently being monitored on at least one node.
   - Applications can be disabled (the Enabled/Disabled toggle "OFF") which means that no traffic for the application is currently collected on any node.

2. Click Add New.
3. Select Choose a pre-configured application.
   **Note:** Applications that are already enabled will not appear in the list.
4. Use the Search or Group By options to find the application you want to monitor, select it, and then click Next.
5. On the Configure Application view, edit the Category, Risk Level, or Productivity Rating as necessary, and then click Next.
6. On the Configure Data Collection view, choose the node(s) you want to monitor for this type of traffic.
   **Note:** Only nodes that have already been specified as nodes to monitor on the Manage QoE Nodes page appear in this list.
Defining Nodes for a Network Sensor

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

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

Defining Nodes for a Network Sensor

Nodes are automatically detected and monitored when network traffic is detected either originating from or terminating at a node. However, you can manually specify the nodes instead. After the network sensor has been successfully deployed, add applications and nodes to monitor. For information about adding applications, see Monitoring QoE Applications.

Note: You can monitor up to 50 nodes per network sensor.

Adding Nodes Automatically

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

Notes:

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

To monitor nodes automatically:

1. Click Settings > QoE Settings > Manage Global QoE Settings.
2. Select Active in Auto-detect QoE nodes.
3. Change other settings to refine the number of nodes you automatically monitor. See Global QoE Settings for more information on the settings.
4. Click Submit.
Monitoring QoE Applications and Nodes

**Adding Nodes Manually**

You may choose to add monitored nodes manually to a Network Sensor. If a node is already monitored and you want to monitor it with a different sensor, you must delete the node from the original sensor before you can add it to the new network sensor.

**To add nodes for a network sensor to monitor:**

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

<table>
<thead>
<tr>
<th>Node</th>
<th>Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.110.67.159</td>
<td>4Shared, Amazon Web Services, CIFS, FTP, HTTP, MS SQL</td>
</tr>
</tbody>
</table>

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

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

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

When you click Edit Sensor, you can configure:

- the monitored interface
- the allocated CPU cores and memory

Configuring the Monitored Interface

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

To change the interface monitored by a sensor:

1. Click Settings > QoE Settings > Manage QoE Packet Analysis Sensors.
2. Select the sensor to edit.
3. Click Edit Sensor.
4. Select the desired interface from the Interface to capture QoE data drop-down list.
5. Click Save.
**Configuring the Number of CPU Cores and Allocated Memory**

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

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

<table>
<thead>
<tr>
<th>Number of CPU Cores</th>
<th>Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Not Recommended</td>
</tr>
<tr>
<td>2</td>
<td>Suitable for 100 Mbps links</td>
</tr>
<tr>
<td>3-4</td>
<td>Gigabit links with low utilization</td>
</tr>
<tr>
<td>5-6</td>
<td>Gigabit links with medium utilization</td>
</tr>
<tr>
<td>7+</td>
<td>Gigabit links with high utilization</td>
</tr>
</tbody>
</table>

To change the sensor thresholds:

1. Click **Settings > QoE Settings > Manage QoE Packet Analysis Sensors**.
2. Select the sensor to edit.
3. Click **Edit Sensor**.
4. In the **Memory** field, select the number of GB you want to allocate to the sensor.
   
   **Note:** If you allocate less than the recommended amount of memory, you may see reduced performance.
5. In the **CPU Cores** field, select the number of CPU cores you want to allocate to the sensor.
   
   **Note:** If you allocate fewer than the recommended number of CPU cores, you may see reduced performance.
6. Click **Save**.
Configuring Thresholds

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

**Note:** It is best to allow the sensors to collect a few days' worth of data before setting thresholds.

**To change the number of CPU cores and memory allocated to the sensor:**

1. Click **Settings > QoE Settings > Manage QoE Applications**.
2. Select the application to edit.
3. Click **Edit**.
4. Click **Next**, and then click **Next** again.
5. On the Summary page, click the plus sign by **Thresholds**.
6. Select **Override Orion General Thresholds** next to each data type.
7. Change the threshold. You can use specific thresholds or you can use a dynamic threshold based on the baseline established. The default baseline is seven days, which is configurable in the **Orion Polling Settings** page.
8. Click **Finish**.